Prof. Dr. jur. Josef Scherer

Rechtsanwalt und Consulter, Professor für Compliance, Risiko- und Krisenmanagement sowie Sanierungs- und Insolvenzrecht und Leiter des Stabsbereichs ESGRC an der Technischen Hochschule Deggendorf; Richter am Landgericht a.D.

Fabian Pothorn

Informationssicherheits-Beauftragter der Technischen Hochschule Deggendorf, Lehrbeauftragter und Unternehmensberater für IT-Governance und Informationssicherheits-Managementsysteme

Prof. Dr. jur. Josef Scherer / Fabian Pothorn[1]

Integriertes IT- (KI-) Governance-Compliance-Managementsystem

- als Basis für Wehr- und Verteidigungsfähigkeit

Deggendorf, 3.1.2026

Gender-Hinweis: Die in diesem Artikel verwendeten Personenbezeichnungen beziehen sich auf sämtliche Geschlechter gleichermaßen. Auf gegenderte Bezeichnungen wird zugunsten einer besseren Lesbarkeit verzichtet.

[1] Die ausführlichen Autorenprofile finden sich am Ende des Artikels.

Einleitung[2]

Ein IT- (KI-) Governance-Compliance-Managementsystem unterstützt Organe und Beschäftigte durch eine angemessene und wirksame Aufbau- und Ablauforganisation bei der Erfüllung rechtlicher und technischer Anforderungen im Rahmen der Führung und Überwachung ihrer Organisation[3] im Bereich IT (mit KI).

Dabei sind die DIN ISO 37000 (Governance von Organisationen), ISO 38500 (IT-Governance), ISO 42001 (KI-Managementsystem), DIN ISO 22301 (Business Continuity-Managementsystem), DIN ISO 22361(Leitlinien für das Krisenmanagement) und nicht zuletzt die DIN ISO 27001 (Informationssicherheits-Managementsystem) (juristisch) ergänzungsbedürftig, um den Anforderungen zwingender Regularien zu genügen.[4]

Die sich weiterhin zuspitzende Cyberbedrohungslage inklusive Bedrohungspotenziale durch die Nutzung von Künstlicher Intelligenz ist die dominierende Sorge der meisten Organisationen. Im Zusammenhang mit der damit verbundenen stark verschärften Regulierung wachsen u.a. auch die Risiken von Streitigkeiten über Versicherungspolicen[5] und Cyber-Compliance in der Lieferkette.[6]

Da der hybride Krieg[7] seitens Russlands, Chinas, Nordkoreas, des Irans und anderen gegen Deutschland und Europa nicht mehr – wie aus „political correctness“ irreführend bezeichnet – lediglich „Bedrohung“, sondern

---

[2] Dieser Artikel baut auf *Scherer, Pothorn, Jones*, *Integriertes Compliance-Management-System für die IT-/KI-Governance im Rahmen der digitalen Transformation*, *IT-Governance* 2025, S. 8-13 auf.

[3] Governance.

[4] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Vorwort.

[5] Vgl. hierzu die aktuelle Rechtsprechung des OLG Frankfurt und des BGH zur Versagung des Versicherungsschutzes bei D&O-Versicherungen bei „wissentlicher Pflichtverletzung“ und Kardinalpflichtverletzung. Dieses Thema wird auch bei Verstoß des Geschäftsführers, Vorstandes oder eines „Leitenden Angestellten“, z.B. CISO (Chief Information Security Officer) oder ISB (Informations-Sicherheits-Beauftragter), gegen gesetzliche Pflichten aus der IT- (KI-) Governance-Compliance relevant. Vgl. hierzu *Scherer, Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, in: ZInsO (Zeitschrift für das gesamte Insolvenz- und Sanierungsrecht), 28. Jahrgang, 31/2025, 31.07.2025, S. 1515-1538, zum kostenlosen download unter: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf und *Scherer, Seehaus*, Managerhaftung, D&O-Versicherung und Risikofrüherkennung im Lichte aktueller Rechtsprechung, 1 / 2026, zum kostenlosen Download auf Risknet.de.

[6] Vgl. *Beck*, Technologiebezogene Streitigkeiten dominieren 2025: Cybersicherheit und KI im Fokus, 14.02.2025, online abrufbar unter https://rsw.beck.de/aktuell/daily/meldung/detail/umfrage-unternehmensjuristen-2025-cybersicherheit-ki-untersuchungen (zuletzt abgerufen am 30.11.2025).

[7] Zu hybrider Kriegsführung zählen u.a. Cyberangriffe, Spionage und Abhöraktionen, Sabotage, Desinformation und Propaganda etc., vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 06.03.2025, Hybride Bedrohungen, abgerufen am 13.12.2025, URL: https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen.

eingetretenes Ereignis ist,[8] sind nachfolgende Ausführungen zugleich auch ein *Beitrag zur Wehr- und Verteidigungsfähigkeit von Organisationen und Nationen*.

Die zahlreichen IT-Vorfälle mit hohen Schäden zeigen, dass sich Vorstände, Geschäftsführer, CISO[9], CIO[10], ISB[11], Aufsichtsorgane, Abschlussprüfer und Lines of Defense-Funktionen ebenso wie Auditoren und Zertifizierer nicht immer das Wichtige richtig machen.[12]

1. Erste Begrifflichkeiten und rechtliche Grundlagen für ein IT- (KI-) Governance-Compliance-Managementsystem

1.1 Erste Begrifflichkeiten

Vorab: Für die meisten hier verwendeten Begriffe gibt es keine sog. Legaldefinitionen, also verbindlich festgelegte Definitionen.

Compliance bedeutet pflichtgemäßes Verhalten in Hinblick auf allgemein verbindliche Regeln (Gesetze, Rechtsprechung), aber auch in Hinblick auf für verbindlich erklärte (interne) Vorgaben [z. B. Regelungen aus dem „Code of Conduct“ (unternehmensspezifische Verhaltensregelungen)] oder einem Anstellungsvertrag.[13]

Der Begriff *Risiko* wird als Streuung um einen Erwartungswert (erwartetes bzw. gewünschtes Ziel) definiert. Nach dieser Definition werden sowohl positive Abweichungen (Chancen) als auch negative Abweichungen (Gefahren) berücksichtigt.[14]

Risikomanagement beschäftigt sich mit Unsicherheiten bei Entscheidungen und der Zielerreichung. (Unternehmerische) Tätigkeiten und Ziele sind fast immer mit Unsicherheiten verbunden. Aufgabe des Risikomanagements ist es, die Chancen und Gefahren systematisch zu identifizieren und sie

---

[8] Vgl. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 06.03.2025, Hybride Bedrohungen, abgerufen am 13.12.2025, URL: https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen.

[9] Chief Information Security Officer (CISO).

[10] Chief Information Officer (CIO).

[11] Informations-Sicherheits-Beauftragter (ISB).

[12] Wichtige – aber häufig vernachlässigte Themen sind aktuell neben IT-Governance- auch Kardinalpflicht-, Financial-Governance-, Risiko-Governance-, Business Continuity-Governance-Compliance, vgl. *Scherer, Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, in: ZInsO (Zeitschrift für das gesamte Insolvenz- und Sanierungsrecht), 28. Jahrgang, 31/2025, 31.07.2025, S. 1515-1538, zum kostenlosen download unter: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf.

[13] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.18.

[14] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.18.

hinsichtlich potenzieller Auswirkungen auf das Unternehmen zu bewerten, d.h. zu analysieren, zu quantifizieren und zu steuern.

Es gibt auch für „*IT- oder KI-Governance*“, ebenso wie für „*Governance*“, keine Legaldefinition. Daher sind die Definitionen für diese Begriffe aus den einschlägigen rechtlichen Regelungen, dem Stand der Technik[15] und aus einschlägigen Standards*, vgl. oben,* jeweils Normabschnitt 3[16] ,,*Definitionen*“ u. v. m. abzuleiten.

IT- (KI-) Governance lässt sich juristisch als die „*nachhaltige, compliance- und risikobasierte gewissenhafte Führung und Überwachung von Organisationen inkl. Interaktion mit relevanten Stakeholdern im Bereich IT (KI)“* definieren.[17]

Das *IT- (KI-) Governance-Compliance-Managementsystem* ist eine Aufbau- und Ablauforganisation mit diversen Komponenten[18], mit dem Zweck, eine Organisation bei Entscheidungen, Zielsetzung, Planung, Umsetzung sowie Steuerung und Überwachung zur Erreichung zwingender und fakultativ gesetzter Ziele im Bereich IT- (KI-) Governance zu unterstützen.[19]

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- (KI-) Compliance-Management (dies an erster Stelle!),
- IT- (KI-) Risikomanagement,
- IT- (KI-) Strategie,
- IT- (KI-) Planung,
- IT- (KI-) Bereichs-Organisation und -Prozesse
- IT- (KI-) Umsetzung,
- IT- (KI-) IKS,
- IT- (KI-) Revision,
- IT- (KI-) Steuerung und -Überwachung,
- IT- (KI-) Reporting,
- IT- (Service-) Management (das serviceorientierte 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- (KI-) Social Engineering,
- IT-Lieferkettenmanagement,
- Etc.

---

[15] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Einleitung.

[16] Definitionen zu Informationssicherheit finden sich auch in der ISO 27000.

[17] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.16, 169.

[18] Z. B. Rollen, Zielen, Ressourcen, Prozessabläufen, Delegationen und Interaktionen etc..

[19] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S. 43.

1.2 Das Verhältnis der IT-Governance nach ISO / IEC 38500:2024 zur Governance nach DIN ISO 37000:2024

Der Beschluss zur identischen Übernahme der ISO 37000:2021 als DIN ISO 37000 fiel im September 2023. Aufgrund ihres Grundlagencharakters für Governance wurde seitens des DIN der Bedarf für eine deutsche Fassung der ISO 37000 für Mittelstand und KMU festgestellt.

Die ISO / IEC 38500 (IT-Governance) ist mit ihrer ersten Version von 2016 wesentlich älter als die ISO 37000: 2021. Die aktuelle dritte Version ISO / IEC 38500: 2024 richtet sich inzwischen stark am Verständnis von Governance nach ISO 37000 aus.[20] Gleichwohl bemerkt *Klotz*[21] zu Recht, es würden in der ISO / IEC 38500 viele, auch wichtige Aspekte der Governance, die in der ISO 37000 dargestellt seien, fehlen. Beispielsweise sei der „Strategie-Grundsatz“ mit der Anforderung der Implementierung eines Internen Kontrollsystems (IKS), eines Risiko- und eines Compliance-Managementsystems und der Nutzung externer Prüfungen bei der IT-Governance nicht enthalten. Dass diese *Lines-of-Defense*-Systeme auch die IT-Governance umfassen *müssen*, ergibt sich unabhängig von deren Erwähnung in einem ISO-Standard bereits aus Gesetzgebung, Rechtsprechung und weiteren verpflichtenden Regularien.[22] Als weiteres Manko nennt *Klotz*[23] das Fehlen des Grundsatzes „Daten und Entscheidungen“, der in der ISO 37000 angemessen ausführlich dargestellt werde.[24]

Bereits aus diesen Ausführungen ergibt sich die Sinnhaftigkeit der Integration diverser Standards sowohl bzgl. Governance und IT-Governance, aber auch in Hinblick auf andere Standards, wie z.B. für Compliance nach DIN ISO 37301: Compliance schafft die Grundlagen, um Risiken, die sich aus der Nichteinhaltung zwingender (rechtlicher und / oder technischer) Anforderungen ergeben, zu identifizieren, zu bewerten und zu steuern und ist somit aufgrund des von allen zu beachtenden Legalitätsprinzips Basis für Governance, IT- oder KI-Governance, Business Continuity oder Informationssicherheit.[25]

---

[20] Vgl. *Klotz*, IT-Governance genormt – die neue ISO / IEC 38500 (revolutions), IT-Governance 2024, S.19 ff.

[21] Vgl. *Klotz*, IT-Governance genormt – die neue ISO / IEC 38500 (revolutions), IT-Governance 2024, S.19 ff., 24.

[22] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.133.

[23] Vgl. *Klotz*, IT-Governance genormt – die neue ISO / IEC 38500 (revolutions), IT-Governance 2024, S.19 ff., 24.

[24] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.169.

[25] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, S.20.

1.3 Rechtliche Grundlagen für ein IT- (KI-) Governance-Compliance-Managementsystem

Leitungsorgane und Führungskräfte tragen Verantwortung für die Erreichung des Zwecks einer Organisation.[26]

Digitale Transformation (mit KI), Nachhaltigkeit (ESG), gewissenhafte Führung von Organisationen (§§ 43 GmbHG, 93, 116 AktG, 130, 30, 9 OWiG, 53 HHGrdsG etc.)[27], die Implementierung und der Betrieb eines (Integrierten*) (IT- / KI-)* Governance-Managementsystems erfordern zuallererst die Beachtung diverser rechtlicher Anforderungen (Compliance), wozu auch die „Anerkannten Regeln der Technik" und der „Stand der Technik" zählen.[28] Ebenso sind für diese Themen angemessene Referenzgrößen, Standards oder Leitfäden heranzuziehen, die auch auf die jeweilige Organisation bzw. das jeweilige Unternehmen anwendbar sind, vgl. dazu unten 2..

Es besteht keine Pflicht, ein IT- (KI-) Governance-Managementsystem in Anlehnung an DIN ISO 37000 bzw. ISO / IEC 38500 zu betreiben.

Anders sieht es die Rechtsprechung bzgl. der von IT- (KI-) Governance umfassten Risiko- und Compliance-Managementsysteme[29] und Internen Kontrollsysteme.[30] Wenn aus der Organisation heraus etwas passiert, wird das Unterlassen der Einrichtung dieser Systeme als (Organisations-) Pflichtverletzung angesehen. Umgekehrt wirken implementierte Compliance- oder Interne Kontroll-Systeme nach neuester höchstrichterlicher Rechtsprechung des BGH und des EuGH u. U. enthaftend[31].

Und: Es sind alle Pflicht-Anforderungen aus dem Bereich IT- (KI-) Governance, also der gewissenhaften Führung und Überwachung von Organisationen im Bereich IT / KI – unabhängig von Standards und Managementsystem – zwingend zu erfüllen und häufig haftungsbewehrt, wie z. B. die Nichtbeachtung regulativer Anforderungen (KI-Verordnung, NIS2-Umsetzungsgesetz, DORA, §§ 43 GmbHG, 93 AktG, u. v. m.).

Dabei wird ersichtlich, dass Zusammenspiel und die Überschneidungen diverser Regulierungen kaum mehr zu überblicken sind.

---

[26] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, Kapitel 6.1.

[27] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kapitel 1.

[28] Vgl. *Scherer, Fruth*, Technik-Governance, Sonderpublikation des Bundesverbandes der Compliance-Manager, 2019.

[29] Vgl. *LG München I*: Urteil vom 10.12.2013, (Az. 5 HK O 1387/10 – „Neubürger").

[30] Vgl. *OLG Nürnberg*, Urteil vom 30.03.2022, (Az. 12 U 1520/19 – „Tankstellenpächter").

[31] Vgl. *Scherer, Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, in: ZInsO (Zeitschrift für das gesamte Insolvenz- und Sanierungsrecht), 28. Jahrgang, 31/2025, 31.07.2025, S. 1515-1538, zum kostenlosen download unter: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf und *Scherer, Seehaus*, Managerhaftung, D&O-Versicherung und Risikofrüherkennung im Lichte aktueller Rechtsprechung, 1 / 2026, zum kostenlosen Download auf Risknet.de.

Für die IT- (KI-) Governance ist eine zunehmende Regulierung zu beobachten. Dabei geht es um die Themenfelder der allgemeinen Datenverarbeitung, spezifische Anforderungen für Anbieter digitaler Dienste, IT- und Informationssicherheit sowie konkrete Regulierung in Bezug auf Künstliche Intelligenz. Da die gesetzlichen Anforderungen nicht immer aufeinander abgestimmt sind, kommt es zu Reibungseffekten. So sehen Unternehmen den Bedarf, die rechtlichen Anforderungen an den Datenschutz (Datenschutz-Grundverordnung) auf die aktuellen Bedürfnisse der KI-Nutzung anzupassen.[32] Für viele Unternehmen erscheinen die bisherigen Datenschutzanforderungen, die mit der DSGVO seit über sieben Jahren in Kraft sind, weiterhin überfordernd.[33]

Im November 2025 wurden Entwürfe für Vereinfachungen der Datenschutz- und KI-Gesetze („*Digitaler Omnibus für Datenschutz und für KI*“) von der EU vorgestellt. Diese zielen auf die Verringerung der Aufwände ab, die mit den rechtlichen Regelungen einhergehen.[34] Daher ist es erforderlich, nicht nur die Gesamtheit der geltenden Rechtsvorschriften zu erfassen, sondern auch die teilweise stark dynamischen Änderungen bestehender Gesetze, die in kurzer Abfolge erfolgen, zu berücksichtigen.

Hierzu als Beispiel „ein Teil der aktuellen Regulierung im Datenschutz- und Datenwirtschaftsrecht“:

[32] Vgl. *Lorber*, Unternehmen fordern Nachbesserung der DSGVO, 2025, online abrufbar unter: https://www.springerprofessional.de/datenschutz/dsgvo/unternehmen-fordern-nachbesserung-der-dsgvo/51803174 (zuletzt abgerufen am 19.12.2025).

[33] Ebenda.

[34] Vgl. *KPMG*, KI und „Digitaler Omnibus“, 2025, online abrufbar unter: https://kpmg.com/at/de/insights/2025/11/ki-und--digitaler-omnibus-.html (zuletzt abgerufen am 19.12.2025).

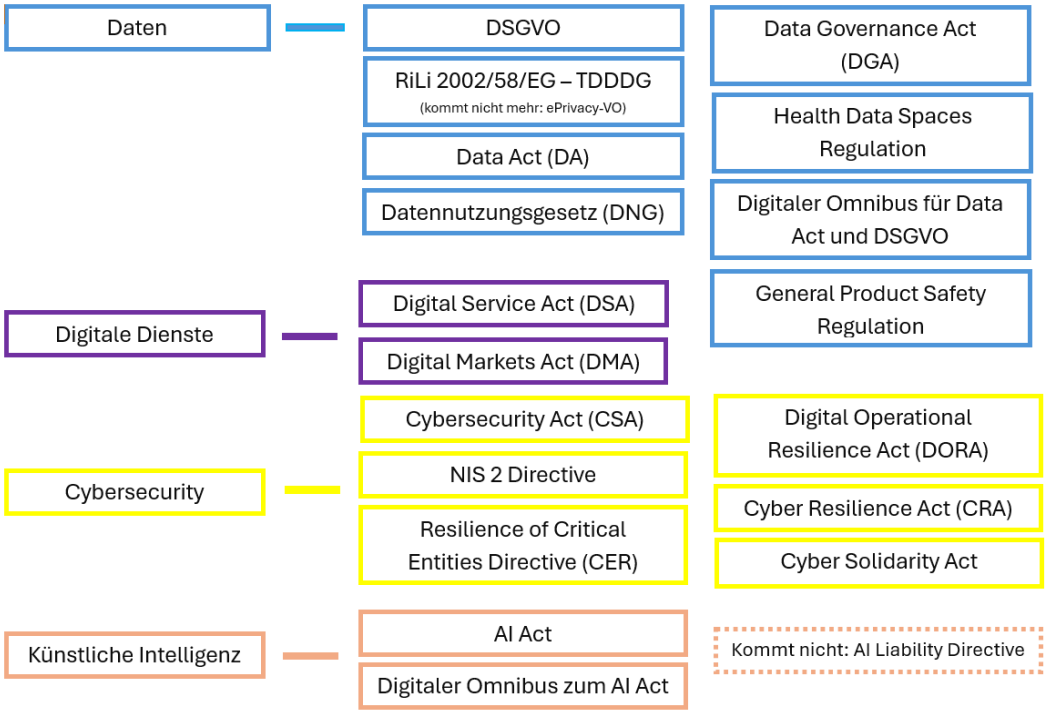

Abbildung 1: Auszug von lediglich eines Teils der aktuellen Regulierung im Datenschutz- und Datenwirtschaftsrecht[35]

In Bezug auf Daten und Informationen ist eine erhebliche Entwicklung regulatorischer Anforderungen ersichtlich. In Zusammenhang mit der o.a. digitalen Transformation und der zunehmenden Komplexität digitaler Technologien, die eine datengetriebene Organisation erst ermöglichen, stellen die gegenwärtigen Entwicklungen der rechtlichen Rahmenbedingungen eine logische Folge dar. „Daten“ und „Informationen“ sind elementare Komponenten in der Organisationssteuerung, wobei die Begrifflichkeiten voneinander zu unterscheiden sind.

Daten werden aus Zeichen gebildet, die als elementare Symbole (z. B. Buchstaben oder Zahlen), ohne inhärente Bedeutung zu verstehen sind. Durch Anwendung einer formalen Syntax werden Zeichen zu strukturierten Daten. Daten erhalten erst dann Informationsgehalt, wenn sie einer definierten Semantik zugeordnet werden.

[35] In Anlehnung an *Eckhardt*, DSGVO & Data Act: Was ist der Unterschied?, 2025. „*Datenwirtschaftsrecht*“ bezeichnet das Teilgebiet des europäischen Rechts, das die rechtlichen Rahmenbedingungen für die Erhebung, Verarbeitung, Nutzung, Weitergabe und den Austausch von Daten innerhalb der Europäischen Union systematisch regelt.

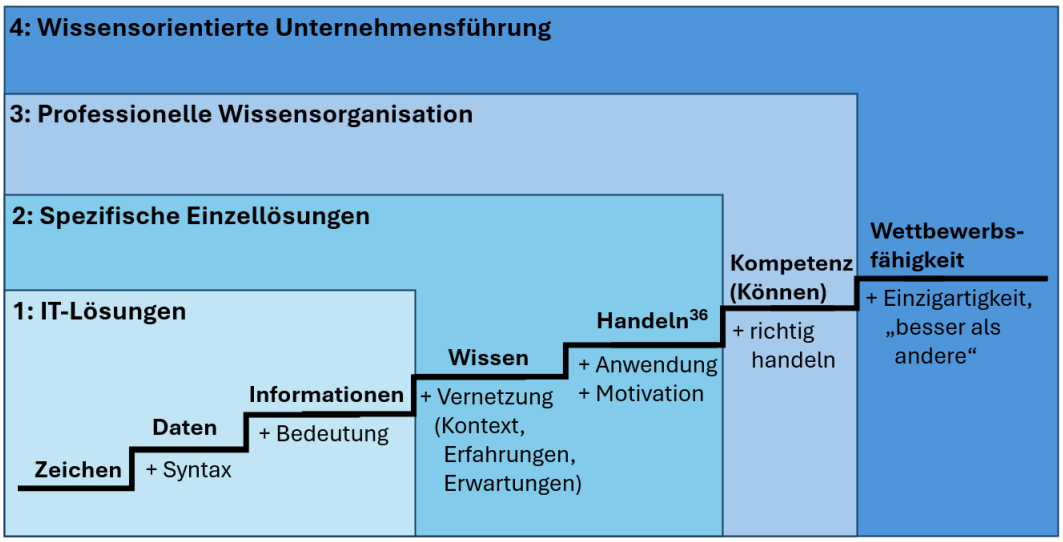

Abbildung 2: Daten als Basis für Wettbewerbsfähigkeit[37]

Insofern bilden Daten und Informationen die Grundlage des Entscheidens und Handelns einer Organisation. Durch das richtige („gute“) Entscheiden und Handeln (auf Basis angemessener und korrekter Informationen – vgl. die Business Judgment Rule, § 93 Abs. 1 S. 2 AktG) entsteht die Möglichkeit, Wettbewerbsfähigkeit und -vorteile zu erzielen. Im Sinne der Governance sind Daten als strategische Ressource anzuerkennen[38], weshalb dessen regulatorischer Rahmen gebührend zu berücksichtigen ist.

Zur Erfüllung der (IT- / KI-) Governance-Pflichten unterstützt ein entsprechendes Compliance-Managementsystem. Die Zertifizierung des (IT- / KI-) Governance-Managementsystems ist (noch) nicht verpflichtend, kann aber erhebliche Vorteile bringen. Während für (IT- / KI-) Governance nach DIN ISO 37000 und ISO / IEC 38500 in der Praxis von CMS-akkreditierten Zertifizierungsstellen nur eine Zertifizierung der inkludierten Compliance-Komponenten nach DIN ISO 37301 angeboten wird, sind die ISO / IEC 42001:2023 oder die DIN ISO 27001:2024 direkt zertifizierbar.

Hinweis: Nachfolgend finden sich eingerahmt z.T. Fragen für (interne) Audits oder Hinweise auf Tools oder Arbeitshilfen.

Diese sind keinesfalls abschließend, sondern zeigen lediglich beispielhaft, dass es sich lohnt, stets die Frage zu stellen:

Womit kann ich die jeweiligen Anforderungen erfüllen bzw. die Konformität auditieren?

---

[36] Anm. der Verfasser: „*Entscheiden und* Handeln“.

[37] Grafik vgl. *North*, Wissensorientierte Unternehmensführung, 2021, S.43.

[38] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.164.

Fragen für (interne) Audits:

Ist die Pflicht, ein wirksames / gelebtes IT- (KI-) Governance-Compliance-Managementsystem vorzuhalten, bekannt und dokumentiert?

Gibt es verbindliche (z. B. in Verträgen niedergelegte) Stakeholder- (z. B. Kunden-) Anforderungen bzgl. Pflicht und Inhalt zum Betrieb des IT- (KI-) Governance-Compliance-Managementsystems?

Sind die verpflichtenden Anforderungen aus Gesetzgebung, Rechtsprechung, Stand der Technik und sonstiger verbindlicher Regelungen (Compliance) im Bereich der IT- (KI-) Governance bekannt und dokumentiert?

2. Anwendbarkeit der zu integrierenden Standards bzw. Inselsysteme

Für *jede Art von Organisation* sind die DIN ISO 37000 und die ISO / IEC 38500 geeignete *Leitfäden* für (IT-) Governance, die ISO / IEC 42001 ein geeigneter *Standard* für ein KI-Managementsystem, die ISO 27001 für ein Informationssicherheits-Managementsystem, die ISO 22301 für ein Business Continuity-Managementsystem und die ISO 37301 für ein Compliance-Managementsystem.

Obwohl sowohl die DIN ISO 37000 als auch die ISO / IEC 38500 nicht gemäß der Harmonized Structure als Managementsystem-Standard mit zehn Normabschnitten ausgestaltet sind, lassen sich beide Standards in die anderen geläufigen Managementsystem-Standards integrieren, implementieren und auditieren.[39]

Mit entsprechenden (juristischen) Ergänzungen[40] ist die Integration dieser „Insel-Systeme“ als ein *angemessenes* IT- (KI-) Governance-Compliance-Managementsystem einfach.

Ob eine Vorgehensweise korrekt war oder Haftung und sonstige (existenzielle) Probleme auslöst, entscheiden jedoch letztendlich nicht Standards, Wissenschaft, gesetzliche oder behördliche Vorgaben, sondern die „letzte irdische Instanz“: Die Gerichtsbarkeit bzw. Judikative. Welches Gericht am Ende letztinstanzlich entscheidet, ist (inter-) national bisweilen eine komplexe Fragestellung.

---

[39] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.18.

[40] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, mit den jeweiligen juristischen Ergänzungen / Kommentierungen zu den einzelnen Normabschnitten.

Deshalb ist es auch bzgl. (IT-) Governance unverzichtbar, sich primär an die relevante Regulierung zu halten, also z. B. einschlägige Gesetze und höchstrichterliche Rechtsprechung, sowie den „Stand der Technik“ zu kennen und deren Anforderungen zu erfüllen.

Die Klärung der rechtlichen Basis und des zu verwendenden Standards[41] für (IT- oder KI-) Governance ist der notwendige „erste Schritt“ der Einführung.

Die oben genannten Standards sind auf jede Art von Organisation oder Teile dieser, unabhängig von ihrer Art, Größe oder Beschaffenheit anwendbar.[42]

Der Umfang der Nutzung von IT ist dabei unerheblich. Aus dem Compliance-Managementsystem heraus lassen sich die rechtlichen Pflichten für die Berücksichtigung der Themen IT-Governance, Informationssicherheit (mit Business Continuity) und KI-Einsatz in einer Organisation ableiten.

3. Definitionen („Digital Literacy“)

Nochmal: Für die diversen Themen im Bereich IT- (KI-) Governance[43] gibt es kaum sogenannte *Legaldefinitionen*. Legaldefinitionen sind vom Gesetzgeber oder der Rechtsprechung fix vorgegebene Begriffserklärungen, die für alle bindend sind.

In der Kalkar-Entscheidung hat beispielsweise das *BVerfG* allgemeinverbindlich festgelegt, was „*Anerkannte Regeln der Technik*“ und „*Stand der Technik*“ (auch für den IT-Bereich) bedeuten.[44]

Die meisten Begriffe – nicht nur im Bereich Governance – sind leider nicht bindend definiert, so dass in Forschung, Lehre und Praxis zunächst genau geklärt werden muss, welche Bedeutung den relevanten verwendeten Begriffen beigemessen wird.

Sofern in international anerkannten Standards Begriffe definiert werden, ist es ratsam, diese Definitionen zu verwenden. Dabei besteht jedoch die Gefahr, dass diese Definitionen sehr abstrakt, wissenschaftlich und unverständlich sein können. Es kann auch vorkommen, dass sie nicht mit den gängigen und anerkannten Definitionen aus dem jeweiligen fachlichen Bereich übereinstimmen oder wichtige Hinweise dazu fehlen.

Beispiel: Die DIN ISO 37000 definiert im Abschnitt 3.1.9 den Begriff „Risikotoleranz“. In den speziellen Risikomanagement-Standards, wie ISO 31000 („Risk management“) oder ISO/IEC 31010 („Risk assessment techniques“), sind ebenfalls viele einschlägige

---

[41] Vgl. *Klotz*, Normen und Standards für die KI-Governance, IT-Governance, 2024, S.37.

[42] Vgl. jeweils den Normabschnitt 1 der DIN ISO 37000, ISO / IEC 38500, ISO 37301, ISO / IEC 42001:2023, ISO 27001:2024.

[43] Vgl. bereits oben 1.1.

[44] „Technikklauseln“ nach BVerfG („Kalkar-Entscheidung“ von 1978). Vgl. hierzu ausführlich *Scherer, Fruth*, Technik-Governance, Sonderpublikation des Bundesverbandes der Compliance-Manager, 2019, zum kostenlosen Download im Internet.

Definitionen für den Themenbereich Risikomanagement zu finden. Statt „Risikotoleranz“ nutzen diese Standards den Begriff „Risiko-Appetit“. In Fachkreisen und gerade im Bereich der Regulierung ist nahezu ausschließlich der Begriff „Risiko-Appetit“ anstelle von „Risikotoleranz“ verbreitet.

Wichtiger als die Wahl der Begrifflichkeit ist aber die Beachtung des in der DIN ISO 37000 fehlende Hinweis, dass bei (IT-) Compliance-Risiken nie ein Risiko-Appetit bzw. eine Risikotoleranz dokumentiert sein sollte: Falls in diesem tolerierten Bereich ein Compliance-Vorfall eintreten würde, wäre ein „für möglich halten und sich damit abfinden“, also Eventualvorsatz, belegt: Fatal für die Betroffenen.

Gesetzgeber und sonstige Ersteller von Regularien verwenden häufig auch sogenannte „*unbestimmte Rechtsbegriffe*“, wie „sicher“, „angemessen“ etc. Hier ist sich der Betroffene nur im Klaren, dass etwas „sicher“ oder „angemessen“ sein muss. Er weiß aber oft nicht, was dies im Einzelfall konkret bedeutet. Da ist dann aufwändig zu recherchieren und darauf zu hoffen, dass ein u. U. damit befasstes Gericht diese Interpretation im Urteil teilt.[45]

Governance-Compliance behandelt alle – größtenteils sanktionsbewehrten – verpflichtenden bzw. zwingenden Anforderungen aus dem Bereich Governance, also der nachhaltigen compliance- und risikobasierten, gewissenhaften Führung und Überwachung von Organisationen inklusive der Interaktion mit relevanten Stakeholdern.

Governance-Compliance-Risiken sind die Gefahren, die sich aus der Nichtbeachtung der verpflichtenden bzw. zwingenden Anforderungen ergeben. Dabei dürften nahezu 90 % aller Governance-Risiken zugleich *Governance-Compliance*-Risiken darstellen, zumal der Bereich Governance größtenteils juristisch reguliert ist.

Digitalisierung heißt zu prüfen, ob das bisherige Geschäftsmodell ganz oder teilweise durch ein digitales Modell (z. B. Ersatz des stationären Handels durch Online-Handel über Plattformlösung) ersetzt oder ergänzt wird. Sofern die bisherigen Prozesse bestehen bleiben, ergibt sich eine verstärkt „geistige Leistung“ („intellectual property“, „digital assets“), die aus Wissen und Informationen in Form von Prozessen mit zugehörigen Komponenten (Rollen, Ziele, Ressourcen), IT-Systemen und IT-Tools, Algorithmen inkl. KI, Robotern und an vielen verbleibenden Stellen Menschen mit angemessenen Kompetenzen und Einstellungen besteht. Diese unterschiedlichen Komponenten einer Organisation werden, sofern sinnvoll, auf die digitale Transformation ausgerichtet.

Die meisten unternehmerischen Aktivitäten sind als Prozesse so zu modellieren, dass sie die diversen Anforderungen aus Compliance, Technik, Betriebswirtschaft, Informationssicherheit, Risikomanagement, Nachhaltigkeit etc. erfüllen und dafür sorgen, die gesetzten Ziele zu erreichen. Zugleich ist zu analysieren, welche Aktivitäten künftig noch von Menschen ausgeführt oder (teil-) automatisiert durch Anwendungen, IT-Systeme, Roboter,

[45] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.53.

Algorithmen oder sonstigen Tools aus den Bereichen Digitalisierung und KI ersetzt bzw. unterstützt werden.

Hierbei stellt sich die Frage, ob *KI-Systeme* nicht mit allgemeinen Anwendungen gleichzusetzen sind. KI-Systeme stellen stets digitale bzw. technische informationsverarbeitende Systeme dar und bilden somit eine Teilmenge der Informationstechnologie. Für diese Teilmenge bestehen spezifische Governance- und Compliance-Anforderungen, die für einen (rechts-) sicheren und ethischen Einsatz von KI-Technologien in Organisationen zu berücksichtigen sind. Spezifische Gesetze (z. B. AI Act) und KI-bezogene Standards (z. B. ISO / IEC 42001 oder NIST AI Risk Management Framework) setzen sich explizit mit den Governance-Compliance-Anforderungen im Kontext der KI auseinander, die im IT-Management auf ganzheitlicher operativer Ebene einzubeziehen sind.

Die vielen Möglichkeiten des Einsatzes von KI mit jeweiligen rechtlichen Anforderungen, Risiken und Chancen für die zu führende Organisation sollten bekannt sein und angemessen genutzt werden.

KI-Governance ist Teil der IT-Governance und diese wiederum der allgemeinen Governance. Diese Bereiche sollten nicht als „Silos“ oder „Managementsystem-Inseln“ ausgestaltet sein, sondern in Aufbau- und Ablauforganisation (Prozesse) integriert werden.

Ein wesentlicher Teil der Governance sind aufgrund umfassender Regulierung verpflichtende (Compliance-) Anforderungen. Deshalb ist Compliance die Basis für Governance, für IT- und auch für KI-Governance, so wie es in der nachfolgenden Abbildung 3 dargestellt wird.

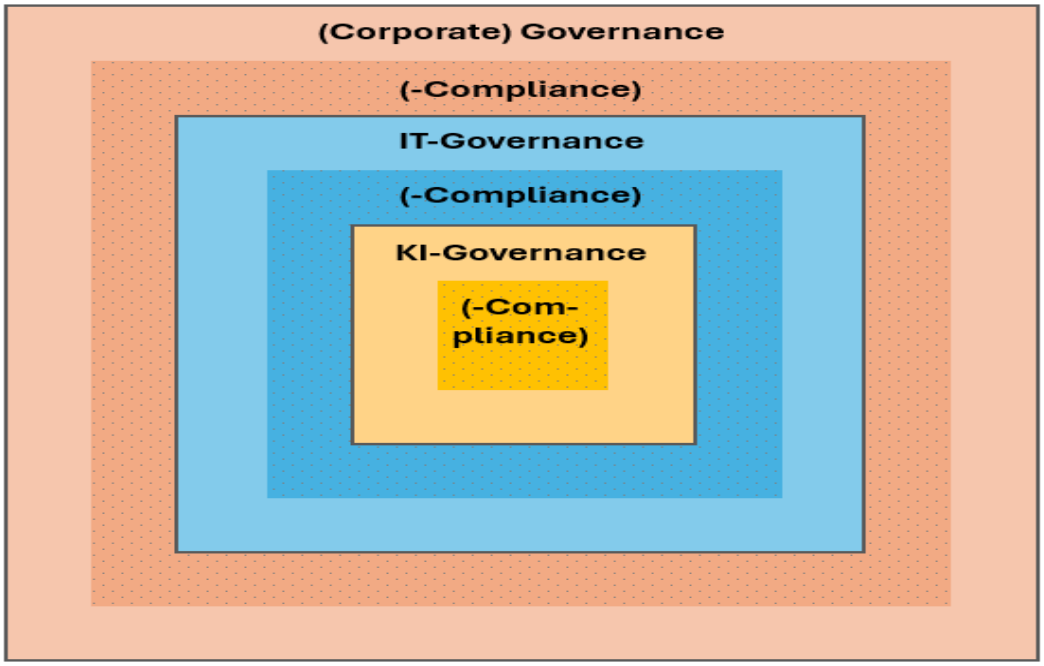

Abbildung 3: Compliance-Anteile der (IT- / KI-) Governance

Die Abgrenzung von *(IT-) Governance* und *(IT-) Management* fällt mangels Legaldefinition ebenfalls nicht leicht:
Die DIN ISO 37000 versucht in Normabschnitt 4.2.3 „Governance und Management“ die beiden Begriffe voneinander abzugrenzen – allerdings sehr unjuristisch und nicht eindeutig: Demnach soll sich „Governance“ mit dem Setzen der Rahmenbedingungen und „Management“ mit der Entscheidungsfindung und praktischen Umsetzung auseinandersetzen.[46]
Das erscheint nicht korrekt, da beide Begriffe strategische und operative Elemente enthalten. Sinnvoll erscheint für die Unterscheidung der Begriffe „Governance“ und „Management“ vielmehr die Klärung, ob das monoistische („Board“) oder dualistische („Leitung und Aufsichtsorgan“) Modell von Organisationen oder Unternehmen untersucht wird. Bei letzterem könnte die Abgrenzung in den zu beschreibenden Rollen, Aufgaben, Rechten und Pflichten der diversen Gremien gesehen werden: Bei „Governance“ stehen Gesellschafter, Leitung, Aufsichtsgremium und Stakeholder im Fokus, bei „Management“ nur die Leitung.[47]

Die ISO 38500 nimmt hingegen keine strikten Abgrenzungsversuche vor. Sie führt „Governance“ und „Management“ über Grundsätze, Modelle und Frameworks zusammen[48] und hebt hervor, dass im Kontext der IT die Bereiche „Governance“ und „Management“ nicht separiert betrachtet werden sollten.[49] Lediglich die Verantwortlichkeiten sind klar zu trennen.[50]

Zwischenfazit: Es besteht noch Diskussionsbedarf und Bedarf an Awareness und Kompetenz bezüglich diverser neuer Begrifflichkeiten und deren Inhalt. Dabei ist stets auf eine Herleitung aus Legaldefinitionen, der Interpretation von unbestimmten Rechtsbegriffen durch die Rechtsprechung und aus anerkannten Standards zu achten.

Es ist davon auszugehen, dass weder bei den Babyboomern, Gen Z oder Gen Alpha, noch bei IT-Fachexperten oder sonstigen Führungskräften diese Begrifflichkeiten in ihrer korrekten Bedeutung bekannt sind.
Ohne gemeinsames Verständnis der Begrifflichkeiten lässt sich aber nicht kommunizieren, zusammenarbeiten oder „Wirksamkeit“ erzielen.

DIN ISO 37000, ISO / IEC 38500 und ISO / IEC 42001 definieren jeweils in Abschnitt 3 relevante Governance-Begriffe.[51]

---

[46] Vgl. *Fröhlich & Glasner (Hrsg.),* IT-Governance, Gabler, 2007, S.18.

[47] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S. 78.

[48] Vgl. ISO/IEC 38500:2024, Kap. 4.2, S.4-5.

[49] Vgl. ISO/IEC 38500:2024, Kap. 6.4, S.16

[50] Vgl. ISO/IEC 38500:2024, Kap. 6.1, S.14 und *Klotz, Goeken, Fröhlich*, IT-Governance - Ordnungsrahmen und Handlungsfelder für eine erfolgreiche Steuerung der Unternehmens-IT, dpunkt.verlag, Heidelberg, 2023, S.36.

[51] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.45.

Welche Hilfsmittel unterstützen beim Thema „Verständnis relevanter Begrifflichkeiten" in der Praxis?

Ein digitales Wiki im Intranet der Organisation, ein Glossar, in Prozesse integrierte einfach verständliche Erklärungen („*IT- (KI-) Governance-Compliance for Beginners*") oder Erklärfilme (u.U. auch erstellt mit KI-Unterstützung) sind bei der Kommunikation der Grundbegriffe hilfreich.

Ergänzend sind angemessene Schulungen durchzuführen.

Idealerweise werden diese Begriffe in der Gruppe der Adressaten für IT-(KI-) Governance diskutiert, sofern nicht Konsens besteht.

Fragen für (interne) Audits:

Sind die relevanten Definitionen für IT- (KI-) Governance, Risikomanagement, Compliance, Transformation, Digitalisierung, Nachhaltigkeit (ESG) etc. bei den relevanten Adressaten (Organe, Lines of Defense-Funktionen, Führungskräften etc.) bekannt, verstanden und werden sie einheitlich verwendet?

Sind angemessene Kenntnisse der gewissenhaften Führung und Überwachung von Organisationen (Governance) bei den relevanten Adressaten (Organe, Lines of Defense-Funktionen, Führungskräften etc.) vorhanden?

Ist die Bedeutung von Technikklauseln („Anerkannte Regeln der Technik"/„Stand der Technik") bekannt?

4. Analysen, Organisation, Ziele, Anwendungsbereich und Komponenten des IT- (KI-) Governance-Compliance-Managementsystems

4.1 Analysen von Organisation, Umfeld, Stakeholder und Risiken

Die *Organisationsanalyse* ist die Darstellung der Organisation inklusive der wirtschaftlichen und finanziellen Situation.

Es empfiehlt sich eine Kurzdarstellung des Geschäftsmodells („Business-Plan light" bzw. „Ratingbericht") und aller Unternehmensbereiche sowie Durchleuchtung dieser Bereiche.[52]

[52] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, S.66.

Bei der Umfeldanalyse werden z.B. mittels der „PESTEL“-Methode die vielfachen Umfeldentwicklungen für die zur betrachtenden Organisation auch in Bezug auf das relevante Thema (hier: IT- (KI-) Governance) analysiert.

Bestandteil der Organisations- und *Umfeldanalyse* ist ein *Basis-Risiko-Check (z.B. eine SWOT-Analyse)*, um Stärken, aber auch Schwachstellen sowie Risiken und brachliegende Chancen im Unternehmen und Gefahren und Chancen aus Umfeldentwicklungen schnell zu erkennen.

Die Organisation muss zudem auch ihre „interested parties“ kennen und deren Anforderungen an die IT und KI bestimmen. Zu den „interessierten Parteien“ (*„Interested Parties“* oder „Stakeholder“) zählen Geschäftsleitung, Gesellschafter, Kunden, Lieferanten, Abschlussprüfer, das Aufsichtsgremium, Behörden, Mitarbeiter u. v. m..[53]

Über eine *Wesentlichkeitsanalyse* bestimmen die Organe unter Einbindung relevanter Stakeholder wesentliche Nachhaltigkeitsthemen, über die gegebenenfalls zu berichten ist.

Zur zusammenfassenden Ermittlung von Stärken, Schwächen, Gefahren und Chancen stehen den Verantwortlichen Methoden, wie die SWOT- oder Szenario-Risikoanalyse, zur Verfügung.

Ein Soll-Ist-Abgleich zeigt Abweichungen von (zwingenden) Zielgrößen (Compliance), wie Gesetzen, Richtlinien, Standards etc. auf.

In erster Linie sind aus den Analysen korrekte Schlussfolgerungen zu ziehen, wie das IT- (KI-) Governance-Compliance-Managementsystem *risikobasiert angemessen* und *wirksam* auszugestalten ist. Je größer die Compliance-Risiko-Exposition der Organisation ist, desto höher sind die Anforderungen. Das Ziel der Analysen ist eine zielgruppengerechte Aufbereitung der Daten, idealerweise als Teil des Geschäfts- und Nachhaltigkeitsberichts.[54]

Die Anfertigung und Auswertung dieser diversen Analysen stellt eine haftungsbewehrte Pflicht der Organe (Geschäftsführer / Vorstand) dar, vgl. die Rechtsprechung des *BGH*[55]: Pflicht des Geschäftsführers, jederzeit die wirtschaftliche und finanzielle Lage der Organisation zu kennen und § 1 StaRUG: Pflicht zur Risiko- und Krisenfrüherkennung.

Ebenso besteht eine Pflicht zur ordnungsgemäßen Planung (§§ 252, 289, 315 HGB, 90 AktG etc.).[56]

---

[53] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, S.67.

[54] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S. 55 f.

[55] BGH, Urteil vom 23.07.2024 (Az. II ZR 206/22 – „Geschäftsführerhaftung“).

[56] Vgl. Bundesverband Deutscher Unternehmensberatungen: Grundsätze ordnungsgemäßer Planung (GoP), Version 3.0, 2022, abrufbar unter https://www.bdu.de/verband/qualitaet-im-consulting/ (zuletzt abgerufen am 30.11.2025).

4.2 Der aus den Analysen abgeleitete organisationsweite Rahmen, Ziele und Strategie des Managementsystems

4.2.1 Organisatorischer Rahmen

Der organisatorische Rahmen einer rechtssicheren Organisation enthält folgende 13 Komponenten:[57]

1) (Eine den rechtlichen Anforderungen genügende) gesellschaftsrechtlich angemessene Unternehmensstruktur (gegebenenfalls auch Holding-Konzernstruktur)
2) Rechtssichere Organigramme (Konzern-, Unternehmens-, Bereichsorganigramme)
3) Schnittstellenmanagement (Kommunikation und Kooperation der notwendigen Schnittstellen zwischen den einzelnen (Prozess-)Themenbereichen und gegebenenfalls auch zu „Sonstigen“ („interested parties“)
4) Rechtssichere Stellen- und Arbeitsplatzbeschreibungen
5) Rechtssicheres Interaktionsmanagement (rechtssichere Regelung, wie die Organe, Gesellschaften (falls Konzernstruktur gegeben), Abteilungen etc. interagieren, u. a. in Hinblick auf: Aufgaben- und Verantwortungsbereiche, Vertretung, Stellvertretung, Aufsicht, Weisung, Kommunikation etc.)
6) Rechtssichere Delegation (durch Auswahl geeigneter Delegationsempfänger, Instruktion und Überwachung – auch Externer)
7) Rechtssichere Prozessbeschreibungen (Verfahrensanweisungen)
8) Wirksame Aufsichts- bzw. Kontrollmechanismen (auch in Hinblick auf Management-Anforderungen) – auch, falls Leistungen von Externen erbracht werden (z. B. im Rahmen von Outsourcing, z. B. bei Auslagerungen, Belieferung oder Delegation) – vgl. „Lines of Defense“
9) Implementiertes und wirksames Informations- und Kommunikationsmanagement
10) Implementiertes und wirksames Dokumentationsmanagement
11) Unterstützendes (Integriertes) Managementsystem
12) Angemessene (Personal-) Ressourcen (in Quantität und Qualität / Kompetenzen)
13) Asset-Management[58]

Die von IT- Governance betroffenen und sonstigen Bereiche einer Organisation sollten einheitlich strukturiert und geführt werden.

---

[57] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, S. 75.

[58] Vgl. DIN ISO 55001 Asset-Managementsystem.

Die nachfolgende Abbildung zeigt mit dem *ESGRC-Haus, das einem funktionalem Organigramm nachempfunden ist,* die Anordnung üblicher Standards im Governance-Rahmen:

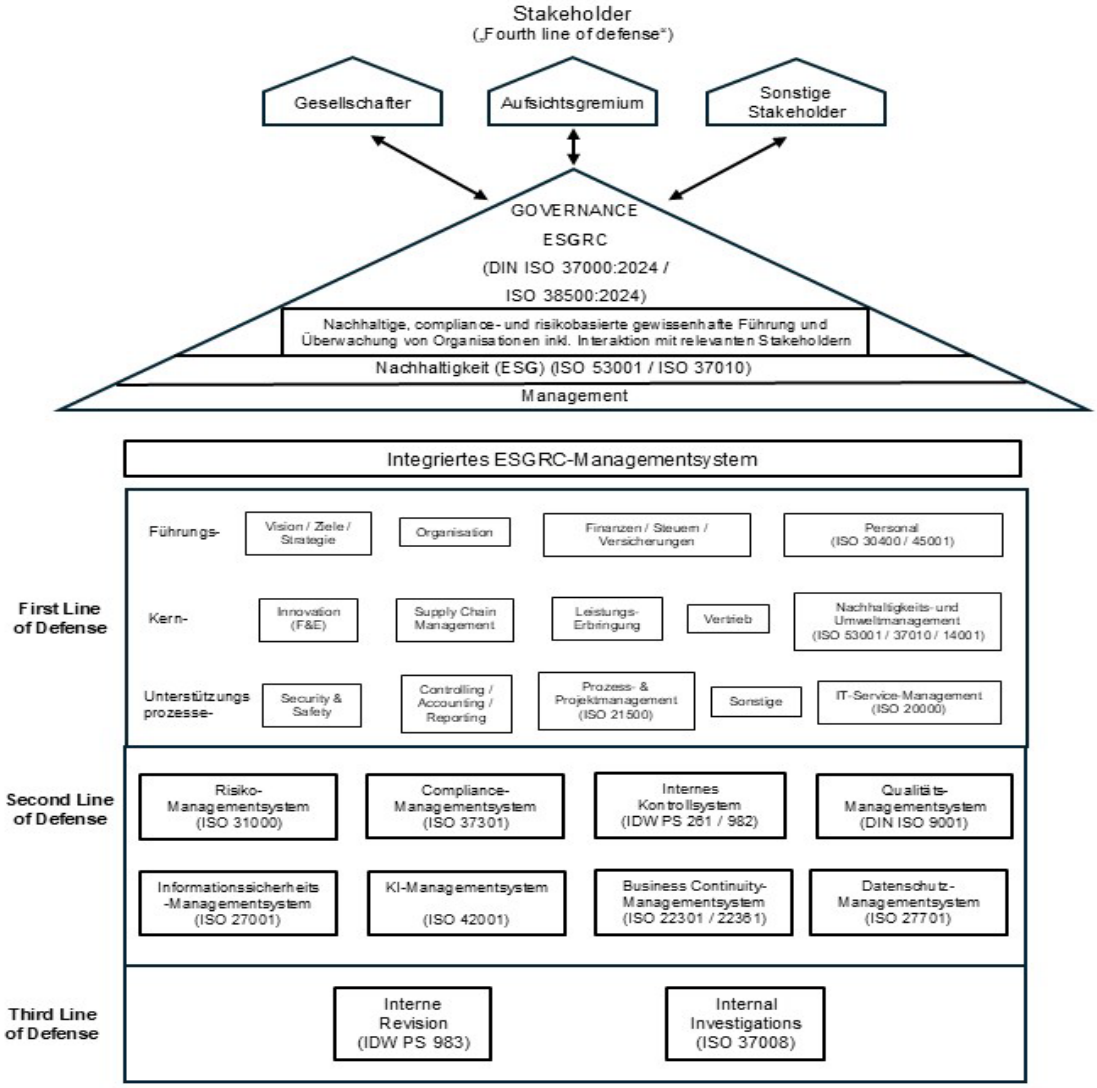

Abbildung 4: Das „ESGRC-Haus"[59]

Dabei sind alle Bereiche über ihre Prozessabläufe vernetzt:

Beispiel: Bereich „IT":

Der *Bereich „IT"* wird u.U. über den Chief Information Officer (CIO) in der Leitung und u.U. über einen Prüfungsausschuss im Aufsichtsrat in der (IT-) Governance vertreten, strategisch geplant, gesteuert und beaufsichtigt sein.

Der Bereich Strategie erarbeitet mit ihm gemeinsam eine von der organisationsweiten Strategie abgeleiteten IT-, Informationssicherheits- und KI-Strategie etc..

[59] In Anlehnung an *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S. 19.

Der Bereich Organisation kümmert sich um einschlägige Organigramme, Stellen-, Arbeitsplatzbeschreibungen, Delegationen, Sonderbeauftrage, Prozessabläufe etc.

Der Bereich Finanzen freut sich über funktionierende Finanz-Planungssysteme und -Auswertungen in Echtzeit und stellt über Budgets die finanziellen Ressourcen für den Bereich IT zur Verfügung.

Und so geht's weiter. In einem prozessbasierten ERP- oder Workflow-Managementsystem können die gegenseitigen Verbindungen sichtbar werden.

In der „first line of defense" findet die ordnungsgemäße operative Arbeit statt. Somit dienen die Arbeiten in der „first line" unmittelbar der Wertschöpfung einer Organisation.

In der „second line" befinden sich die steuernden und überwachenden Stabsstellen, die der Leitungsebene unterstellt sind. Sie erarbeiten entlang der strategischen Vorgaben, Gesetze, externen Anforderungen und Rechtsprechung organisationsinterne Regelwerke, die von der first line in ihrer Arbeit zu berücksichtigen sind. Sie prüft und steuert den Umgang von Abweichungen mit Hilfe von Risikoanalysen. Es erfolgt eine Berichterstattung an die Leitungsebene.

Die „third line" prüft die ersten beiden Verteidigungslinien hinsichtlich der Angemessenheit und Wirksamkeit.

Wenn die first line ertüchtigt werden würde, das Wichtige und Richtige richtig zu tun, könnten in den übrigen lines of defense viele Ressourcen eingespart werden.

Die Verteilung der Aufgaben der jeweiligen Verteidigungslinien ist in der nachfolgenden Abbildung beispielhaft an der Eingliederung der Aufgaben des Business Continuity Managements dargestellt:

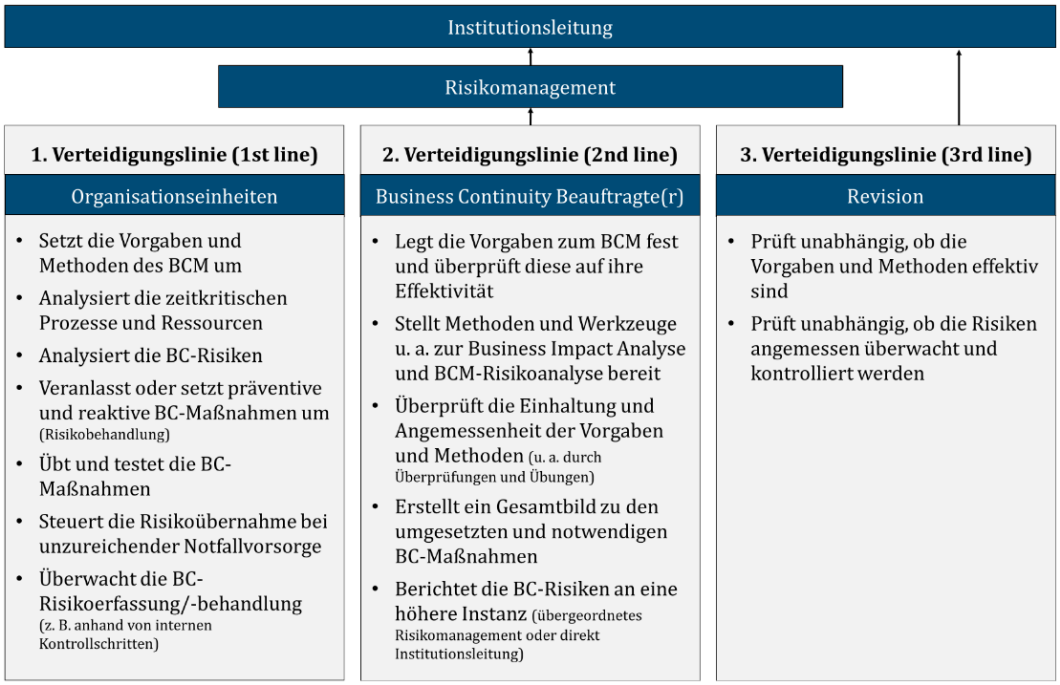

Abbildung 5: Das „three lines of defense"-Modell in Verbindung mit BCMS[60]

Das in Abbildung 5 dargestellte Aufgabenspektrum lässt sich auf andere Managementsysteme übertragen. Organisationseinheiten müssen demzufolge die Vorgaben aus dem IT- (KI-) Governance-Managementsystem verstehen und umsetzen sowie entsprechende Risiken mit ihrer fachspezifischen Expertise analysieren und behandeln.

Die Vorgaben für die Organisation (und somit zur Umsetzung in den Organisationseinheiten) werden von den Managementsystem-Beauftragten entlang der angewandten Standards abgeleitet und festgelegt.

Die nachfolgende Abbildung zeigt die Beziehung zwischen den relevanten Normen.

[60] Vgl. *BSI*, 2023, S.77, online abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf (zuletzt abgerufen am 30.11.2025).

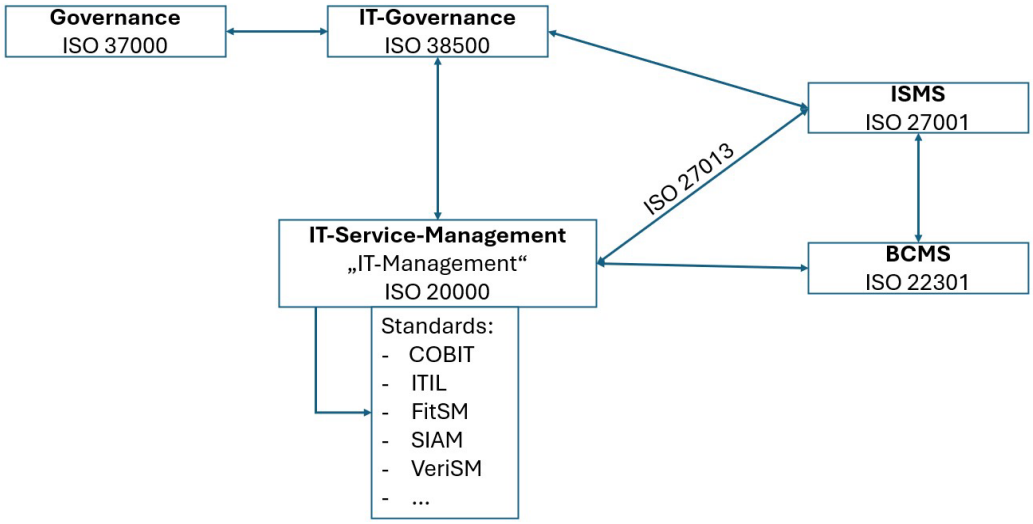

Abbildung 6: Zusammenhänge relevanter Normen

Die umschließenden Governance-Normen, also die ISO 37000 und ISO 38500 stehen in Zusammenhang mit verschiedenen Managementsystemen, die für eine Organisation relevant sind: Governance-Management, Compliance-Management, Informationssicherheit, Business Continuity etc. beeinflussen die operative IT-Ebene (IT-Service-Management nach ISO 20000 oder einem anderen Standard) in einer Organisation maßgeblich.

4.2.2 IT-Ziele und -Strategien

Angemessene Zielsetzung, Strategieentwicklung und Planung – auch im Bereich IT – gehören zu den wesentlichen Pflichten eines Geschäftsführers, Vorstandes etc. (§§ 43 GmbHG, 93 und 116 AktG).[61]

Nur, wenn *organisationsweit* Vision, Ziele und Strategie aus den Analysen abgeleitet werden und als Vorgaben für Vision, Ziele und Strategie des IT-(KI-) Governance-Managementsystems dienen, haben alle Anstrengungen des Managements und der Beschäftigten die gleiche Richtung. Dadurch wird der „rote Faden“ bei den Zielen und Strategien ersichtlich und alle können „an einem Strang ziehen“. Zielkonflikte werden so vermieden.

Welche Hilfsmittel unterstützen beim Thema „*aus Analysen abgeleiteter organisationsweiter Rahmen, Ziele und Strategie des Managementsystems*“ in der Praxis?

Für die IT- sowie für die KI-Verwendung in der Organisation sind Vision/Mission/Ziele/Strategie fachspezifisch im Kontext der Gesamtorganisation zu beschreiben. Die Ziele sind „SMART“ zu formulieren.

[61] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.57.

Unterstützend hierzu sind die Geschäftsprozesse der Organisation zu analysieren. Welche Anforderungen an die IT / KI stellt das business?[62]

Für die Setzung der IT- / KI-Governance-Compliance-Ziele und -Strategien sollte ein formaler Beschluss gefasst werden. Dies gilt auch für das Aufsetzen eines Projektes, das mit der Konzeption eines IT- / KI-Governance-Compliance-Managementsystems einhergeht. Die Beschlüsse sind von der Leitung zu verabschieden.

4.3 Der Anwendungsbereich des IT- (KI-) Governance-Managementsystems

Den Anwendungsbereich (Scope) des IT- (KI-) Governance-Managementsystems festzulegen, wird von Standards gefordert und bezieht sich auf den Wirkungsbereich *des Managementsystems*. Jedoch besteht aus der Rechtsprechung eine verbindliche Pflicht, in *allen* Unternehmensbereichen für IT- (KI-) Compliance zu sorgen.[63]

Beispiel: Der Scope des ISMS könnte auf Rechenzentrum und eine Tochtergesellschaft beschränkt werden. Danach würde sich auch u.U. eine Zertifizierung ausrichten. Das Zertifikat muss den gewählten Scope des Systems klar bezeichnen, um nicht Scheinsicherheit zu suggerieren.

Die Pflicht, für Informationssicherheit zu sorgen, erstreckt sich aber auf die gesamte Organisation inklusive ausgelagerter Leistungen.

4.4 Elemente des IT- (KI-) Governance-Compliance-Managementsystems

Die wesentlichen Elemente für ein Compliance-Managementsystem finden sich in der ISO 37301.[64] Das Governance-Managementsystem entlang der DIN ISO 37000 basiert auf elf Grundsätzen, die als zentrale Elemente anzusehen sind. Das IT-Governance-Managementsystem im Sinne der ISO / IEC 38500 greift ebenjene Elemente auf und konkretisiert diese hinsichtlich informationstechnologischer Schwerpunkte (siehe Tabelle 2).

DIN ISO 37000:2024	**ISO 38500:2024**	**Grundsatz / Element**
6.1	5.2	Zweck
6.2	5.3	Wertschöpfung
6.3	5.4	Strategie

[62] Siehe hierzu auch Kapitel 4.1.

[63] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S. 58.

[64] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kapitel 4.4.

6.4	5.5	Aufsicht
6.5	5.6	Rechenschaftspflicht
6.6	5.7	Einbindung der Stakeholder
6.7	5.8	Führung
6.8	5.9	Daten und Entscheidungen
6.9	5.10	Risiko-Governance
6.10	5.11	Gesellschaftliche Verantwortung
6.11	5.12	Langfristige Existenzfähigkeit und Leistung

Tabelle 1: Elemente des IT- (KI-) Governance-Compliance-Managementsystems

Das aktuelle IT-Governance-Managementmodell, wie es in der ISO / IEC 38500:2024 beschrieben ist, führt sechs wesentliche Elemente an, die sich im IT-Governance-Managementsystem wiederfinden.[65]

Welche Hilfsmittel unterstützen beim Thema „*Elemente des IT- (KI-) Governance-Compliance-Managementsystems*“ in der Praxis?

In einer „Elementenliste“ werden entsprechend der Anforderungen von Rechtsprechung und Standards die wesentlichen Elemente des Systems aufgeführt.

Eine „Managementsystem-Beschreibung“ stellt auf Basis eines Soll-Ist-Abgleichs den Reifegrad der diversen Elemente fest.

4.5 IT-Governance-Compliance-Anforderungen, Rechtsinformationsdienst und prozessbezogenes Rechtskataster

Um die rechtlichen Anforderungen als Teil des IT- (KI-) Governance-Compliance-Managementsystems zu identifizieren, zu bewerten und zu steuern, sollte ein prozessbezogenes Rechtskataster angelegt und gepflegt werden.

Abbildung 7 zeigt beispielhaft, wie mit dem Aufbau eines derartigen Rechtskatasters begonnen werden könnte:

[65] Vgl. ISO / IEC 38500:2024, Kap. 7.1, S.17.

Fachbereich (zuständig: Leitung des Bereichs)	Rechtsgebiet	Anwendbar?	Sehr hohe Relevanz?	Gesetz	Regularien (Gesetze/§§/ Richtlinien)	Anforderungen und Pflichten	Risiko bewertet?		Risiko gesteuert?	
							Ja	nein	Ja	nein
IT-Governance	Sorgfaltspflichten	☐		AktG	§ 93	**Unternehmerische Entscheidungen auf Grundlage angemessener Information zum Wohle der Gesellschaft:** Nach § 93 Aktiengesetz (AktG) sind Vorstandsmitglieder verpflichtet, unternehmerische Entscheidungen auf Grundlage angemessener Informationen und zum Wohl der Gesellschaft zu treffen, wobei sie stets die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden haben.	☐	☐	☐	☐
		☐		GmbhG	§ 43	**Haftung der Geschäftsführer:** Nach § 43 Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG) haften Geschäftsführer bei Pflichtverletzung gemeinschaftlich für Schäden. Besonders haftbar sind sie für verbotene Zahlungen aus dem Stammkapital und unerlaubten Erwerb eigener Anteile der Gesellschaft.	☐	☐	☐	☐
		☐		StaRUG	§ 1	**Krisenfrüherkennung:** Nach § 1 Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG) müssen Geschäftsleiter kontinuierlich mögliche Gefährdungen des Unternehmens überwachen. Bei Gefahr ergreifen sie Gegenmaßnahmen und berichten den Überwachungsorganen unverzüglich. Maßnahmen, die andere Organe betreffen, werden schnellstmöglich in deren Zuständigkeit überführt.	☐	☐	☐	☐
	Datenschutzrecht	☐		DSGVO	Art. 5	**Grundsätze der Verarbeitung:** Nach Artikel 5 Datenschutz-Grundverordnung (DSGVO) müssen personenbezogene Daten: - Rechtmäßig, nach Treu und Glauben und transparent verarbeitet werden. - Für festgelegte, eindeutige und legitime Zwecke erhoben und nur für diese Zwecke weiterverarbeitet werden. - Auf das notwendige Maß für den Verarbeitungszweck beschränkt sein. - Richtig und aktuell gehalten werden; unrichtige Daten müssen gelöscht oder berichtigt werden. - Nur so lange gespeichert werden, wie es für den Verarbeitungszweck erforderlich ist. - Sicher verarbeitet werden, um Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor Verlust, Zerstörung oder Schädigung zu gewährleisten.	☐	☐	☐	☐

Abbildung 7: Beispiel für die Struktur eines ersten Schrittes zu einem Rechtskataster für IT-Governance[66]

Idealerweise werden diese Regulierungs-Anforderungen in eine verständliche Sprache übersetzt und Aktivitäten zur Erfüllung der Anforderungen in Aufbau- und Ablauforganisation implementiert.[67]
An dieser Stelle wird das IT- (KI-) Governance-Managementsystem mit dem Compliance-Managementsystem (DIN ISO 37301) verknüpft. Die Integration von Compliance in Prozesse über moderne Tools ist inzwischen Stand der Technik.

Beispiel: Für die Ausgestaltung eines Informationssicherheits-Managementsystems, als Teil des IT- (KI-) Governance-Managementsystems, sind folgende rechtliche Anforderungen alleine schon aus dem NIS2-Richtlinien-Umsetzungsgesetz zu entnehmen:

Bestandteil	Zielsetzung	NIS2-Richtlinie
Management-system	Ein ISMS muss eine klare Systematik verfolgen und sich dynamisch an neue Anforderungen anpassen	Art. 21 Abs. 1
Governance und der „Tone from the top“	Die Führung des Systems muss von der Leitungsebene der Organisation ausgehen	Art. 20 Abs. 1
Asset Management	Identifikation, Einordnung und Schutz aller organisatorischen Assets (Prozesse, IT-Komponenten, Services etc.)	Art. 21 Abs. 2 j)

[66] Diese Art von *Rechtskataster-Basisschritt* weist noch einen geringen Reifegrad auf. Ideal wäre eine revisionssichere Integration sämtlicher relevanter IT- (KI-) Compliance-Anforderungen in die Tool-gestützten Prozesse. Dabei sollten eine Bewertung des Risikos, die jeweilige Anforderung nicht zu erfüllen, abgeleitete und überwachte Steuerungsmaßnahmen und Reportings für Wirksamkeit / Effektivität sorgen. Dies ist inzwischen „Stand der Technik“.

[67] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kapitel 4.5 und S.93.

Risikomanagement	Erstellung einer Risikosystematik und Identifikation, Beurteilung und Steuerung von Schwachstellen und Risiken	Art. 21 Abs. 2 a), e) und f)
Lieferketten-management	Bewertung von Lieferanten und Dienstleistern als mögliches Sicherheitsrisiko	Art. 21 Abs. 2 d)
Sicherheits-maßnahmen	Umsetzung technischer und organisatorischer Maßnahmen zum Schutz von Assets vor identifizierten Risiken	Art. 21 Abs. 2 g), h), i) und j)
Vorfalls-management	Maßnahmen zur Erkennung, Meldung und Bewältigung von (IT-/Informations-sicherheits-)Vorfällen	Art. 21 Abs. 2 b), c), j) und Art. 23
Business Continuity Management	Erstellung von Notfallplänen und Wiederherstellungsmaßnahmen zur Bewältigung von Sicherheitsvorfällen	Art. 21 Abs. 2 b), und c) und Art. 22

Tabelle 2: Rechtliche Anforderungen des NIS2-Richtlinien-Umsetzungsgesetzes an ein Informationssicherheits-Managementsystem[68]

Zudem ist sicherzustellen, dass neue oder geänderte Regulierung in Echtzeit erfasst und umgesetzt wird. Bei Rechtsinformationsdiensten verändert sich die Anbieterlandschaft aufgrund der Möglichkeiten der KI rasant.

Welche Hilfsmittel unterstützen beim Thema „*prozessbezogenes Rechtskataster*“ in der Praxis?

Es ist ein prozessbezogenes, risikobewertetes Rechtskataster anzulegen und stets aktuell zu halten (Rechtsinformationsdienst).

IT- und KI-Compliance ist mehr als NIS2 und KI-Verordnung: Spannungen zwischen Datenschutz, Urheberrecht, gewerblicher Rechtsschutz, Product-Compliance und KI-rechtlichen Anforderungen können die rechtliche Sicherheit einer Organisation beim Einsatz von KI-Technologien gefährden.[69] Die Erstellung einer Rechtsgebiete-Matrix erweist sich als hilfreich. Diese kann auch hinsichtlich einer Rechtsgebiete-Risikobewertung herangezogen werden.

Die DIN ISO 27001:2024, Anhang A, Maßnahme 5.31 verlangt die Erfüllung „*juristischer, gesetzlicher, regulatorischer und vertraglicher Anforderungen*“ und die Anlage eines Rechtskatasters.

Fragen für (interne) Audits:

Ist ein stets aktuelles prozessbezogenes Rechtskataster zur Erfüllung der IT- (KI-) Compliance-Anforderungen implementiert und wirksam?

[68] In Anlehnung an *Haider*, Umsetzung von NIS2 mit Zero Trust – Ein praxistauglicher Ansatz. In: Kälberer, D.R., Staffler, L. (eds) Regulierung und Innovation im Zeichen der Digitalisierung. Springer Gabler, 2025, S. 69.

[69] Vgl. *World Economic Forum*, Governance in the Age of Generative AI, 2024, S. 6-7, online abrufbar unter https://www3.weforum.org/docs/WEF_Governance_in_the_Age_of_Generative_AI_2024.pdf (zuletzt abgerufen am 30.11.2025).

Werden auch relevante Standards für Governance, Risikomanagement, Compliance, Informationssicherheit etc. als Referenzgrößen herangezogen?

Wird das Erreichen der zwingenden und freiwillig gesetzten Ziele durch eine angemessene prozessorientierte Aufbau- und Ablauforganisation sichergestellt?

4.6 IT- (KI-) Governance-Compliance-*Risiko*management

Der IT- (KI-) Governance-Compliance-Risikomanagement-Prozess[70] dient der frühzeitigen Identifikation, Bewertung und Steuerung von Gefahren und Chancen, die die Zielerreichung einer Organisation beeinflussen könnten.
Eine Risiko-Analyse sucht systematisch nach Ursachen und Gefahren für Abweichungen.
Allein schon alle IT- (KI-) Compliance-Anforderungen stellen im nicht erfüllten Zustand Gefahren (Risiken) dar. Daneben existieren außerhalb der Compliance jede Menge weitere sonstige Risiken.

Alle Beschäftigten sollten ein Basiswissen im Risikomanagement haben. Auch ausgegliederte Leistungen müssen einbezogen werden. Für nicht steuerbare relevante Rest-Risiken ist ein Business Continuity-Managementsystem erforderlich.[71]

Insbesondere in regulierten Organisationen, die als kritische Infrastruktur im Sinne der BSI-Kritis-Verordnung gelten, unter die NIS2-Richtlinie oder unter den Digital Operational Resilience Act (DORA) fallen, gibt es besondere Anforderungen an das IT-Governance-Risikomanagement:

So heißt es in der NIS2-Richtlinie, die seit März 2025 in Kraft ist, in Artikel 21 Abs. 1[72] und nahezu gleichlautend in dem durch das NIS2-Umsetzungsgesetz ergänzten § 30 BSIG:

„Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und

---

[70] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301:2021 erfolgreich implementieren, integrieren, auditieren, zertifizieren, DIN Media, 2022, Kapitel 4.5.

[71] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.180.

[72] Am 05.12.2025 trat das NIS2-Umsetzungsgesetz in Kraft. Artikel 21 der NIS2-Richtlinie ergänzt über das NIS2-Umsetzungsgesetz den § 30 BSIG um den gleichen Regelungsinhalt.

Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen."

Hierbei werden Risiken für die Sicherheit der Netz- und Informationssysteme betreffender Organisationen, also grundsätzlich die IT einschließlich KI, mit der Gesamtrisikoexposition der Organisation in Verbindung gebracht. Dies erfordert einen ganzheitlichen Risikomanagement-Ansatz, der aus der Governance der Organisation erwächst.

Besondere Aktualität erfahren die Anforderungen an ein (IT- und KI-) Risiko- und Krisenfrüherkennungs-System im Lichte neuester Regulierung (z.B. §§ 1 StaRUG, 91 Abs. 1 und 3 AktG etc.), Rechtsprechung (BGH, OLG Nürnberg, OLG Frankfurt etc.) und Standards (IDW S 16 und PS 340, DIIR Nr. 2 etc.).[73]

Welche Hilfsmittel unterstützen beim Thema „IT- (KI-) Governance-Compliance-Risikomanagement" in der Praxis?

Idealerweise besteht bereits ein angemessenes Risiko-Managementsystem.
Die Prozesse, Methoden und Tools sollten dokumentiert, bekannt und im Kontext des IT- (KI-) Governance-Managementsystems wirksam sein.

Fragen für (interne) Audits:

Ist das IT- (KI-) Risikomanagement Teil des Integrierten Risiko-Früherkennungs- und Risiko-Managementsystems?

Sind die Steuerungsprozesse der Unternehmensleitung risikobasiert ausgerichtet und in die strategische Gesamtführung integriert?

Sind Risiken im Bereich der Operational Technology (OT) identifiziert und in das organisationsweite Risiko-Managementsystem integriert?

Werden Risiken im Zusammenhang mit dem Einsatz von Künstlicher Intelligenz systematisch – nicht nur nach Maßgabe der KI-Verordnung – bewertet und durch Governance-Maßnahmen gesteuert?

[73] Vgl. *Scherer / Seehaus*, Pflicht zu Governance mit Risikofrüherkennung, Resilienz und Transformation als Kardinalpflicht von Organen und Führungskräften, in: ZInsO (Zeitschrift für das gesamte Insolvenz- und Sanierungsrecht), 28. Jahrgang, 31/2025, 31.07.2025, S. 1515-1538, zum kostenlosen download unter: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf, sowie *Scherer, Seehaus*, Managerhaftung, D&O-Versicherung und Risikofrüherkennung im Lichte aktueller Rechtsprechung, 1 / 2026, zum kostenlosen Download auf Risknet.de.

5 Führung und Verpflichtung

5.1 „Tone from the Top“ im integrierten (IT- / KI-) Governance-Compliance-Managementsystem[74]

„Führung“, „Leadership“ oder der sogenannte *Tone from the Top,* also die Vorbildfunktion von Geschäftsleitung, Aufsichtsorgan, Gesellschafter sowie Führungskräften in Bezug auf das (Integrierte) IT- (KI-) Governance-Compliance-Managementsystem sind die Basis für die *Wirksamkeit* (das „Gelebtwerden“) in allen Bereichen und Prozessen des Unternehmens.

Auch die IT- (KI-) Governance- „Kultur“ sowie die Wahrnehmung von Verantwortung für das Governance-Managementsystem durch alle Beschäftigten sind elementar wichtig.[75]

5.2 Politik des (IT- / KI-) Governance-Compliance-Managementsystems[76]

Die grundsätzliche Ausrichtung („Politik“) des entsprechenden Managementsystems („Leuchtturm“, „best in class“, „gemäß Stand der Technik“, „risikoavers“, „risikoaffin“, …) muss ebenfalls von der Leitung beschlossen werden, um den Beschäftigten eine Orientierung zu ermöglichen.

5.3 Rollen und Verantwortlichkeiten

Im Zuge des anhaltenden Trends der zunehmenden Digitalisierung entstehen viele neue Rollen, die Organisationen zu berücksichtigen haben. Insbesondere in den Bereich der IT gliedert sich zunehmend das KI-Management ein. Die Übergänge sind fließend und somit eng mit der IT-Governance verwoben.
Neben den „klassischen“ Rollen, wie dem Chief Information Officer (CIO), Chief Information Security Officer (CISO), Business Continuity Officer (BCO), Chief Risk Officer (CRO), IT-Administrator, IT-Architekt, dem Programmierer usw., entwickeln sich derzeit neue Rollen bzw. Berufsbilder.
Darunter zählen zum Beispiel KI-Architekten, Chief AI Officer (CAIO), KI Risikomanager, Prompt Engineer, KI-Ethikspezialisten und viele weitere, wie in Abbildung 8 zu sehen ist:

---

[74] Vgl. Harmonized Structure Abschnitt 5.1

[75] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.119.

[76] Vgl. Harmonized Structure Abschnitt 5.2

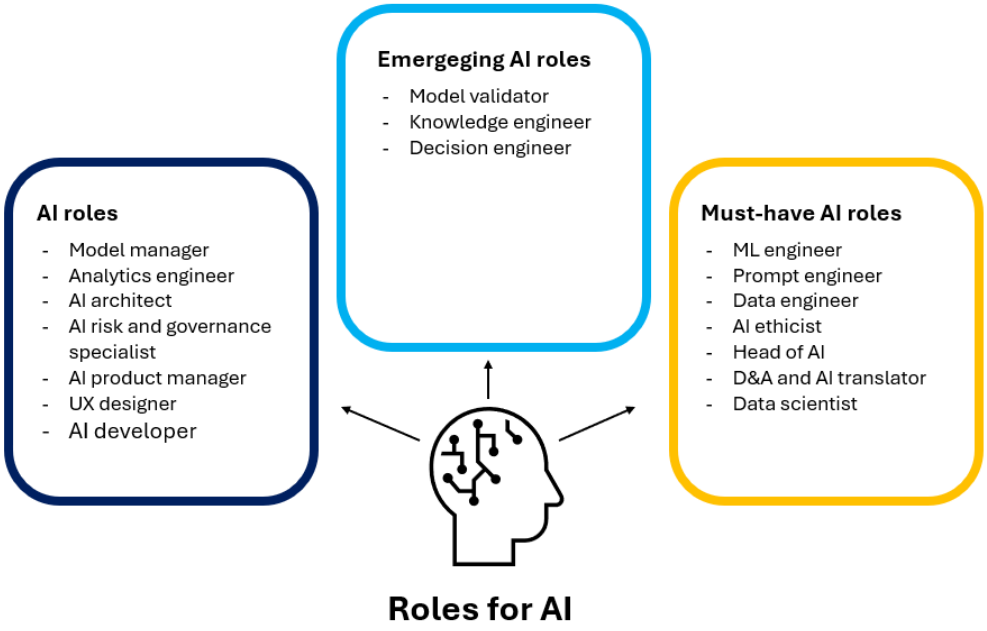

Abbildung 8: Neue Rollen mit KI-Bezug[77]

Die neu entstehenden Rollen, die sich derzeit erst etablieren, sind in der Organisation zunächst zu definieren. Dabei ist zu beachten, dass die Definition neuer Rollen bisherige Annahmen durchaus konterkarieren können. Als Beispiel hierfür dient der Decision Engineer, bei dem es insbesondere um die Unterstützung der *datenbasierten Entscheidungsfindung*[78] geht. Während IBM als Computerpionier und führender IT-Konzern 1979 noch klarstellte, dass Computer niemals die Verantwortung für Managemententscheidungen übernehmen dürfen, so wird die Thematik der computergestützten Entscheidungsfindung entlang der neuen technologischen Errungenschaften neu diskutiert.[79]

Welche Hilfsmittel unterstützen beim Thema* „Rollen im IT- (KI-) Governance-Compliance-Managementsystem“ *in der Praxis?

Zunächst ist eine fundierte Stellenbedarfsanalyse für die IT- und KI-Governance-Compliance erforderlich, um den quantitativen und qualitativen Personalbedarf systematisch zu ermitteln. Dies ist erforderlich für die Personalstellenplanung.

---

[77] Eigendarstellung in Anlehnung an *Gartner*, 2025, online abrufbar unter: https://www.gartner.com/en/newsroom/press-releases/2024-05-14-artificial-intelligence-is-creating-new-roles-and-skills-in-data-and-analytics (zuletzt abgerufen am 30.11.2025).

[78] Vgl. *Scherer*, Digital Decision Management, 2020, online abrufbar unter https://www.scherer-grc.net/files/fil/digital-decision-management.pdf (zuletzt abgerufen am 21.12.2025) und *Rieger, Scherer*, Der digitale Zwilling im Gesundheitswesen, JMG, 2021, S. 12f., online abrufbar unter: https://www.govsol.de/files/fil/jmg-2-21-art-rieger-scherer-korr.pdf (zuletzt abgerufen am 21.12.2025).

[79] Vgl. *IBM*, AI decision-making: Where do businesses draw the line?, 2025, online abrufbar unter https://www.ibm.com/think/insights/ai-decision-making-where-do-businesses-draw-the-line (zuletzt abgerufen am 21.12.2025).

Auf Basis dieser Analyse müssen anschließend präzise Stellenbeschreibungen entwickelt werden, die die spezifischen Aufgaben, Verantwortlichkeiten und erforderlichen Kompetenzen der neu zu schaffenden Rollen klar definieren.

Schließlich ist ein gezieltes Recruiting-Konzept zu etablieren, das durch passgenaue Aus- und Weiterbildungsmaßnahmen die erforderlichen Qualifikationen nachhaltig vermittelt.

Fragen für (interne) Audits:

Wird ein angemessener „Tone from the top" - auch - in Bezug auf Governance auf Führungsebene, Abteilungsebene und Vorgesetztenebene gewährleistet?

Verfügt das Unternehmen über qualifizierte und engagierte Mitarbeitende, die durch eine positive Unternehmenskultur unterstützt werden?

6. Planung und Konzeption

In der Planung *des IT- (KI-) Governance-Managementsystems* geht es um die Darstellung von Zielen und den Wertbeitrag, die Definition des Soll-Zustandes, den Soll-Ist-Abgleich, die Bewertung von alternativen Strategien sowie die Entscheidung für und Projektierung von Maßnahmen zur Erreichung der Ziele *des Systems*.

Auch bei der Planung einer Digitalisierungskampagne sollte ein *IT- und Informationssicherheitskonzept* nach Stand der Technik umgesetzt werden: Mit zunehmendem Digitalisierungsgrad steigt die Verletzbarkeit der Organisation.[80]

Dabei gilt zu berücksichtigen: „*If you fail to plan, you are planning to fail!*"[81].

Bzgl. der Ziele des IT- (KI-) Governance-Managementsystems vgl. bereits oben 4.2: Sie sind nicht willkürlich zu bestimmen, sondern zum großen Teil aufgrund von bestehenden Soll- oder Referenzgrößen bereits vorgegeben: Gesetze, die Rechtsprechung, Stand der Technik und z.T. auch Standards (ISO 37000:2024, ISO / IEC 38500:2024, DIN ISO 27001:2024, 22301:2020, ISO 42001:2023 etc.) etc. geben vor, was zwingend zu erreichen ist.

Dazu können dann noch weitere, von der Geschäftsleitung (fakultativ) beschlossene Ziele hinzutreten.

---

[80] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S. 20.

[81] Zitat von Benjamin Franklin.

Die Ziele sollten dabei „SMART“ ausgestaltet und dokumentiert sein. Dieses Akronym setzt sich aus folgenden Wörtern zusammen:

S – Specific, M – Measurable, A – Achievable, R – Relevant, T – Time-bound.

Ziele sollten spezifisch („specific“) formuliert sein – es sollte genau ersichtlich sein, worum es geht. Sie sollten auch messbar („measurable“) sein, sodass jederzeit ausgesagt werden kann, ob und inwieweit das Ziel erreicht wird. Zudem müssen Ziele grundsätzlich erreichbar („achievable“) sein. Ziele sollten für die Organisation ebenso relevant sein. Und letztlich sollten Ziele terminiert („time-bound“) sein, das Zeitfenster bis zur Erreichung ist also genau zu definieren.[82]

Für die Einplanung der Informationssicherheitsanforderungen aus der ISO 27001, Anhang A, ist ein *Statement of Applicability* zu erstellen. Hierbei werden die 93 Maßnahmen aus dem Anhang A auf ihre Anwendbarkeit und Relevanz in der Organisation geprüft. Dies stellt ein wesentlicher Aspekt bei der Konzeption des IT- (KI-) Governance-Managementsystems dar.

Welche Hilfsmittel unterstützen beim Thema „*Planung und Konzeption des IT- (KI-) Governance-Compliance-Managementsystems*“ in der Praxis?

Es sollte ein Ziele- und Kennzahlensystem etabliert werden, das strategische Vorgaben in messbare KPIs übersetzt und damit die Erfolgskontrolle ermöglicht.

Maßnahmen können mithilfe einer Aufgabenverwaltung – von einfachen Excel-Listen bis zu modernen Workflow-Tools – strukturiert geplant, zugewiesen und nachverfolgt werden.

Fragen für (interne) Audits:

Sind Ziele und Strategie des IT- (KI-) Governance-Compliance-Managementsystems aus Organisations-, Umfeld-, Interested Parties-, Wesentlichkeits-, SWOT-, (Compliance-) Risiko-Analyse aktuell abgeleitet, dokumentiert und mit „smarten“ Zielen hinterlegt?

7. Ressourcen, Awareness, Kommunikation und Dokumentation

Die Geschäftsleitung muss die Ressourcen, die für ein angemessenes, wirksames IT- (KI-) Governance-Managementsystem erforderlich sind, zur Verfügung stellen.

[82] Vgl. *Reynvaan, Conrad Hans Hendrik: Wie geht Industrie?: Erfahrungswissen eines Managers für Absolventen der MINT-Fächer*, Berlin, Heidelberg 2022, S.36-37.

Die Fragen, wo im Arbeitsprozess zwischen Robotern, Algorithmen und (teil-) automatisierten, intelligenten Prozessabläufen der Manager oder Mitarbeiter steht, was seine Aufgaben und Ziele – vor allem auch in Hinsicht auf Informationssicherheit und KI-Einsatz – sind und welche Kompetenzen er dafür braucht, sind zu beantworten. Dabei ist sicherzustellen, dass die erforderlichen Ressourcen und Kompetenzen in erforderlicher Qualität und Quantität verfügbar sind.

Bzgl. des Systems muss eine angemessene Awareness existieren und alle relevanten Informationen müssen angemessen intern und nach außen kommuniziert werden.

Die allgemeinen Anforderungen an Dokumente und Aufzeichnungen müssen entsprechend der unternehmensweit geltenden Regelungen und verpflichtenden rechtlichen Anforderungen eingehalten werden. Alle wesentlichen Bestandteile des IT- (KI-) Governance-Managementsystems sind grundsätzlich rechtssicher zu dokumentieren und zu archivieren.

Dabei ist empfehlenswert, möglichst früh zu beschließen, in welchem IT-System (Intranet, Dokumenten-Managementsystem, Cloud etc.) welche Elemente des Managementsystems dokumentiert werden.[83]

Welche Hilfsmittel unterstützen beim Thema „*Ressourcen, Awareness und Kommunikation im IT- (KI-) Governance-Compliance-Managementsystem*“ in der Praxis?

Für das IT- (KI-) Governance-Managementsystem müssen zunächst die notwendigen Ressourcen (finanzielle Mittel, Räumlichkeiten, IT, Personal etc.) ermittelt werden. Es ist – ganz im Sinne des risikobasierten Ansatzes – auf die Verhältnismäßigkeit zu achten. Das heißt nicht, dass die günstigsten Handlungsoptionen stets auch die Wirtschaftlichsten sind.

Es empfiehlt sich für die Zuordnung der Kompetenzen eine Wissens- und Kompetenzmatrix zu erstellen. Hierzu können interne Wiki-Seiten angelegt, E-Learnings bereitgestellt und interne Newsletter verteilt werden.

Zudem ist die IT-gestützte Form der Steuerung des IT- (KI-) Governance-Managementsystems zu überlegen. Dazu dienen entsprechende digitale ESGRC-Tools, die bei der Ausgestaltung und Steuerung zweckdienlich sind. Eine Excel-basierte Steuerung empfiehlt sich nicht.
Für fachspezifische Tools sind entsprechende Pflichtenhefte zu erstellen.

Festgelegte Kommunikationsprozesse und Dokumentenmanagementsysteme unterstützen ebenso bei der Ausgestaltung des IT- (KI-) Governance-Managementsystems. Die wesentlichen Inhalte können in einem Kommunikations- bzw. Dokumentationshandbuch zusammengeführt werden.

[83] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301 – erfolgreich implementieren, integrieren, auditieren, zertifizieren, Beuth, 2022, Kapitel 7.1 und 7.2.

Fragen für (interne) Audits:

Gibt es ein unterstützendes System (z. B. Prozess- und ESGRC-Plattform), das die Umsetzung des IT- (KI-) Governance-Managementsystems unterstützt?

Sind für das IT- (KI-) Governance-Managementsystem ausreichende Kompetenzen und Ressourcen sichergestellt?

8. Betrieb – Operationalisierung der IT-Governance-Compliance und Prozessmanagement

Sämtliche Elemente des (IT- / KI-) Governance-Managementsystems müssen in die betrieblichen Abläufe (Prozesse) integriert werden. Gewissenhafte Geschäftsführer und Vorstände sind für die Wirksamkeit des IT- (KI-) Governance-Managementsystems verantwortlich. Wirksamkeit bedeutet Effektivität und „Gelebt werden".

Menschen handeln aufgrund der Funktionsweise des Gehirns oder mangels aktuellen Wissens oft unvernünftig oder sogar pflichtwidrig.[84] Hier können führende *„Human Workflow Prozesse"* unterstützen, das *„Richtige richtig"* zu tun. Jeder Prozessbeteiligte weiß dann im Idealfall, *was* er *wann, wie* und *wo* zu tun hat. Auch *ausgegliederte Prozesse* müssen in Hinblick auf Compliance effektiv sein. Dies ist ebenfalls zu überwachen. Beispielsweise ist dieses Vorgehen auch für die Nutzung generativer KI-Modelle in Organisationen relevant. Für kritische Informationen eignen sich öffentliche KI-Systeme wie ChatGPT oder Gemini nicht. Es gilt vor allem, KI-generierte Inhalte von Experten prüfen zu lassen. Zudem ist zu beachten, dass kritische Entscheidungen stets in menschlicher Verantwortung verbleiben.

Für das IT-Management, das in den Anwendungsbereich des IT- (KI-) Governance-Managementsystems fällt, stellt die ISO / IEC 20000-1:2018 gewisse Standard-Prozessthemenfelder vor, die von verschiedenen Best-Practice-Standards wie COBIT, ITIL oder FitSM aufgegriffen werden.[85] In ITIL werden in der aktuellen Version 4 insgesamt 34 Prozessthemenfelder beschrieben, die in Tabelle 4 dargestellt sind.

---

[84] Vgl. *Kahneman*, Thinking fast and slow, 2011, Einleitung, sowie *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.168 und *Rieger, Scherer*, Der digitale Zwilling im Gesundheitswesen, JMG, 2021, S. 83, online abrufbar unter https://www.govsol.de/files/fil/jmg-2-21-art-rieger-scherer-korr.pdf (zuletzt abgerufen am 21.12.2025).

[85] Vgl. *Pilorget*, Managing IT in einer digitalen Welt, Springer Vieweg, 2025, S.38 ff.

General Management	Service Management	Technical Management
• Strategy management process • Portfolio management process • Architecture management • Service financial management • Workforce and talent management • Continual improvement • Measurement and reporting • Risk management • Information security management • Knowledge management • Organizational change management • Project management • Relationship management • Supplier management	• Business analysis process • Service catalogue management process • Service design • Service level management • Availability management • Capacity and performance management • Service continuity management • Monitoring and event management • Service desk • Incident management • Service request management • Problem management • Release management • Change enablement • Service validation and testing • Service configuration management • IT asset management	• Deployment management process • Infrastructure and platform management process • Software development and management

Tabelle 3: 34 Prozessthemenfelder für das IT-Management nach ITIL v4

Beim IT-Service-Management geht es um die Verknüpfung der IT-Organisation mit den Governance-Strukturen einer Organisation. Dazu zählen zum Beispiel das Strategiemanagement, Risikomanagement, Informationssicherheitsmanagement, Wissensmanagement oder Projektmanagement. Somit wird systematisch sichergestellt, dass die relevanten IT-Governance-Anforderungen in der Organisation erkannt und in der operativen Ebene berücksichtigt werden.

Die Service Management-Praktiken beziehen sich auf die direkte Wertschöpfung der IT-Services einer Organisation. Sie sollen eine angemessene Planung, Bereitstellung und Verbesserung der IT-Services gewährleisten. So sind beispielsweise im Sinne des *Incident-Managements* Prozesse zu entwickeln, die sich auf den Umgang mit Störungen in der IT beziehen.

Die Praktiken des Technical Managements gehen tiefer auf die technische Ebene der IT-Infrastruktur ein und unterstützen ebenfalls die Bereitstellung technischer Services. An dieser Stelle geht es zum Beispiel um Prozesse für die sichere Softwareentwicklung.

Wie unterstützt das IT-Service-Management bei der Operationalisierung der (IT-/KI-)Governance?

Die ISO 38500 und die ISO 20000 werden vom gleichen Subkommitee der ISO entwickelt[86]. Insofern ergibt sich ohnehin eine gewisse fachliche Nähe. Die ISO 20000 bzw. ITIL[87] wird in großen Teilen in der „first line“ einer Organisation (Schwerpunkt IT-Abteilung) implementiert. Dabei ist sicherzustellen, dass die Anforderungen der Managementsysteme in die IT-Prozesse (siehe Abbildung 6) berücksichtigt werden. Die ISO 27013 stellt hierzu eine Verbindungsnorm dar.

Während ITIL 3 noch recht konkrete IT-Prozesse vorgestellt hat, beinhaltet ITIL 4 nun eher Prozessanforderungen (mit KPIs), die die Organisation im eigenen Prozessdesign berücksichtigen muss. Dies ermöglicht einen individuelleren Ansatz, bei der das IT-Business-Alignment besser optimiert werden kann. Ohne IT-Service-Management (ob mit ITIL, FitSM, ISO 20000 oder einem anderen best practice Ansatz) wird kein wirksame Managementsystemstruktur – dessen Anforderungen von der „second line“ abgeleitet sind – möglich sein. Je nach Größe und Umfang der IT-Abteilung variiert die Stärke der Beziehung zwischen ITSM und den Managementsystemen (wie z. B. Informationssicherheitsmanagementsystem, Business Continuity Managementsystem, KI-Managementsystem etc.). Allenfalls gibt stets eine kritische beidseitige Abhängigkeit.

Hervorzuheben ist die "information security management" Praktik aus ITIL 4. Diese Praktik stellt die konkrete Operationalisierung der ISMS-Anforderungen (second line to first line) dar. Ohne ISMS wird die Praktik „information security management“ nicht funktionieren. Um in Organisationen die Angemessenheit und Wirksamkeit eines ISMS beurteilen zu können, ist ein Blick in die IT-Service-Prozesse unabdingbar (information security "by design"). Das gilt auch für das BCMS (vgl. hierzu Praktik "Availability Management", "Service Continuity Management", "Incident Management", "Service Level Management") und weitere Managementsysteme.

Es ist darauf zu achten, dass Digitalisierung und Compliance im Integrierten IT- (KI-) Governance-Managementsystem konzeptionell und „ganzheitlich“ („aus einem Guss“) eingeführt werden. Das heißt, dass das Prozessmanagement der Organisation (General Management) mit dem IT-Service-Management und dem Technical Management verknüpft ist. Daraus resultiert eine „top down“-Sicht, die die Governance-Compliance-Anforderungen den Geschäftsprozessen, den IT-Services und den einzelnen IT-Komponenten zuordnet und diese Ebenen in Verbindung stellt.

---

[86] Vgl. ISO/IEC JTC 1/SC 40, https://committee.iso.org/home/jtc1sc40 (zuletzt abgerufen am 12.08.2025).

[87] *IT Infrastructure Library* – ein Sammlung von IT-Management best practices vom PeopleCert.

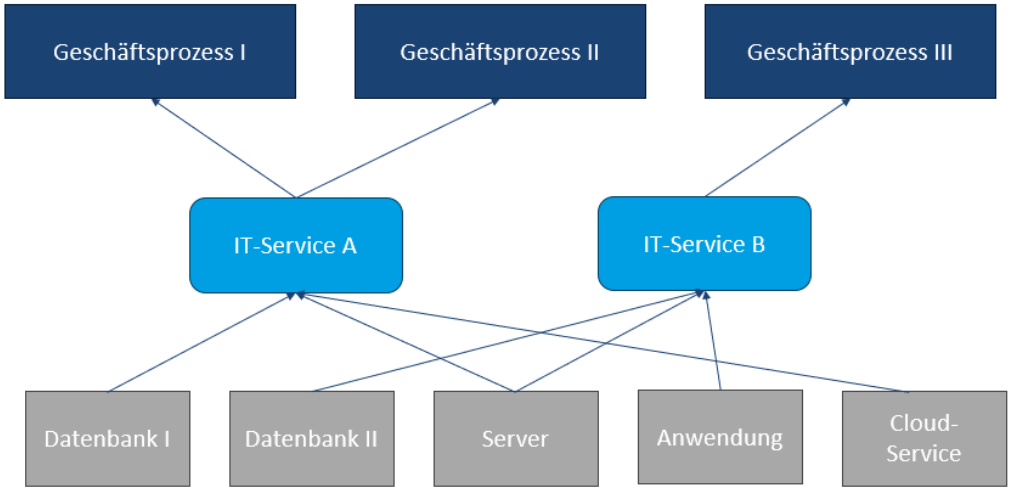

Abbildung 9: Verknüpfung der Geschäftsprozesse mit IT-Services und IT-Komponenten[88]

Geschäftsprozesse müssen aus dem Business heraus gewisse (Informations-) Sicherheitsanforderungen berücksichtigen, die sich mit der Vertraulichkeit, Integrität oder Verfügbarkeit bestimmter Informationsarten auseinandersetzen. Daraus ergeben sich technische und organisatorische Anforderungen, die im Service Design der IT-Services berücksichtigt werden müssen, um die Funktionsfähigkeit der betroffenen Geschäftsprozesses sicherzustellen. Dies bedingt wiederum die Einhaltung spezifischer technischer Vorgaben bei der Konfiguration der beteiligten IT-Komponenten, um die geforderte Vertraulichkeit, Integrität und Verfügbarkeit zuverlässig zu gewährleisten.

Welche Hilfsmittel unterstützen beim Thema „*Operationalisierung des IT- (KI-) Governance-Compliance-Managementsystems*“ in der Praxis?

Es ist ein angemessenes digitalisiertes bzw. toolbasiertes Prozessmanagement erforderlich. Die Modellierung von Prozessen sollten sich nach etablierten Standards richten, wie z. B. BPMN 2.0. Zudem sollten die Prozessabläufe Workflow-basiert sein.

Die Erstellung einer Prozesslandkarte – bzw. die Zusammenstellung relevanter Prozessthemenfelder – bildet eine angemessene Grundlage für die Integration des IT- (KI-) Governance-Compliance-Managementsystems in die Ablauforganisation.

Die Klassifizierungsvorgaben für die Informationsverarbeitung in den Geschäftsprozessen kommen aus dem Informationssicherheitsmanagement – die organisationsspezifischen Vorgaben dazu könnten in einer Richtlinie zur Informationsklassifizierung festgelegt werden.

[88] Eigendarstellung.

Die Anforderungen an die Verfügbarkeit der Geschäftsprozesse (die wiederum das IT-Service Design beeinflussen) können mit einer Business Impact Analyse untersucht werden.

Fragen für (interne) Audits:

Sind die relevanten Unternehmensprozesse dokumentiert, versioniert und für das IT- (KI-) Governance-Managementsystem nachvollziehbar definiertund ist Prozesstreue sichergestellt?

Sind die IT-Compliance-Governance-Anforderungen in der Aufbau- und Ablauforganisation der Organisation berücksichtigt?

Wird ein angemessenes IT-Management (z. B. nach ISO 20000, ITIL, COBIT, FitSM o.ä.) betrieben?

9. Überwachung und Bewertung

Das IT- (KI-) Governance-Managementsystem muss regelmäßig angemessen überwacht und bewertet werden. Bei Bedarf müssen Steuerungsmaßnahmen durchgeführt werden.

Die Überwachung und Bewertung des IT- (KI-) Governance-Managementsystems an sich erfolgt ebenfalls primär intern durch diverse, idealerweise „gebündelte“, Funktionen (Controlling, Compliance, Risk, ISM, BCM, KIM, Internes Audit, IKS, Revision (vgl. auch die „Three lines of defense“)), kann aber auch Gegenstand externer Überwachung (Aufsichtsrat, Behörden, „Second party“ und „Third party“ (Zertifizierungs-) Audits etc.) sein.

Reifegrad, Effektivität (Zielerreichung) und Effizienz (Wirtschaftlichkeit) der Managementsystemlandschaft müssen kontinuierlich analysiert, bewertet und von den verantwortlichen Stellen beobachtet werden. Dazu gehört das Sammeln und Auswerten relevanter Informationen und die Entwicklung und Implementierung von (wertorientierten) Kennzahlen, die dabei helfen, die Objekte der „Überwachung“ messen zu können.[89]

Die ISO/IEC 27004:2016 *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation* schlägt diverse Kennzahlen für das ISMS vor und gibt Hinweise, wie diese gemessen und bereitgestellt werden können. Die ISO 42001:2023 nennt in Anhang B Themenfelder, aus denen Kennzahlen für die Managementsystembewertung hinsichtlich des KI-Managements abgeleitet werden können.

[89] Vgl. *Scherer*, Compliance-Managementsystem nach DIN ISO 37301 – erfolgreich implementieren, integrieren, auditieren, zertifizieren, Beuth, 2022, Kapitel 9.

Welche Hilfsmittel unterstützen beim Thema „*Überwachung und Bewertung des IT- (KI-) Governance-Compliance-Managementsystems*“ in der Praxis?

Zur Steuerung und Bewertung des IT- (KI-) Governance-Managementsystems sollte ein Kennzahlensystem eingerichtet werden.

Die Durchführung von (internen) Audits decken viele Verbesserungspotentiale auf. Daher sollte ein Auditprogramm zusammengestellt werden, das ebenso interne wie externe Audits beinhaltet. Resultierende Auditberichte sind wesentliche Bestandteile für die Analyse von Verbesserungspotentialen des IT- (KI-) Governance-Managementsystems.

Managementreviews helfen bei der Beurteilung des Reifegrades des IT- (KI-) Governance-Managementsystems. Hierüber kann – entlang der festgelegten strategischen Ziele – ermittelt werden, ob und inwieweit eine Zertifizierungsreife vorliegt.

Fragen für (interne) Audits:

Gibt es regelmäßige Reviews des IT- (KI-) Governance-Managementsystems inkl. Bewertung der Zielerreichung und Wirksamkeit?

Gibt es ein (internes) Auditprogramm, das die relevanten Normanforderungen und Risiken abdeckt?

10. Verbesserung und Corrective Action

Das (IT- / KI-) Governance-Managementsystem muss angemessen überwacht und regelmäßig bewertet werden. Bei Bedarf müssen Steuerungsmaßnahmen durchgeführt werden.[90]

Aufgrund kontinuierlicher Veränderungen in Organisation und Umfeld muss das (IT- / KI-) Governance-Managementsystem fortlaufend angepasst und verbessert werden, um angemessen und wirksam zu bleiben. Mithilfe eines Prozesses für die Erkennung von Zielabweichungen und der angemessenen Reaktionen darauf können Zielabweichungen frühzeitig erkannt und gesteuert werden. Die gleichen Pflichtverstöße dürfen keinesfalls wiederholt auftreten, weil dies ein wesentliches Indiz dafür wäre, dass das in Governance enthaltene Compliance-Managementsystem *nicht* (!) wirksam ist. Rechtsprechung[91] und Wissenschaft fordern *angemessene* Reaktionen bei relevanten Veränderungen und Compliance-Vorfällen.[92]

---

[90] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.246.

[91] Vgl. *BGH,* Urteil vom 09.05.2017 (Az. StR 265/16 – „KMW“ 1 Rn. 190).

[92] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.248.

Fragen für (interne) Audits:

Gibt es einen dokumentierten Plan zur Steuerung, Überwachung und kontinuierlichen Verbesserung des IT- (KI-) Governance-Systems?

Wird das System regelmäßig überwacht und verbessert?

Werden Governance-Strukturen regelmäßig an Veränderungen angepasst?

Gibt es einen Prozess zum Umgang mit Nichtkonformitäten?

11 Ausblick

Die unzähligen schwerwiegenden täglichen Gefährdungssituationen und Schäden aus der IT-Welt (bis hin zu Gefahren für Leib und Leben bei Ausfall lebensschützender Systeme oder bis zur Insolvenzverursachung) zeigen, dass das Thema IT- / KI- Governance nicht sensibel genug behandelt werden kann. Die aus IT- / KI- Governance abzuleitenden zwingenden Anforderungen und Maßnahmen klingen erschlagend, sind es aber nicht.

Sofern die IT- / KI- Governance korrekt in die Corporate Governance integriert und als Teil des Integrierten Managementsystems (IMS) geführt wird, ergeben sich zum einen zahlreiche Überschneidungen mit bereits im IMS vorhandenen Elementen, zum anderen werden die korrekt zu erledigenden Aufgaben auf viele Schultern verteilt.

IT- / KI- Governance ist primär „*Chefsache*“, also als Teil der Corporate Governance von der Unternehmensleitung (z. B. *Geschäftsführer, Vorstand*) in Primär- und Letztverantwortung zu übernehmen, wie sämtliche Aufgaben der Leitung. Nur durch *rechtssichere Pflichtendelegation* können Aufgabe und Verantwortung auf andere, z. B. Bereichsleitung IT, delegiert werden. IT- / KI- Governance heißt aber auch, dass das Thema in der *Überwachungsverantwortung des Aufsichtsgremiums* bzgl. der Geschäftsführung und der *Weisungsbefugnis des Gesellschafters* liegt.

All das, was im Themenfeld IT- / KI- Governance getan werden muss, muss (!) getan werden. Das ist reine Compliance ohne Ermessensspielraum bzgl. des „Ob“ und damit gebundene Entscheidung.

Beispiel: Mittlerweile ist die Nutzung von KI als weitere Informationsquelle im Rahmen der sog. Business Judgment Rule nach den Grundsätzen ständiger BGH-Rechtsprechung in sicherer Anwendung sogar Pflicht der Entscheider[93].

[93] Vgl. *Scherer*, Die haftungsbewehrte Pflicht zur Verwendung von KI bei unternehmerischen Entscheidungen – auch im Rahmen des Transformations-, Risiko- und Krisenmanagements, 2024, abrufbar unter https://www.risknet.de/elibrary/paper/die-haftungsbewehrte-pflicht-zur-verwendung-von-ki-bei-unternehmerischen-entscheidungen/, abgerufen am 30.11.2025.

Bei IT- (KI-) Governance-Compliance gibt es auch keinen Risiko-Appetit und kein Pareto-Prinzip. Da gibt es nur den „*risikobasierten Ansatz*“.[94] Statt alles gleichzeitig – was in der Praxis unmöglich ist: *Das Wichtigste zuerst*!

Um nicht aufgrund des Vorwurfs einer nicht rechtssicheren Organisation in die *persönliche Haftungsfalle* zu stolpern, ist ein *enthaftendes* IT- / KI- Compliance-Managementsystem unverzichtbar[95].

Für Compliance-Managementsysteme *akkreditierte Zertifizierer* bieten hierzu 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.

Neue technische Entwicklungen *erfordern neue Kompetenzen bei Organen und Beschäftigten*: Die Arbeitslosenquote im US-IT-Sektor stieg im Januar 2025 auf 5,7 Prozent. Branchenanalysten führen dies auf die Automatisierung durch künstliche Intelligenz zurück. Stellenausschreibungen für Softwareentwickler sanken um 8,5 Prozent im Vergleich zum Vorjahr. Vor allem große IT-Konzerne wie Meta und Workday reduzieren ihre Belegschaften[96]. Gleichzeitig entstehen im Bereich IT und KI äußerst viele neue Tätigkeitsfelder[97].

Erforderliche Skills zur Bewältigung der IT- (KI-) Transformation

Nachfolgende Abbildung zeigt – nach Auffassung der *Boston Consulting Group* – die prozentuale Verteilung erforderlicher Kompetenzen zwischen Algorithmen, Technologie, Menschen und Prozessen, um die Anforderungen der IT- (KI-) Transformation zu bewältigen. *Menschen und Prozesse* nehmen hier mit 70 % den größten Raum ein.

---

[94] Vgl. *Scherer*, Nachhaltige Führung und Überwachung von Organisationen (Governance) nach DIN ISO 37000, DIN Media, 2025, S.17.

[95] Vgl. *Scherer*, KI-Verantwortung und enthaftende Wirkung eines KI-Compliance-Managementsystems für Leitung (Vorstand, Geschäftsführer, Officers), Aufsichtsgremium und sonstige Führungskräfte, 2023, abrufbar unter https://www.risknet.de/elibrary/paper/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/, abgerufen am 30.11.2025.

[96] Vgl. *Linden*, Arbeitslosigkeit im IT-Sektor steigt - auch wegen KI?, golem.de, 10.02.2025, abrufbar unter https://www.golem.de/news/tech-branche-anstieg-der-arbeitslosenquote-im-zuge-der-ki-nutzung-2502-193189.html, abgerufen am 30.11.2025.

[97] Vgl. *World Economic Forum,* The Future of Jobs Report 2025, 07.01.2025, abrufbar unter https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf, abgerufen am 30.11.2025.

Abbildung 10: Das „BCG 10-20-70-Modell“[98]

Aus- und Weiterbildung sollten diesen Megatrend nicht verpassen. Die Aktivitäten zur Bewältigung dieser Transformationsanforderungen findet sich *in den nichtfinanziellen Geschäfts- oder Nachhaltigkeitsberichten* von immer mehr Organisationen wieder.[99]

Governance heißt nicht zuletzt, im Rahmen eines effektiven *Changeprozesses* trotz wissenschaftlich nachgewiesener „vorsätzlicher Ignoranz“[100] und typisch menschlicher Beharrungskräfte die Organisation und ihre Menschen erfolgreich durch die *Transformation* zu führen.

In Zeiten des hybriden Krieges ist die **IT- (KI-) Governance-Compliance eine wesentliche *Voraussetzung für Verteidigungsfähigkeit ziviler und militärischer Organisationen und Systeme*.**

---

[98] In Anlehnung an *BCG*, Where is the value in AI, 2024, S.15, online abrufbar unter: https://web-assets.bcg.com/a5/37/be4ddf26420e95aa7107a35aae8d/bcg-wheres-the-value-in-ai.pdf (zuetzt abgerufen am 29.12.2025).

[99] *SGL Carbon*, CSR-Bericht, 2024, S.41-42, abrufbar unter https://www.sglcarbon.com/news/user-upload/SGL-Carbon-2023-CSR-Bericht-DE-22-03-2024-s.pdf, abgerufen am 30.11.2025.

[100] Vgl. *Dörr*, Vorsätzliche Ignoranz: Von den Hindernissen digitaler Transformation und Schrödingers Katze, 13.01.2025, abrufbar unter https://rsw.beck.de/aktuell/daily/meldung/detail/vorsaetzliche-ignoranz-justiz-behoerden-digitale-transformation-studie, abgerufen am 30.11.2025.

Prof. Dr. jur. Josef Scherer

Prof. Dr. jur. Josef Scherer ist Rechtsanwalt und Consulter, Gründer (2012) und Leiter des Internationalen Instituts für Governance, Management, Risk- und Compliance-Management und Leiter der Stabsstelle ESGRC der Technischen Hochschule Deggendorf (THD). Seit 1996 ist er Professor für Unternehmensrecht (Compliance), Risiko- und Krisenmanagement, Sanierungs- und Insolvenzrecht an der THD. Zuvor arbeitete er als Staatsanwalt an diversen Landgerichten und als Richter am Landgericht in einer Zivilkammer.

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

Von 2001 bis 2024 arbeitete er auch als Insolvenzverwalter in verschiedenen Amtsgerichtsbezirken.

Prof. Dr. Scherer ist in diversen Unternehmen und Körperschaften als Compliance-Ombudsperson oder externer Compliance-Beauftragter tätig. Er ist gesuchter Referent bei Managementschulungen in namhaften Unternehmen sowie im Weiterbildungsprogramm des Senders BR-alpha und der Virtuellen Hochschule Bayern (VHB).

In Kooperation mit dem TÜV konzipierte er als Studiengangsleiter den seit über 15 Jahren renommierten und akkreditierten berufsbegleitenden Masterstudiengang Risikomanagement und Compliance-Management an der THD und leitet den Zertifikatskurs „Nachhaltigkeit und GRC“ sowie den berufsbegleitenden Bachelor „Nachhaltigkeit, Governance und Digitalisierung“.

Seit 2015 ist Prof. Dr. Scherer Mitglied des Beirats 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.

Seit 2016 ist Prof. Dr. Scherer Fachlicher Leiter der „User Group Nachhaltige Unternehmensführung (ESG/CSR/GRC) und Compliance“ der Energieforen Leipzig, seit 2018 Mitglied der Arbeitsgruppe 252.07 von Austrian Standards International zur Erarbeitung einer ÖNORM D 4900 ff. (Risiko-Managementsystem-Standards) und seit 2021 Mitglied im DICO (Deutsches Institut für Compliance e. V.).

Seine Forschungs- und Tätigkeitsschwerpunkte liegen auf den Gebieten Nachhaltigkeit (ESG), Integrierte ESGRC-Managementsysteme, Managerenthaftung, Governance-, Risiko- und Compliance-Management, 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.

www.scherer-grc.net

Linkedin: Prof. Dr. Josef Scherer
Der Verfasser publiziert über LinkedIn regelmäßig aktuelle Urteile, Gesetze, Artikel etc. zu ESGRC-Themen.

Fabian Pothorn

Fabian Pothorn studierte Verwaltungsinformatik (Diplom-Verwaltungswirt (FH)) und anschließend Risiko- und Compliancemanagement (M.A.). Seit 2024 ist er der Informationssicherheits-Beauftragte der Technischen Hochschule Deggendorf.
Fabian Pothorn ist Lehrbeauftragter für die Fachgebiete Informationssicherheit, Business Continuity Management, KI-Management sowie Prozessmanagement.
Darüber hinaus ist er als Unternehmensberater tätig und unterstützt Organisationen beim Aufbau und der Optimierung von IT-Governance- und Informationssicherheits-Managementsystemen.