Prof. Dr. jur. Josef Scherer

Lawyer and consultant, Professor of Compliance, Risk and Crisis Management as well as Restructuring and Insolvency Law and Head of the ESGRC Staff Unit at the Deggendorf University of Applied Sciences; Judge at the Regional Court (ret.)

Fabian Pothorn

Information Security Officer at Deggendorf University of Applied Sciences, Lecturer and Management Consultant for IT Governance and Information Security Management Systems

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

Integrated IT (AI) governance compliance Management System

- as a basis for defence and defence capability

Deggendorf, 3.1.2026

Gender note: The personal designations used in this article refer to all genders equally. Gendered designations are dispensed with in favor of better readability.

[1] The detailed author profiles can be found at the end of the article.

Introduction[2]

An IT (AI) governance compliance management system supports executive bodies and employees in meeting legal and technical requirements in the context of managing and monitoring their organization in the[3] field of IT (with AI) through an appropriate and effective organizational structure and process organization.

DIN ISO 37000 (Governance of Organizations), ISO 38500 (IT Governance), ISO 42001 (AI Management System), DIN ISO 22301 (Business Continuity Management System), DIN ISO 22361 (Guidelines for Crisis Management) and, last but not least, DIN ISO 27001 (Information Security Management System) (legal) are in need of supplementation in order to meet the requirements of mandatory regulations.[4]

The continuing escalation of cyber threats, including potential threats through the use of artificial intelligence, is the dominant concern of most organizations. In connection with the associated sharply tightened regulation, the risks of disputes over insurance policies[5] and cyber compliance in the supply chain are also growing.[6]

Since the hybrid war on the[7] part of Russia, China, North Korea, Iran and others against Germany and Europe is no longer – as misleadingly described out of "political correctness" – merely a "threat", but an event that

[2] This article builds on *Scherer, Pothorn, Jones*, *Integrated Compliance Management System for IT/AI Governance in the Context of Digital Transformation*, *IT-Governance* 2025, pp. 8-13.

[3] Governance.

[4] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, Foreword.

[5] In this regard, see the current case law of the Higher Regional Court of Frankfurt and the Federal Court of Justice on the refusal of insurance cover for D&O insurance policies in the event of "deliberate breach of duty" and cardinal breach of duty. This topic also becomes relevant in the event of a violation of legal obligations arising from IT (AI) governance compliance by the managing director, board member or a "senior executive", e.g. CISO (Chief Information Security Officer) or ISB (Information Security Officer). Cf. *Scherer, Seehaus*, Duty to Governance with Early Risk Detection, Resilience and Transformation as a Cardinal Duty of Bodies and Executives, in: ZInsO (Journal for the Entire Insolvency and Restructuring Law), Volume 28, 31/2025, 31.07.2025, pp. 1515-1538, for free download at: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf and *Scherer, Seehaus*, Managerhaftung, D&O Insurance and Early Risk Detection in the Light of Current Case Law, 1 / 2026, for free download on Risknet.de.

[6] Cf. *Beck*, Technology-related disputes dominate 2025: Cybersecurity and AI in focus, 14.02.2025, available online at https://rsw.beck.de/aktuell/daily/meldung/detail/umfrage-unternehmensjuristen-2025-cybersicherheit-ki-untersuchungen (last accessed on 30.11.2025).

[7] Hybrid warfare includes, among other things, cyber attacks, espionage and wiretapping, sabotage, disinformation and propaganda, etc., cf. Federal Office of Civil Protection and Disaster Assistance, 06.03.2025, Hybrid Threats, accessed on 13.12.2025, URL: https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen.

has occurred,[8] the following remarks are also a *contribution to the defense and defense capability of organizations and nations*.

The numerous IT incidents with high losses show that board members, managing directors, CISOs[9], CIOs[10], ISBs[11], supervisory bodies, auditors and lines of defense functions, as well as auditors and certifiers, do not always get the important things right.[12]

1. Initial terminology and legal basis for an IT (AI) governance compliance management system

1.1 First terms

First of all: For most of the terms used here, there are no so-called legal definitions, i.e. binding definitions.

Compliance means dutiful conduct with regard to generally binding rules (laws, case law), but also with regard to (internal) requirements that have been declared binding [e.g. regulations from the Code of Conduct (company-specific rules of conduct)] or an employment contract.[13]

The term *risk* is defined as a spread around an expected value (expected or desired goal). According to this definition, both positive deviations (opportunities) and negative deviations (hazards) are taken into account.[14]

Risk management deals with uncertainties in decisions and the achievement of goals. (Entrepreneurial) Activities and goals are almost always associated with uncertainties. The task of risk management is to systematically identify the opportunities and threats and to evaluate them with regard to potential effects on the company, i.e. to analyze, quantify and manage them.

There is also no legal definition for "*IT or AI governance*", as well as for "*governance*". Therefore, the definitions for these terms are to be derived

[8] Cf. Federal Office of Civil Protection and Disaster Assistance, 06.03.2025, Hybrid Threats, accessed on 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] Information Security Officer (ISB).

[12] In addition to IT governance, important – but often neglected topics are currently also cardinal duty, financial governance, risk governance, business continuity governance compliance, cf. *Scherer, Seehaus*, Duty to Governance with Early Risk Detection, Resilience and Transformation as a Cardinal Duty of Organs and Executives, in: ZInsO (Journal for the Entire Insolvency and Restructuring Law), Volume 28, 31/2025, 31.07.2025, pp. 1515-1538, for free download at: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf.

[13] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.18.

[14] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.18.

from the relevant legal regulations, the state of the art[15] and from relevant standards*, cf. above,* in each case section 3[16] "*Definitions*" and many more.

IT (AI) governance can be legally defined as the "*sustainable, compliance- and risk-based conscientious management and monitoring of organizations, including interaction with relevant stakeholders in the field of IT (AI)".* [17]

The *IT (AI) governance compliance management system* is structural and process organization with various components[18], with the purpose of supporting an organization in decision-making, goal setting, planning, implementation, as well as control and monitoring in order to achieve mandatory and optional goals in the field of IT (AI) governance.[19]

IT (AI) governance represents that part of the structural and process organization or the integrated IT (AI) governance management system that refers, among other things, to:

- IT (AI) compliance management (this in the first place!),
- IT (AI) risk management,
- IT (AI) strategy,
- IT (AI) planning,
- IT (AI) division organization and processes
- IT (AI) implementation,
- IT (AI) ICS,
- IT (AI) audit,
- IT (AI) control and monitoring,
- IT (AI) reporting,
- IT (service) management (the service-oriented management (P/D/C/A) of IT, e.g. everything that has to do with hardware and software),
- IT security management,
- Information security management,
- data protection,
- Digitization incl. use of AI,
- IT (AI) social engineering,
- IT supply chain management,
- Etc.

1.2 The relationship of IT governance according to ISO / IEC 38500:2024 to governance according to DIN ISO 37000:2024

The decision to adopt ISO 37000:2021 identically as DIN ISO 37000 was made in September 2023. Due to its fundamental character for governance,

[15] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, Introduction.

[16] Definitions of information security can also be found in ISO 27000.

[17] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.16, 169.

[18] E.g. roles, goals, resources, process flows, delegations and interactions, etc.

[19] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p. 43.

DIN has identified the need for a German version of ISO 37000 for SMEs and SMEs.

ISO/IEC 38500 (IT governance), with its first version of 2016, is much older than ISO 37000:2021. The current third version, ISO/IEC 38500:2024, is now strongly aligned with the understanding of governance according to ISO 37000. Nevertheless, [20]Klotz *rightly notes* [21] that ISO/IEC 38500 lacks many important aspects of governance that are presented in ISO 37000. For example, the "strategy principle" with the requirement to implement an internal control system (ICS), a risk and compliance management system and the use of external audits in IT governance is not included. The fact that these *lines of defense* systems must also include IT governance is already evident from legislation, case law and other mandatory regulations, regardless of their mention in an ISO standard.[22] As a further shortcoming, *Klotz*[23] mentions the lack of the principle of "data and decisions", which is presented in appropriate detail in ISO 37000.[24]

These explanations alone show the usefulness of integrating various standards both with regard to governance and IT governance, but also with regard to other standards, such as for compliance according to DIN ISO 37301: Compliance creates the basis for identifying, evaluating and controlling risks resulting from non-compliance with mandatory (legal and/or technical) requirements and is therefore indispensable due to the principle of legality that must be observed by everyone. Basis for governance, IT or AI governance, business continuity or information security.[25]

1.3 Legal Basis for an IT (AI) Governance Compliance Management System

Governing bodies and executives bear responsibility for achieving the purpose of an organization.[26]

Digital transformation (with AI), sustainability (ESG), conscientious management of organizations (§§ 43 GmbHG, 93, 116 AktG, 130, 30, 9 OWiG, 53 HHGrdsG etc.)[27], the implementation and operation of an (integrated*) (IT*

[20] Cf. *Klotz*, IT-Governance genormiert – die neue ISO/IEC 38500 (revolutions), IT-Governance 2024, p.19 ff.

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

[22] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.133.

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

[24] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.169.

[25] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, p.20.

[26] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, Chapter 6.1.

[27] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, Chapter 1.

/ AI) governance management system require first and foremost the observance of various legal requirements (compliance), including the "Recognized Rules of Technology" and the "State of the Art".[28] Appropriate reference values, standards or guidelines must also be used for these topics, which are also applicable to the respective organization or company, see 2 below.

There is no obligation to operate an IT (AI) governance management system based on DIN ISO 37000 or ISO / IEC 38500.

The case law takes a different view with regard to risk and compliance management systems and internal control systems covered by IT (AI) governance[29].[30] If something happens within the organization, the failure to set up these systems is considered an (organizational) breach of duty. Conversely, according to the latest supreme court case law of the Federal Court of Justice and the ECJ, implemented compliance or internal control systems may have a detention[31] effect.

And: All mandatory requirements from the area of IT (AI) governance, i.e. the conscientious management and monitoring of organizations in the field of IT / AI – regardless of standards and management system – must be met and are often subject to liability, such as non-compliance with regulatory requirements (AI Regulation, NIS2 Implementation Act, DORA, §§ 43 German Limited Liability Companies Act (GmbHG), 93 the German Stock Corporation Act (AktG), and many more).

It becomes apparent that the interaction and overlaps of various regulations can hardly be overlooked.

Increased regulation can be observed for IT (AI) governance. This will cover the topics of general data processing, specific requirements for providers of digital services, IT and information security, and specific regulation with regard to artificial intelligence. Since the legal requirements are not always coordinated, friction effects occur. For example, companies see the need to adapt the legal requirements for data protection (General Data Protection Regulation) to the current needs of AI use.[32] For many companies, the

[28] Cf. *Scherer, Fruth*, Technology Governance, Special Publication of the Federal Association of Compliance Managers, 2019.

[29] Cf. *LG Munich I*: Judgment of 10.12.2013, (Az. 5 HK O 1387/10 – "Neubürger").

[30] Cf. *Nuremberg Higher Regional Court*, judgment of 30.03.2022, (case no. 12 U 1520/19 – "Gas station tenant").

[31] Cf. *Scherer, Seehaus*, Duty to Governance with Early Risk Detection, Resilience and Transformation as a Cardinal Duty of Governing Bodies and Executives, in: ZInsO (Journal for the Entire Insolvency and Restructuring Law), Volume 28, 31/2025, 31.07.2025, pp. 1515-1538, for free download at: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf und *Scherer, Seehaus*, Managerhaftung, D&O Insurance and Early Risk Detection in the Light of Current Case Law, 1 / 2026, for free download on Risknet.de.

[32] Cf. *Lorber*, Companies demand improvement of the GDPR, 2025, available online at: https://www.springerprofessional.de/datenschutz/dsgvo/unternehmen-fordern-nachbesserung-der-dsgvo/51803174 (last accessed on 19.12.2025).

previous data protection requirements, which have been in force for over seven years with the GDPR, continue to seem overwhelming.[33]

In November 2025, drafts for simplifications of data protection and AI laws ("*Digital Omnibus for Data Protection and for AI")* were presented by the EU. These are aimed at reducing the expenses associated with the legal regulations.[34] It is therefore necessary not only to cover the entirety of the applicable legislation, but also to consider the sometimes highly dynamic changes to existing laws, which take place in quick succession.

As an example, "part of the current regulation in data protection and data management law":

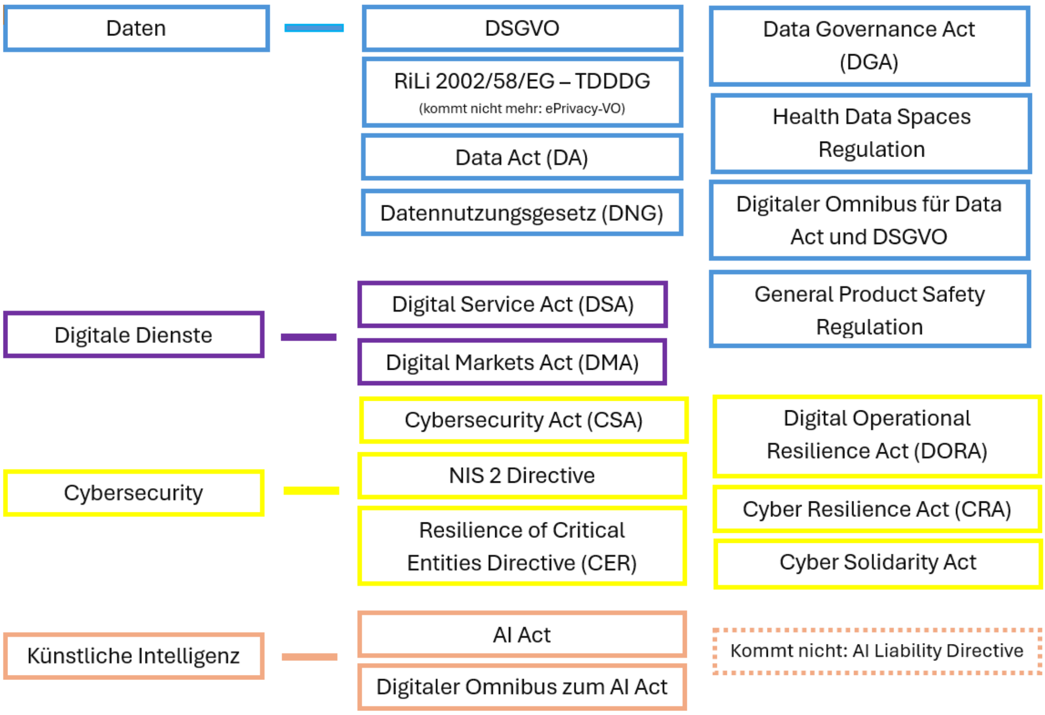

Daten
DSGVO
RiLi 2002/58/EG – TDDDG
(kommt nicht mehr: ePrivacy-VO)
Data Act (DA)
Datennutzungsgesetz (DNG)
Data Governance Act (DGA)
Health Data Spaces Regulation
Digitaler Omnibus für Data Act und DSGVO
General Product Safety Regulation
Digitale Dienste
Digital Service Act (DSA)
Digital Markets Act (DMA)
Cybersecurity
Cybersecurity Act (CSA)
NIS 2 Directive
Resilience of Critical Entities Directive (CER)
Digital Operational Resilience Act (DORA)
Cyber Resilience Act (CRA)
Cyber Solidarity Act
Künstliche Intelligenz
AI Act
Digitaler Omnibus zum AI Act
Kommt nicht: AI Liability Directive

Figure 1: Excerpt from only part of the current regulation in data protection and data management law[35]

In terms of data and information, a significant evolution of regulatory requirements is evident. In connection with the above-mentioned digital transformation and the increasing complexity of digital technologies, which make a data-driven organization possible in the first place, the current developments in the legal framework represent a logical consequence. "Data" and "information" are elementary components in organizational control, whereby the terms must be distinguished from each other.

[33] Ibid.

[34] Cf. *KPMG,* AI and "Digital Omnibus", 2025, available online at: https://kpmg.com/at/de/insights/2025/11/ki-und--digitaler-omnibus-.html (last accessed on 19.12.2025).

[35] Based on *Eckhardt*, DSGVO & Data Act: What is the difference?, 2025. "*Data business law*" refers to the subfield of European law that systematically regulates the legal framework for the collection, processing, use, disclosure and exchange of data within the European Union.

Data is formed from characters that are to be understood as elementary symbols (e.g. letters or numbers) with no inherent meaning. By applying a formal syntax, characters become structured data. Data only acquires information content when it is assigned to defined semantics.

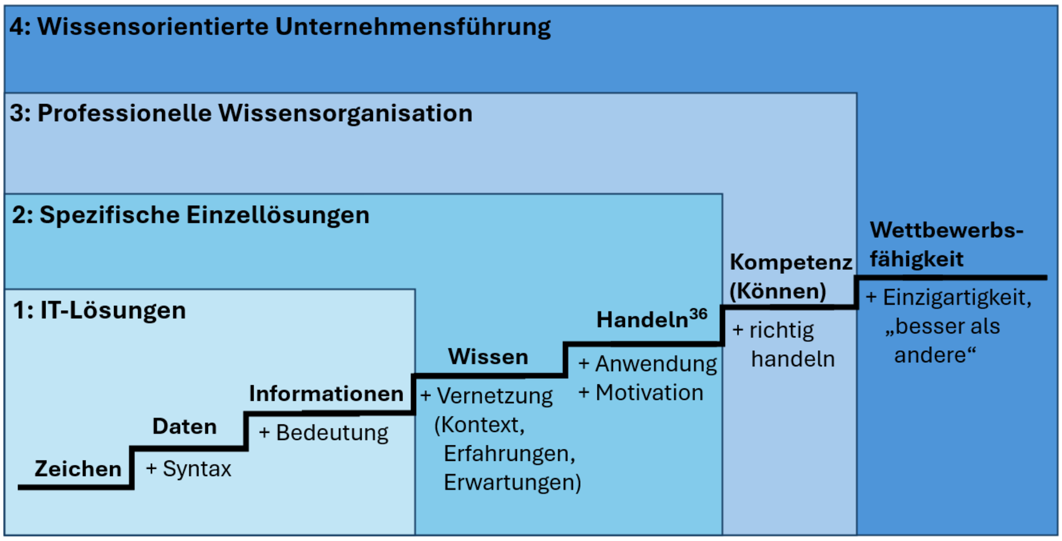

4: Wissensorientierte Unternehmensführung
3: Professionelle Wissensorganisation
2: Spezifische Einzellösungen
1: IT-Lösungen
Zeichen
+ Syntax
Daten
+ Bedeutung
Informationen
+ Vernetzung (Kontext, Erfahrungen, Erwartungen)
Wissen
+ Anwendung
+ Motivation
Handeln[36]
+ richtig handeln
Kompetenz (Können)
+ Einzigartigkeit, „besser als andere“
Wettbewerbs-fähigkeit

Figure 2: Data as the basis for competitiveness[37]

In this respect, data and information form the basis of an organization's decision-making and action. The right ("good") decision-making and action (on the basis of appropriate and correct information – cf. the Business Judgment Rule, Section 93 (1) sentence 2 AktG) creates the opportunity to achieve competitiveness and advantages. In terms of governance, data must be recognized as a strategic resource[38], which is why its regulatory framework must be duly considered.

A corresponding compliance management system supports the fulfilment of (IT / AI) governance obligations. The certification of the (IT / AI) governance management system is not (yet) mandatory, but it can bring significant benefits. While for (IT / AI) governance according to DIN ISO 37000 and ISO / IEC 38500 only certification of the included compliance components according to DIN ISO 37301 is offered in practice by CMS-accredited certification bodies, ISO / IEC 42001:2023 or DIN ISO 27001:2024 are able to be certified.

Note: Below you will find framed questions for (internal) audits or references to tools or work aids.

These are by no means conclusive, but merely show by way of example that it is always worthwhile asking the question:

[36] Author's note: "*Decide and* act".

[37] Graph cf. *North*, Knowledge-Oriented Business Management, 2021, p.43.

[38] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.164.

How can I meet the respective requirements or audit conformity?

Questions for (internal) audits:

Is the obligation to maintain an effective / lived IT (AI) governance compliance management system known and documented?

Are there any binding (e.g. laid down in contracts) stakeholder (e.g. customer) requirements regarding the obligation and content of the operation of the IT (AI) governance compliance management system?

Are the mandatory requirements from legislation, case law, state of the art and other binding regulations (compliance) in the area of IT (AI) governance known and documented?

2. Applicability of the standards or stand-alone systems to be integrated

For *any type of organization*, DIN ISO 37000 and ISO/IEC 38500 are suitable *guidelines* for (IT) governance, ISO/IEC 42001 a suitable *standard* for an AI management system, ISO 27001 for an information security management system, ISO 22301 for a business continuity management system, and ISO 37301 for a compliance management system.

Although both DIN ISO 37000 and ISO / IEC 38500 are not designed according to the Harmonized Structure as a management system standard with ten standard sections, both standards can be integrated, implemented and audited into the other common management system standards.[39]

With appropriate (legal) additions, [40] the integration of these "island systems" as an *appropriate* IT (AI) governance compliance management system is easy.

Whether a procedure was correct or triggers liability and other (existential) problems, however, is ultimately not decided by standards, science, legal or official requirements, but by the "last earthly authority": the judiciary. Which court ultimately decides in the final instance is sometimes a complex question (inter-)nationally.

[39] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.18.

[40] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, with the respective legal supplements / commentaries on the individual standard sections.

Therefore, it is also indispensable with regard to (IT) governance to primarily adhere to the relevant regulation, e.g. relevant laws and supreme court case law, as well as to know the "state of the art" and to meet its requirements.

Clarifying the legal basis and the standard to be used[41] for (IT or AI) governance is the necessary "first step" of the introduction.

The above standards are applicable to any type of organization or parts thereof, regardless of its nature, size or nature.[42]

The extent of the use of IT is irrelevant. The compliance management system can be used to derive the legal obligations for considering the topics of IT governance, information security (with business continuity) and the use of AI in an organization.

3. Definitions ("Digital Literacy")

Again, there are hardly any so-called [43]legal definitions *for the various topics in the field of IT (AI) governance*. Legal definitions are fixed definitions given by the legislator or case law that are binding for everyone.

In the Kalkar decision, for example, the Federal Constitutional Court of Germany *(BVerfG)* laid down in a generally binding manner what "*recognized rules of technology*" and "*state of the art*" mean (also for the IT sector).[44]

Unfortunately, most terms – not only in the field of governance – are not bindingly defined, so that in research, teaching and practice, it must first be clarified exactly what meaning is attached to the relevant terms used.

If terms are defined in internationally recognized standards, it is advisable to use these definitions. However, there is a risk that these definitions can be very abstract, scientific and incomprehensible. It may also happen that they do not correspond to the common and recognized definitions from the respective subject area or that important information is missing.

Example: DIN ISO 37000 defines the term "risk tolerance" in section 3.1.9. In the special risk management standards, such as ISO 31000 ("Risk management") or ISO/IEC 31010 ("Risk assessment techniques"), many relevant definitions for the topic of risk management can also be found. Instead of "risk tolerance", these standards use the term "risk appetite". In expert circles and especially in the field of regulation, the term "risk appetite" is almost exclusively used instead of "risk tolerance".

More important than the choice of terminology, however, is the observance of the note, which is missing in DIN ISO 37000, that a risk appetite or risk tolerance should never be documented in the case of (IT) compliance risks: If a compliance incident were to occur in

[41] Cf. *Klotz*, Norms and Standards for AI Governance, IT Governance, 2024, p.37.

[42] Cf. standard section 1 of DIN ISO 37000, ISO / IEC 38500, ISO 37301, ISO / IEC 42001:2023, ISO 27001:2024.

[43] Cf. 1.1 above.

[44] "Technology clauses" according to the Federal Constitutional Court ("Kalkar decision" of 1978). In detail, see *Scherer, Fruth*, Technik-Governance, special publication of the Federal Association of Compliance Managers, 2019, for free download on the Internet.

this tolerated area, a "consider possible and accept it", i.e. contingent intent, would be proven: fatal for those affected.

Legislators and other drafters of regulations often use so-called "*indefinite legal terms*", such as "safe", "appropriate", etc. Here, the person concerned is only aware that something must be "safe" or "appropriate". However, he often does not know what this means in concrete terms in individual cases. There is then a lot of research to be done and it is to be hoped that a court that may be dealing with it shares this interpretation in the judgment.[45]

Governance compliance deals with all mandatory or mandatory requirements from the area of governance – most of which are subject to sanctions, i.e. the sustainable compliance- and risk-based, conscientious management and monitoring of organizations, including interaction with relevant stakeholders.

Governance compliance risks are the dangers that result from non-compliance with mandatory or mandatory requirements. Almost 90% of all governance risks are likely to be *governance compliance* risks at the same time, especially since the area of governance is largely legally regulated.

Digitization means examining whether the previous business model will be replaced or supplemented in whole or in part by a digital model (e.g. replacement of brick-and-mortar retail with online retail via platform solution). If the previous processes remain in place, there will be an increased "intellectual property" (digital assets), which consists of knowledge and information in the form of processes with associated components (roles, goals, resources), IT systems and IT tools, algorithms including AI, robots and, in many remaining places, people with appropriate competencies and attitudes. These different components of an organization are aligned with digital transformation where appropriate.

Most entrepreneurial activities must be modeled as processes in such a way that they meet the various requirements of compliance, technology, business administration, information security, risk management, sustainability, etc. and ensure that the set goals are achieved. At the same time, it must be analyzed which activities will still be carried out by humans in the future or (partially) automated by applications, IT systems, robots, algorithms or other tools from the fields of digitization and AI.

This raises the question of whether *AI systems* are not to be equated with general applications. AI systems always represent digital or technical information processing systems and thus form a subset of information technology. For this subset, there are specific governance and compliance requirements that must be considered for the (legally) secure and ethical use of AI technologies in organizations. Specific laws (e.g. AI Act) and AI-related standards (e.g. B. ISO / IEC 42001 or NIST AI Risk Management Framework) explicitly deal with the governance compliance requirements in the

[45] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.53.

context of AI, which must be included in IT management at a holistic operational level.

The many possibilities of using AI with the respective legal requirements, risks and opportunities for the organization to be managed should be known and used appropriately.

AI governance is part of IT governance, which in turn is part of general governance. These areas should not be designed as "silos" or "management system islands" but should be integrated into structural and procedural organization (processes).

An essential part of governance is mandatory (compliance) requirements due to comprehensive regulation. That's why compliance is the basis for governance, for IT and also for AI governance, as shown in Figure 3 below.

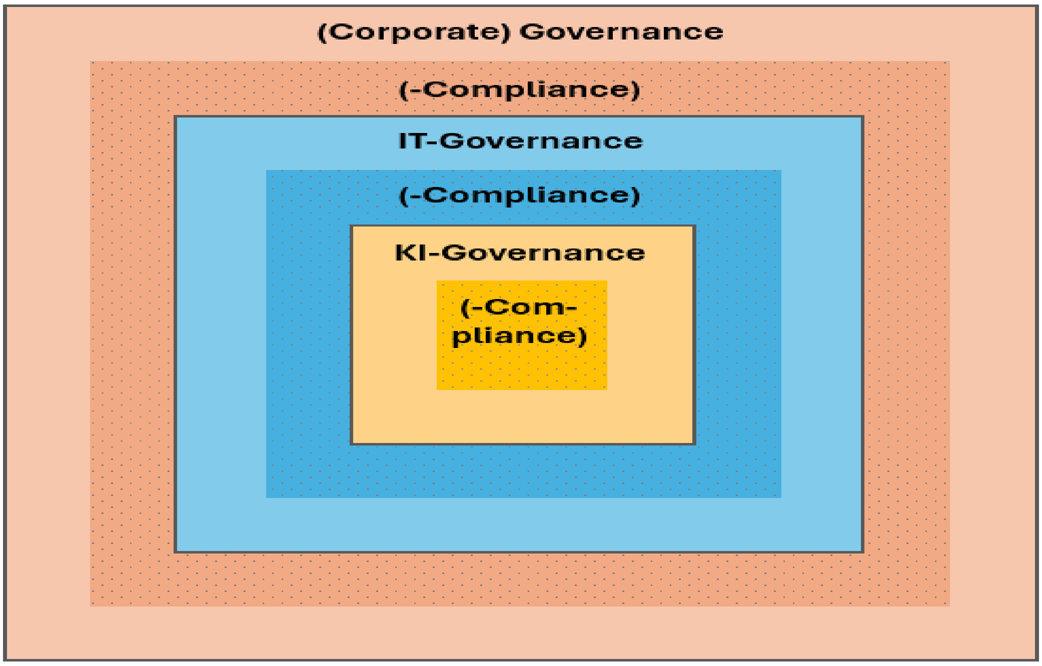


Figure 3: Compliance Components of (IT / AI) Governance

The distinction between *(IT) governance* and *(IT) management* is also not easy due to the lack of a legal definition:

DIN ISO 37000 attempts to distinguish the two terms from each other in standard section 4.2.3 "Governance and management" – but in a very ambiguous, non-legally binding way: According to this, "governance" should deal with setting the framework conditions and "management" with decision-making and practical implementation.[46]

This does not seem correct, since both terms contain strategic and operational elements. Rather, in order to distinguish between the terms "governance" and "management", it seems useful to clarify whether the unitary ("board") or dual ("management and supervisory body") model of

[46] Cf. *Fröhlich & Glasner (eds.),* IT-Governance, Gabler, 2007, p.18.

organizations or companies is being examined. In the case of the latter, demarcation could be seen in the roles, tasks, rights and duties of the various bodies to be described: "Governance" focuses on shareholders, management, supervisory board and stakeholders, while "Management" focuses only on management.[47]

ISO 38500, on the other hand, does not make any strict demarcation attempts. It brings together "governance" and "management" via principles, models and frameworks[48] and emphasizes that in the context of IT, the areas of "governance" and "management" should not be considered separately.[49] Only the responsibilities are to be clearly separated.[50]

Interim conclusion: There is still a need for discussion and awareness and competence regarding various new terms and their content. In doing so, care must always be taken to derive them from legal definitions, the interpretation of indeterminate legal terms by case law and from recognized standards.

It can be assumed that neither baby boomers, Gen Z or Gen Alpha, nor IT experts or executives are familiar with these terms in their correct interpretation. Without a common understanding of terminology, however, it is not possible to communicate, work together or achieve effectiveness.

DIN ISO 37000, ISO/IEC 38500 and ISO/IEC 42001 each define relevant governance terms in Section 3.[51]

Which tools support the topic of "understanding relevant terminology" in practice?

A digital wiki on the organization's intranet, a glossary, easy-to-understand explanation integrated into processes ("*IT (AI) Governance Compliance for Beginners*") or explanatory films (possibly also created with AI support) are helpful in communicating the basic terms.

In addition, appropriate training must be carried out.

[47] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p. 78.

[48] Cf. ISO/IEC 38500:2024, Chapter 4.2, pp. 4-5.

[49] Cf. ISO/IEC 38500:2024, Chapter 6.4, p.16

[50] Cf. ISO/IEC 38500:2024, chap. 6.1, p.14 and *Klotz, Goeken, Fröhlich*, IT-Governance - Ordnungsrahmen und Handlungsfelder für eine erfolgreich Steuerungs der Unternehmens-IT, dpunkt.verlag, Heidelberg, 2023, p.36.

[51] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.45.

Ideally, these terms are addressed for IT (AI) governance, unless there is consensus.

Questions for (internal) audits:

Are the relevant definitions for IT (AI) governance, risk management, compliance, transformation, digitalization, sustainability (ESG), etc. known, understood, and used consistently by the relevant functionaries (executive bodies, lines of defense functions, executives, etc.)?

Are the relevant functionaries (bodies, lines of defense functions, executives, etc.) adequately aware of the conscientious management and monitoring of organizations (governance)?

Is the meaning of technology clauses ("Recognized Rules of Technology"/"State of the Art") known?

4. Analytics, organization, goals, scope, and components of the IT (AI) governance compliance management system

4.1 Analyses of organization, environment, stakeholders and risks

The *organizational analysis* is the presentation of the organization, including the economic and financial situation.

It is advisable to provide a brief description of the business model ("business plan" or a "ratings report") and all areas of the company, as well as an examination of these areas.[52]

In the environment analysis, for example, the "PESTEL" method is used to analyze the multiple environmental developments for the organization under consideration also in relation to the relevant topic (here: IT (AI) governance).

Part of the organizational and *environmental analysis* is a *basic risk check (e.g. a SWOT analysis)* in order to quickly identify strengths, but also weaknesses as well as risks and untapped opportunities in the company and dangers and opportunities from environmental developments.

The organization must also know its "interested parties" and determine their requirements for IT and AI. "*Interested parties"* or "stakeholders" include management, shareholders, customers, suppliers, auditors, the supervisory board, authorities, employees and many more.[53]

By means *of a materiality analysis,* the bodies determine material sustainability topics with the involvement of relevant stakeholders, which may have to be reported.

[52] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, p.66.

[53] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, p.67.

To summarize strengths, weaknesses, threats and opportunities, those responsible have methods such as SWOT or scenario risk analysis at their disposal.

A target-actual comparison shows deviations from (mandatory) target variables (compliance), such as laws, guidelines, standards, etc.

First and foremost, correct conclusions must be drawn from the analyses as to how the IT (AI) governance compliance management system can be designed *in a risk-based, appropriate* and *effective* manner. The greater the organization's compliance risk exposure, the higher the requirements. The aim of these analyses is to prepare the data in a way that is tailored to the target group, ideally as part of the annual or sustainability report.[54]

The preparation and evaluation of these various analyses represent a duty of the organs (managing director / board of directors) with liability, cf. the case law of the *Federal Court of Justice*[55]: Duty of the managing director to know the economic and financial situation of the organization at all times and § 1 StaRUG (The Act on the Stabilization and Restructuring Framework): Duty to identify risks and crises at an early stage.

There is also an obligation to plan properly (§§ 252, 289, 315 HGB, 90 AktG, etc.).[56]

4.2 The organization-wide framework, objectives and strategy of the management system derived from analyses

4.2.1 Organizational framework

The organizational framework of a legally compliant organization contains the following 13 components:[57]

1) (A corporate structure that meets the legal requirements) appropriate under company law (possibly also a holding group structure)
2) Legally compliant organizational charts (group, company, divisional organizational charts)
3) Interface management (communication and cooperation of the necessary interfaces between the individual (process) subject areas and, if necessary, also to "other" ("interested parties")
4) Legally compliant job and job descriptions
5) Legally compliant interaction management (legally compliant regulation

[54] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p. 55 f.

[55] Federal Court of Justice, judgment of 23.07.2024 (Az. II ZR 206/22 – "Managing Director Liability").

[56] Cf. Federal Association of German Management Consultancies: Principles of Proper Planning (GoP), Version 3.0, 2022, available at https://www.bdu.de/verband/qualitaet-im-consulting/ (last accessed on 30.11.2025).

[57] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, p. 75.

of how the executive bodies, companies (if the group structure exists), departments, etc. interact, including with regard to areas of responsibility and responsibilities, representation, deputy, supervision, instructions, communication, etc.)

6) Legally compliant delegation (through selection of suitable delegation recipients, instruction and monitoring – also external)
7) Legally compliant process descriptions (procedural instructions)
8) Effective supervisory and control mechanisms (also with regard to management requirements) – even if services are provided by external parties (e.g. in the context of outsourcing, e.g. in the case of outsourcing, supply or delegation) – see "Lines of Defense"
9) Implemented and effective information and communication management
10) Implemented and effective documentation management
11) Supporting (integrated) management system
12) Adequate personnel resources (in quantity and quality / competencies)
13) Asset Management[58]

The areas of an organization affected by IT governance and other areas should be structured and managed in a uniform manner.

The following figure shows the arrangement *of common standards in the governance framework with the* ESGRC house, which is modelled on a functional organizational chart:

[58] Cf. DIN ISO 55001 Asset Management System.

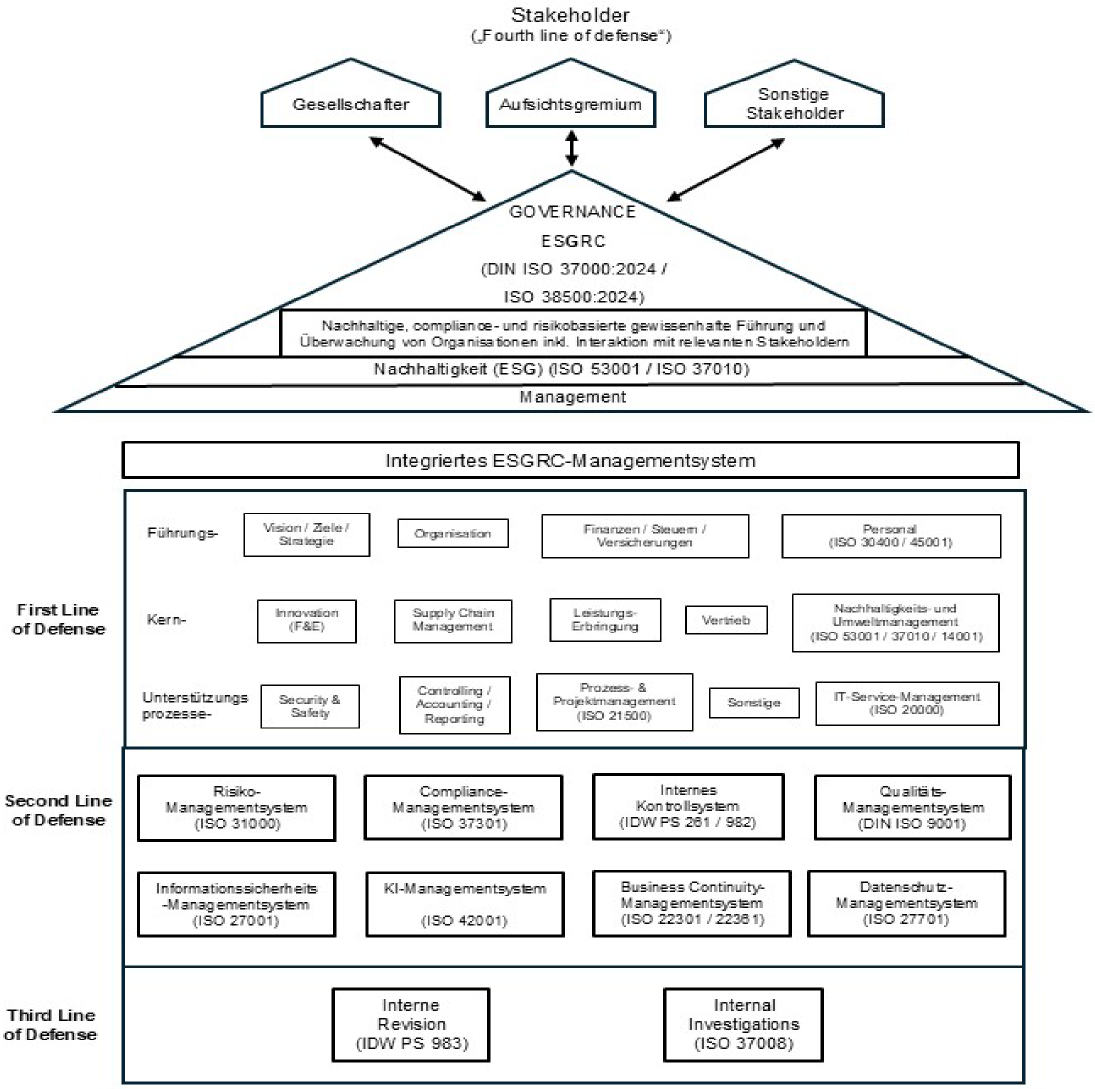

Stakeholder
(„Fourth line of defense")
Gesellschafter
Aufsichtsgremium
Sonstige Stakeholder
GOVERNANCE
ESGRC
(DIN ISO 37000:2024 /
ISO 38500:2024)
Nachhaltige, compliance- und risikobasierte gewissenhafte Führung und Überwachung von Organisationen inkl. Interaktion mit relevanten Stakeholdern
Nachhaltigkeit (ESG) (ISO 53001 / ISO 37010)
Management
Integriertes ESGRC-Managementsystem
First Line of Defense
Führungs-
Vision / Ziele / Strategie
Organisation
Finanzen / Steuern / Versicherungen
Personal (ISO 30400 / 45001)
Kern-
Innovation (F&E)
Supply Chain Management
Leistungs-Erbringung
Vertrieb
Nachhaltigkeits- und Umweltmanagement (ISO 53001 / 37010 / 14001)
Unterstützungs prozesse-
Security & Safety
Controlling / Accounting / Reporting
Prozess- & Projektmanagement (ISO 21500)
Sonstige
IT-Service-Management (ISO 20000)
Second Line of Defense
Risiko-Managementsystem (ISO 31000)
Compliance-Managementsystem (ISO 37301)
Internes Kontrollsystem (IDW PS 261 / 982)
Qualitäts-Managementsystem (DIN ISO 9001)
Informationssicherheits-Managementsystem (ISO 27001)
KI-Managementsystem (ISO 42001)
Business Continuity-Managementsystem (ISO 22301 / 22361)
Datenschutz-Managementsystem (ISO 27701)
Third Line of Defense
Interne Revision (IDW PS 983)
Internal Investigations (ISO 37008)

Figure 4: The "ESGRC House"[59]

All areas are networked via their process flows:

Example: "IT" area:

The *"IT" division* may be represented in (IT) governance by the Chief Information Officer (CIO) and possibly by an audit committee on the Supervisory Board in (IT) governance, strategically planned, managed and supervised.

The Strategy department works with him to develop IT, information security and AI strategy, etc., derived from the organization-wide strategy.

The Organization department takes care of relevant organizational charts, job descriptions, job descriptions, delegations, special representatives, process flows, etc.

[59] Based on *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p. 19.

The Finance department is pleased with functioning financial planning systems and evaluations in real time and provides the financial resources for the IT department via budgets.

And so, it goes on. In a process-based ERP or workflow management system, the mutual connections can become visible.

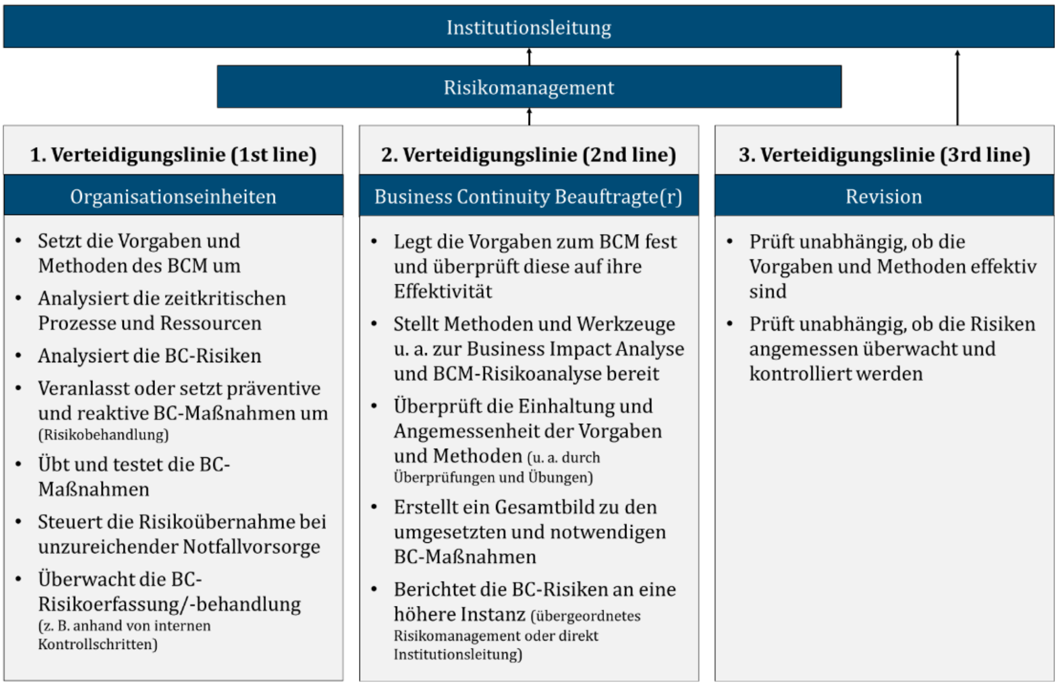
In the first line of defense the operational work takes place. Thus, the work in the "first line" directly serves the value creation of an organization.

In the "second line" are the controlling and monitoring staff units, which are subordinate to the management level. They develop internal organizational regulations in line with strategic guidelines, laws, external requirements and case law. It checks and controls the handling of deviations with the help of risk analyses. Reports will be sent to the management level.

The third line examines the first two lines of defense in terms of appropriateness and effectiveness.

If the first line were to be trained to do the important and right thing correctly, many resources could be saved in the other lines of defense.

The distribution of the tasks of the respective lines of defense is shown in the following figure as an example of the integration of the tasks of business continuity management:



Institutionsleitung

Risikomanagement

1. Verteidigungslinie (1st line)

Organisationseinheiten

- Setzt die Vorgaben und Methoden des BCM um
- Analysiert die zeitkritischen Prozesse und Ressourcen
- Analysiert die BC-Risiken
- Veranlasst oder setzt präventive und reaktive BC-Maßnahmen um (Risikobehandlung)
- Übt und testet die BC-Maßnahmen
- Steuert die Risikoübernahme bei unzureichender Notfallvorsorge
- Überwacht die BC-Risikoerfassung/-behandlung (z. B. anhand von internen Kontrollschritten)

2. Verteidigungslinie (2nd line)

Business Continuity Beauftragte(r)

- Legt die Vorgaben zum BCM fest und überprüft diese auf ihre Effektivität
- Stellt Methoden und Werkzeuge u. a. zur Business Impact Analyse und BCM-Risikoanalyse bereit
- Überprüft die Einhaltung und Angemessenheit der Vorgaben und Methoden (u. a. durch Überprüfungen und Übungen)
- Erstellt ein Gesamtbild zu den umgesetzten und notwendigen BC-Maßnahmen
- Berichtet die BC-Risiken an eine höhere Instanz (übergeordnetes Risikomanagement oder direkt Institutionsleitung)

3. Verteidigungslinie (3rd line)

Revision

- Prüft unabhängig, ob die Vorgaben und Methoden effektiv sind
- Prüft unabhängig, ob die Risiken angemessen überwacht und kontrolliert werden

Figure 5: The "three lines of defense" model in conjunction with BCMS[60]

The range of tasks shown in Figure 5 can be transferred to other management systems. Organizational units must therefore understand and implement the requirements from the IT (AI) governance management system

[60] Cf. *BSI,* 2023, p.77, available online at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf (last accessed on 30.11.2025).

and analyze and treat corresponding risks with their subject-specific expertise.

The requirements for the organization (and thus for implementation in the organizational units) are derived and defined by the management system officers in accordance with the standards applied.

The figure below shows the relationship between the relevant standards.

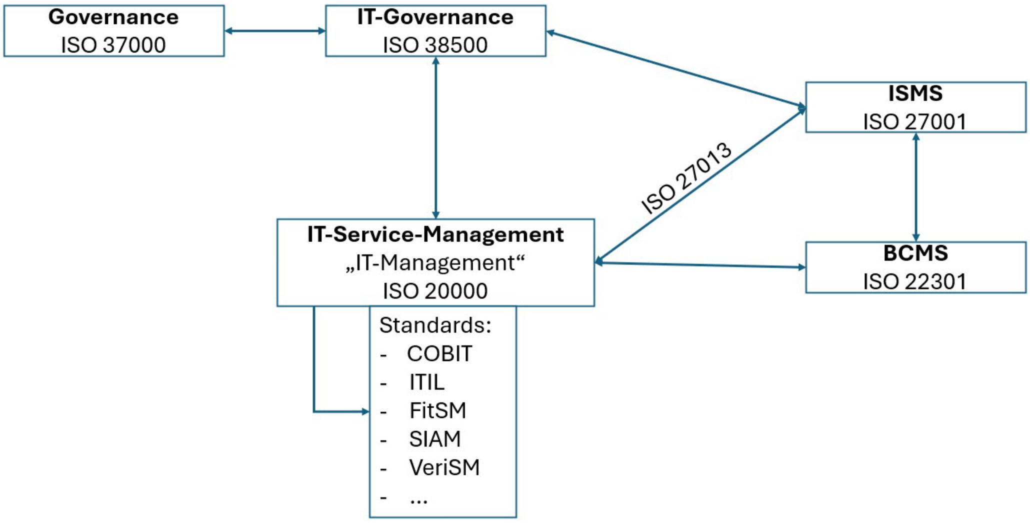


Figure 6: Relationships between relevant norms

The encompassing governance standards, i.e. ISO 37000 and ISO 38500, are related to various management systems that are relevant to an organization: Governance management, compliance management, information security, business continuity, etc. have a significant influence on the operational IT level (IT service management according to ISO 20000 or another standard) in an organization.

4.2.2 IT Goals and Strategies

Appropriate objectives, strategy development and planning – also in the area of IT – are among the essential duties of a managing director, board of directors, etc. (§§ 43 GmbHG, 93 and 116 AktG).[61]

Only if the *organization-wide* vision, goals and strategy are derived from the analyses and serve as specifications for the vision, goals and strategy of the IT (AI) governance management system, will all efforts of management and employees have the same direction. This makes the "red thread" in the goals and strategies visible, and everyone can "pull together". This avoids conflicting goals.

[61] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.57.

What tools support the topic of "**organization-wide framework, goals and strategy of the management system derived from analyses*** ***" in practice?***

For the use of IT and AI in the organization, the vision/mission/goals/strategy must be described in a subject-specific manner in the context of the organization as a whole. The goals are to be formulated by using the "SMART" system of analyzing goals.

To support this, the business processes of the organization must be analyzed. What are the requirements for IT / AI in business?[62]

A formal decision should be made to set the IT/AI governance compliance goals and strategies. This also applies to setting up a project that goes hand in hand with the conception of an IT / AI governance compliance management system. The resolutions are to be adopted by the management.

4.3 The scope of the IT (AI) governance management system

Defining the scope of the IT (AI) governance management system is required by standards and refers to the scope *of the management system*. However, there is a binding obligation from case law to ensure IT (AI) compliance in all areas of the company.[63]

Example: The scope of the ISMS could be limited to a data center and a subsidiary. Certification would also be based on this. The certificate must clearly indicate the selected scope of the system so as not to suggest false security.

However, the obligation to ensure information security extends to the entire organization, including outsourced services.

4.4 Elements of the IT (AI) Governance Compliance Management System

The essential elements for a compliance management system can be found in ISO 37301.[64] The governance management system along DIN ISO 37000 is based on eleven principles, which are to be regarded as central elements. The IT governance management system in the sense of ISO / IEC 38500 takes up precisely these elements and specifies them with regard to information technology focal points (see Table 2).

[62] See also Chapter 4.1.

[63] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p. 58.

[64] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, chapter 4.4.

DIN ISO 37000:2024	ISO 38500:2024	Principle / Element
6.1	5.2	Purpose
6.2	5.3	Value creation
6.3	5.4	Strategy
6.4	5.5	Supervision
6.5	5.6	Accountability
6.6	5.7	Stakeholder involvement
6.7	5.8	Guided tour
6.8	5.9	Data and decisions
6.9	5.10	Risk governance
6.10	5.11	Social responsibility
6.11	5.12	Long-term viability and performance

Table 1: Elements of the IT (AI) Governance Compliance Management System

The current IT governance management model, as described in ISO/IEC 38500:2024, lists six essential elements that can be found in the IT governance management system.[65]

What tools support the topic of "*Elements of the IT (AI) Governance Compliance Management System*" in practice?

A "list of elements" lists the essential elements of the system in accordance with the requirements of case law and standards.

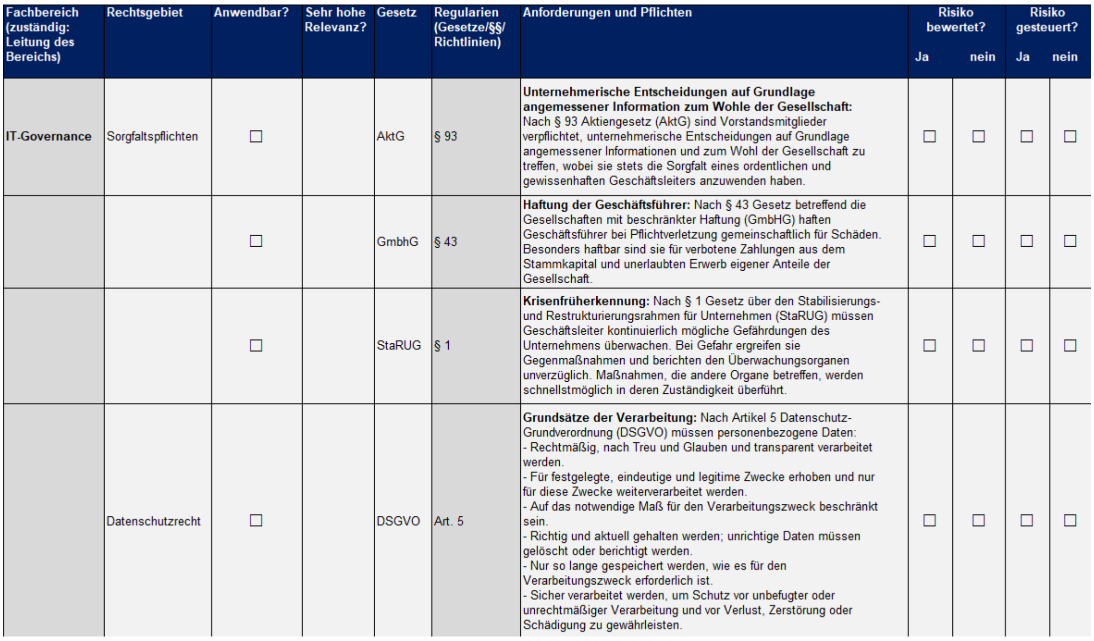
A "management system description" determines the maturity level of the various elements on the basis of a target-actual comparison.

4.5 IT governance compliance requirements, legal information service and process-related legal register

In order to identify, evaluate and control the legal requirements as part of the IT (AI) governance compliance management system, a process-related legal register should be created and maintained.

Figure 7 shows an example of how the development of such a legal register could be started:

[65] Vgl. ISO / IEC 38500:2024, chap. 7.1, p.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.	□	□	□	□

Figure 7: Example of the structure of a first step towards a legal cadaster for IT governance[66]

Ideally, these regulatory requirements are translated into an understandable language, and activities are implemented to meet the requirements in structural and process organization.[67]
At this point, the IT (AI) governance management system is linked to the compliance management system (DIN ISO 37301). The integration of compliance into processes via modern tools is now state of the art.

Example: For the design of an information security management system, as part of the IT (AI) governance management system, the following legal requirements can be derived from the NIS2 Directive Implementation Act alone:

Component	**Objective**	**NIS2 Directive**
Management System	An ISMS must follow a clear system and dynamically adapt to new requirements	Article 21(1)
Governance and the "tone from the top"	The management of the system must come from the management level of the organization	Article 20(1)
Asset Management	Identification, classification and protection of all organizational assets (processes, IT components, services, etc.)	Art. 21 para. 2 j)

[66] This type of *legal cadastral basic step* still has a low degree of maturity. Ideally, an audit-proof integration of all relevant IT (AI) compliance requirements into the tool-supported processes would be possible. An assessment of the risk of not meeting the respective requirement, derived and monitored control measures and reporting should ensure effectiveness / effectiveness. This is now "state of the art".

[67] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, chapter 4.5 and p.93.

Risk management	Creation of a risk system and identification, assessment and management of vulnerabilities and risks	Art. 21 para. 2 a), e) and f)
Supply chain Management	Assessment of suppliers and service providers as a possible security risk	Art. 21 para. 2 d)
Safety Measures	Implementation of technical and organizational measures to protect assets from identified risks	Art. 21 para. 2 g), h), i) and j)
Incident Management	Measures for the detection, reporting and management of (IT/information security) incidents	Art. 21 para. 2 b), c), j) and Art. 23
Business Continuity Management	Preparation of emergency plans and recovery measures to deal with security incidents	Art. 21 para. 2 b), and c) and Art. 22

Table 2: Legal requirements of the NIS2 Directive Implementation Act for an information security management system[68]

In addition, it must be ensured that new or amended regulations are recorded and implemented in real time. In the case of legal information services, the provider landscape is changing rapidly due to the possibilities of AI.

What tools support the topic of* "process-related legal registers" *in practice?

A process-related, risk-assessed legal register must be created and kept up to date at all times (Legal Information Service).

IT and AI compliance is more than NIS2 and the AI Regulation: Tensions between data protection, copyright, intellectual property rights, product compliance and AI legal requirements can jeopardize the legal security of an organization when using AI technologies.[69] The creation of a matrix of legal areas proves to be helpful. This can also be used with regard to a risk assessment of areas of law.

DIN ISO 27001:2024, Annex A, Measure 5.31 requires the fulfilment of "*legal, statutory, regulatory and contractual requirements*" and the creation of a legal register.

Questions for (internal) audits:

Is an always up-to-date process-related legal register implemented and effective to meet IT (AI) compliance requirements?

[68] Following *Haider*, Implementing NIS2 with Zero Trust – A Practical Approach. In: Kälberer, D.R., Staffler, L. (eds) Regulation and Innovation in the Age of Digitalization. Springer Gabler, 2025, p. 69.

[69] Cf. *World Economic Forum*, Governance in the Age of Generative AI, 2024, pp. 6-7, available online at https://www3.weforum.org/docs/WEF_Governance_in_the_Age_of_Generative_AI_2024.pdf (last accessed on 30.11.2025).

Are relevant standards for governance, risk management, compliance, information security, etc. also used as reference values?

Is the achievement of the mandatory and voluntarily set goals ensured by an appropriate process-oriented structural and procedural organization?

4.6 IT (AI) Governance Compliance *Risk Management*

The IT (AI) governance compliance-risk management process[70] serves to identify, assess and manage threats and opportunities at an early stage that could influence the achievement of an organization's goals.

A risk analysis systematically searches for the causes and dangers of deviations. All IT (AI) compliance requirements alone pose dangers (risks) in an unfulfilled state. In addition, there are a lot of other risks outside of compliance.

All employees should have a basic knowledge of risk management. Outsourced services must also be included. For non-controllable relevant residual risks, a business continuity management system is required.[71]

There are special requirements for IT governance risk management, especially in regulated organizations that are considered critical infrastructure within the meaning of the BSI Critical Infrastructure Ordinance, fall under the NIS2 Directive or under the Digital Operational Resilience Act (DORA):

For example, the NIS2 Directive, which has been in force since March 2025, states in Article 21 (1) [72] and almost identically in Section 30 BSIG, which is supplemented by the NIS2 Implementation Act:

'Member States shall ensure that essential and essential entities take appropriate and proportionate technical, operational and organizational measures to manage the risks to the security of the network and information systems used by those entities for their operation or for the provision of their services and to prevent or minimize the impact of security incidents on the recipients of their services and on other services.

The measures referred to in the first subparagraph shall ensure a level of security on the network and information systems commensurate with the existing risk, considering the state of the art and, where appropriate, the relevant European and international standards, as well as the costs of implementation. In assessing the proportionality of those measures, due consideration shall be given to the extent of the institution's risk exposure, the size of the facility and the likelihood of the occurrence of security incidents and their severity, including their social and economic impact.'

[70] Cf. *Scherer*, Successfully implementing, integrating, auditing, certifying compliance management system according to DIN ISO 37301:2021, DIN Media, 2022, chapter 4.5.

[71] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.180.

[72] On 05.12.2025, the NIS2 Implementation Act came into force. Article 21 of the NIS2 Directive supplements § 30 BSIG with the same regulatory content via the NIS2 Implementation Act.

Risks to an organization's network and information systems, including those involving AI, contribute to its overall risk exposure. This requires a holistic risk management approach that grows out of the organization's governance.

The requirements for an (IT and AI) risk and early crisis detection system are particularly topical in the light of the latest regulation (e.g. §§ 1 StaRUG, 91 paras. 1 and 3 AktG, etc.), case law (BGH, OLG Nuremberg, OLG Frankfurt, etc.) and standards (IDW S 16 and PS 340, DIIR No. 2 etc.).[73]

_What tools support the topic of "_IT (AI) governance-compliance-risk management_" in practice?_

Ideally, an appropriate risk management system is already in place.
The processes, methods and tools should be documented, known and effective in the context of the IT (AI) governance management system.

Questions for (internal) audits:

Is IT (AI) risk management part of the Integrated Risk Early Detection and Risk Management System?

Are the management processes of the company management risk-based and integrated into the overall strategic management?

Have operational technology (OT) risks been identified and integrated into the organization-wide risk management system?

Are risks associated with the use of artificial intelligence systematically assessed – not only in accordance with the AI Regulation – and managed by governance measures?

5 Leadership and commitment

5.1 "Tone from the Top" in the Integrated (IT / AI) Governance Compliance Management System[74]

"Leadership" or the so-called *tone from the top,* i.e. the role model function of management, supervisory body, shareholders and executives with regard to the (integrated) IT (AI) governance compliance management system is

[73] Cf. *Scherer / Seehaus*, Duty to Governance with Early Risk Detection, Resilience and Transformation as a Cardinal Duty of Organs and Executives, in: ZInsO (Journal for the Entire Insolvency and Restructuring Law), Volume 28, 31/2025, 31.07.2025, pp. 1515-1538, for free download at: https://www.govsol.de/files/fil/artikel-scherer-seehaus--pflicht-zu-governance-.pdf, and *Scherer, Seehaus*, Managerhaftung, D&O Insurance and Early Risk Detection in the Light of Current Case Law, 1 / 2026, for free download on Risknet.de.

[74] See Harmonized Structure Section 5.1

the basis for *effectiveness* ("being lived") in all areas and processes of the company.

The IT (AI) governance culture and the perception of responsibility for the governance management system by all employees are also of basic importance.[75]

5.2 Policy of the (IT/AI) Governance Compliance Management System[76]

The basic orientation ("policy") of the corresponding management system ("lighthouse", "best in class", "state of the art", "risk-averse", "risk-affine", ...) must also be decided by the management in order to enable employees to find their way around.

5.3 Roles and responsibilities

In the course of the ongoing trend of increasing digitalization, many new roles are emerging that organizations have to consider. AI management is increasingly becoming part of the IT sector in particular. The transitions are fluid and thus closely interwoven with IT governance.

In addition to the "classic" roles, such as the Chief Information Officer (CIO), Chief Information Security Officer (CISO), Business Continuity Officer (BCO), Chief Risk Officer (CRO), IT administrator, IT architect, programmer, etc., new roles or job profiles are currently developing.

These include, for example, AI architects, chief AI officers (CAIO), AI risk managers, prompt engineers, AI ethics specialists and many more, as shown in Figure 8:

[75] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.119.

[76] See Harmonized Structure Section 5.2

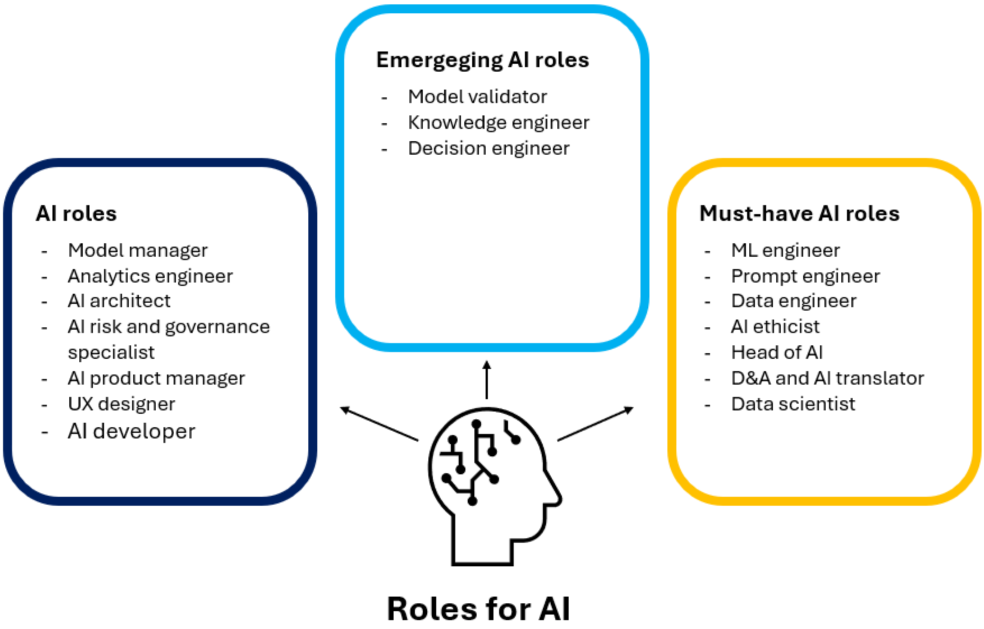


Figure 8: New AI-related roles[77]

The newly emerging roles, which are only just beginning to be established, must first be defined in the organization. It should be noted that the definition of new roles can certainly counteract previous assumptions. The Decision Engineer serves as an example of this, which is particularly concerned with supporting *data-based decision-making*[78] . While IBM, as a computer pioneer and leading IT company, still made it clear in 1979 that computers should never take responsibility for management decisions, the topic of computer-aided decision-making is being discussed anew in line with the new technological achievements.[79]

What tools support the topic of* "roles in the IT (AI) governance compliance management system"** ***in practice?

First of all, a well-founded job needs analysis for IT and AI compliance is required in order to systematically determine the quantitative and qualitative personnel requirements. This is necessary for personnel office planning.

[77] Self-presentation based on *Gartner*, 2025, available online at: https://www.gartner.com/en/newsroom/press-releases/2024-05-14-artificial-intelligence-is-creating-new-roles-and-skills-in-data-and-analytics (last accessed on 30.11.2025).

[78] Cf. *Scherer*, Digital Decision Management, 2020, available online at https://www.scherer-grc.net/files/fil/digital-decision-management.pdf (last accessed on 21.12.2025) and *Rieger, Scherer*, Der digitale Zwilling im Gesundheitswesen, JMG, 2021, p. 12f., available online at: https://www.govsol.de/files/fil/jmg-2-21-art-rieger-scherer-korr.pdf (last accessed on 21.12.2025).

[79] Cf. *IBM*, AI decision-making: Where do businesses draw the line?, 2025, available online at https://www.ibm.com/think/insights/ai-decision-making-where-do-businesses-draw-the-line (last accessed on 21.12.2025).

Based on this analysis, precise job descriptions must then be developed that clearly define the specific tasks, responsibilities and required competencies of the new roles to be created.

Finally, a targeted recruiting concept must be established that sustainably imparts the necessary qualifications through tailor-made training and further training measures.

Questions for (internal) audits:

Is an appropriate "tone from the top" ensured - also - in terms of governance at management level, department level and supervisor level?

Does the company have qualified and committed employees who are supported by a positive corporate culture?

6. Planning and conception

The planning *of the IT (AI) governance management system* is about the presentation of goals and the value contribution, the definition of the target state, the target-actual comparison, the evaluation of alternative strategies as well as the decision for and project planning of measures to achieve the goals *of the system*.

A state-of-the-art IT and information security concept *should also be implemented when planning a digitization campaign*: The vulnerability of the organization increases with an increasing degree of digitalization.[80]
It is important to consider: "*If you fail to plan, you are planning to fail!*"[81].

With regard to the goals of the IT (AI) governance management system, see already 4.2 above: They cannot be determined arbitrarily, but are to a large extent already predetermined on the basis of existing target or reference parameters: Laws, case law, state of the art and in some cases also standards (ISO 37000:2024, ISO / IEC 38500:2024, DIN ISO 27001:2024, 22301:2020, ISO 42001:2023, etc.) etc. specify what must be achieved.

In addition, further goals (optionally) decided by the management can then be added.

The goals should be "SMART" and documented. This acronym is made up of the following words:

S – Specific, M – Measurable, A – Achievable, R – Relevant, T – Timely.

[80] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p. 20.

[81] Quote from Benjamin Franklin.

Goals should be specific – it should be clear exactly what it is about. They should also be measurable, so that it can be said at any time whether and to what extent the goal will be achieved. In addition, goals must always be achievable. Goals should be equally relevant to the organization. And finally, goals should be time-bound, so the time window until they are achieved must be precisely defined.[82]

For the planning of the information security requirements from ISO 27001, Annex A, a *statement of applicability* must be prepared. The 93 measures from Appendix A are examined for their applicability and relevance in the organization. This is an essential aspect in the design of the IT (AI) governance management system.

What tools support the topic of "**planning and conception of the IT (AI) governance compliance management system*****" in practice?***

The aim was to establish a system of goals and key figures that translates strategic specifications into measurable KPIs and thus enables success to be monitored.

Measures can be planned, assigned and tracked in a structured way using task management, from simple Excel lists to modern workflow tools.

Questions for (internal) audits:

Are the goals and strategy of the IT (AI) governance compliance management system currently derived from organizational, environmental, interested parties, materiality, SWOT, (compliance) risk analysis, documented and backed up with "smart" goals?

7. Resources, awareness, communication and documentation

The management must provide the resources necessary for an appropriate, effective IT (AI) governance management system.

The questions of where the manager or employee stands in the work process between robots, algorithms and (partially) automated, intelligent process flows, what their tasks and goals are – especially with regard to information security and the use of AI – and what skills they need for this must be answered. In doing so, it must be ensured that the necessary resources and competencies are available in the required quality and quantity.

There must be appropriate awareness of the system, and all relevant information must be communicated appropriately, internally and externally.

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

The general requirements for documents and records must be complied with in accordance with company-wide regulations and mandatory legal requirements. All essential components of the IT (AI) governance management system must always be documented and archived in a legally compliant manner.

It is advisable to decide as early as possible which IT system (intranet, document management system, cloud, etc.) and elements of the management system will be documented.[83]

What tools support the topic of "*Resources, awareness and communication in the IT (AI) governance compliance management system*" in practice?

For the IT (AI) governance management system, the necessary resources (financial resources, premises, IT, personnel, etc.) must first be determined. In line with the risk-based approach, proportionality must be considered. This does not mean that the cheapest options for action are always the most economical.

It is advisable to create a knowledge and competence matrix for the assignment of competencies. For this purpose, internal wiki pages can be created, e-learning courses can be made available and internal newsletters can be distributed.

In addition, the IT-supported form of control of the IT (AI) governance management system must be considered. Appropriate digital ESGRC tools are used for this purpose, which are useful for design and control. Excel-based control is not recommended. Corresponding functional specifications must be drawn up for subject-specific tools.

Defined communication processes and document management systems also support the design of the IT (AI) governance management system. The essential contents can be brought together in a communication or documentation manual.

Questions for (internal) audits:

Is there a supporting system (e.g. process and ESGRC platform) that supports the implementation of the IT (AI) governance management system?

Are sufficient competencies and resources ensured for the IT (AI) governance management system?

[83] Cf. *Scherer*, Compliance management system according to DIN ISO 37301 – successfully implementing, integrating, auditing, certifying, Beuth, 2022, chapters 7.1 and 7.2.

8. Operations – Operationalization of IT governance compliance and process management

All elements of the (IT / AI) governance management system must be integrated into the operational procedures (processes). Conscientious managing directors and board members are responsible for the effectiveness of the IT (AI) governance management system. Effectiveness means effectiveness and "being lived".

People often act irrationally or even in breach of duty due to the way the brain works or a lack of up-to-date knowledge.[84] This is where leading *human workflow processes* can help you do the *right thing*. Ideally, each participant in the process then knows *what* to do *when, how* and *where*. Even *outsourced processes* must be effective in terms of compliance. This must also be monitored. For example, this approach is also relevant for the use of generative AI models in organizations. Public AI systems such as ChatGPT or Gemini are not suitable for critical information. Above all, AI-generated content must be checked by experts. It should also be noted that critical decisions always remain the responsibility of humans.

For IT management, which falls within the scope of the IT (AI) governance management system, ISO / IEC 20000-1:2018 presents certain standard process topics that are taken up by various best practice standards such as COBIT, ITIL or FitSM.[85] In ITIL, a total of 34 process topics are described in the current version 4, which are shown in Table 4.

General Management	**Service Management**	**Technical Management**
• Strategy management process • Portfolio management process • Architecture management • Financial management service • Workforce and talent management	• Business analysis process • Service catalogue management process • Service design • Service level management • Availability management	• Deployment management process • Infrastructure and platform management process • Software development and management

[84] Cf. *Kahneman*, Thinking fast and slow, 2011, introduction, as well as *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.168 and *Rieger, Scherer*, The Digital Twin in Healthcare, JMG, 2021, p. 83, available online at https://www.govsol.de/files/fil/jmg-2-21-art-rieger-scherer-korr.pdf (last accessed on 21.12.2025).

[85] Cf. *Pilorget*, Managing IT in a digital world, Springer Vieweg, 2025, p.38 ff.

- Continual improvement - Measurement and reporting - Risk management - Information security management - Knowledge management - Organizational change management - Project management - Relationship management - Supplier 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	

Table 3: 34 process topics for IT management according to ITIL v4

IT service management is about linking the IT organization with the governance structures of an organization. These include, for example, strategy management, risk management, information security management, knowledge management or project management. This systematically ensures that the relevant IT governance requirements in the organization are recognized and considered at the operational level.

Service management practices refer to the direct value creation of an organization's IT services. These services are intended to ensure appropriate planning, delivery and improvement of IT. For example, on the topic of *incident management*, processes must be developed that relate to dealing with disruptions in IT.

Technical management practices go deeper into the technical level of IT infrastructure and also support the delivery of technical services. At this point, for example, we are talking about processes for secure software development.

How does IT service management support the operationalization of (IT/AI) governance?

ISO 38500 and ISO 20000 are developed by the same subcommittee of ISO[86]. In this respect, there is a certain professional proximity anyway. ISO

[86] Vgl. ISO/IEC JTC 1/SC 40, https://committee.iso.org/home/jtc1sc40 (last accessed on 12.08.2025).

20000 or ITIL[87] is largely implemented in the "first line" of an organization (focus on the IT department). It must be ensured that the requirements of the management systems in the IT processes (see Figure 6) are considered. ISO 27013 is a connected standard for this.

While ITIL 3 still presented quite concrete IT processes, ITIL 4 now contains more process requirements (with KPIs) that the organization must consider in its own process design. This allows for a more customized approach where IT-business alignment can be better optimized. Without IT service management (whether with ITIL, FitSM, ISO 20000 or another best practice approach), an effective management system structure – whose requirements are derived from the "second line" – will not be possible. Depending on the size and scope of the IT department, the strength of the relationship between ITSM and the management systems (such as information security management system, business continuity management system, AI management system, etc.) varies. At best, there is always a critical dependence on both sides.

The "information security management" practice from ITIL 4 deserves special mention. This practice represents the concrete operationalization of the ISMS (second line to first line) requirements. Without ISMS, the practice of "information security management" will not work. In order to be able to assess the appropriateness and effectiveness of an ISMS in organizations, a look at the IT service processes is indispensable (information security "by design"). This also applies to the BCMS (see practice "Availability Management", "Service Continuity Management", "Incident Management", "Service Level Management") and other management systems.

Care must be taken to ensure that digitization and compliance are introduced conceptually and "holistically" ("from a single source") in the integrated IT (AI) governance management system. This means that the organization's process management (general management) is linked to IT service management and technical management. This results in a "top-down" view that assigns governance compliance requirements to business processes, IT services and the individual IT components and connects these levels.

[87] *IT Infrastructure Library* – a collection of IT management best practices from PeopleCert.

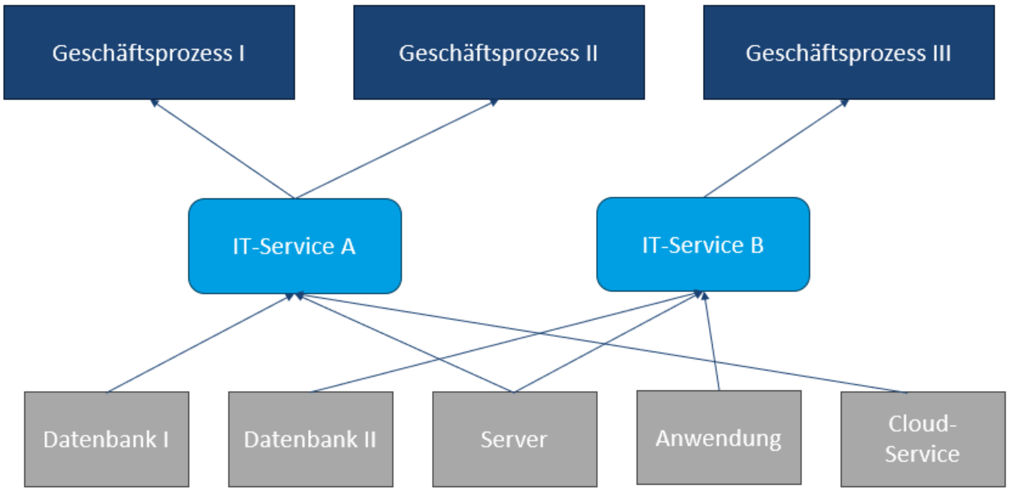


Figure 9: Linking business processes with IT services and IT components[88]

Business processes must consider certain (information) security requirements from within the business that deal with the confidentiality, integrity or availability of certain types of information. This results in technical and organizational requirements that must be considered in the service design of the IT services in order to ensure the functionality of the affected business processes. This in turn requires compliance with specific technical specifications when configuring the IT components involved in order to reliably guarantee the required confidentiality, integrity and availability.

What tools support the topic of* "operationalization of the IT (AI) governance compliance management system" *in practice?

Appropriate digitized or tool-based process management is required. The modeling of processes should be based on established standards, such as BPMN 2.0. In addition, the process flows should be workflow-based.

The creation of a process map – or the compilation of relevant process topics – forms an appropriate basis for the integration of the IT (AI) governance compliance management system into the process organization.

The classification specifications for information processing in business processes come from information security management – the organization-specific requirements for this could be defined in a guideline for information classification.

The requirements for the availability of business processes (which in turn influence IT service design) can be examined with a business impact analysis.

[88] Self-presentation.

Questions for (internal) audits:

Are the relevant business processes documented, versioned and defined in a way that is comprehensible for the IT (AI) governance management system, and is process adherence ensured?

Are the IT compliance governance requirements considered in the organizational structure and process organization?

Is appropriate IT management (e.g. according to ISO 20000, ITIL, COBIT, FitSM or similar) operated?

9. Monitoring and evaluation

The IT (AI) governance management system must be adequately monitored and evaluated on a regular basis. If necessary, control measures must be carried out.

The monitoring and evaluation of the IT (AI) governance management system itself is also primarily carried out internally by various, ideally "bundled" functions (Controlling, Compliance, Risk, ISM, BCM, KIM, Internal Audit, ICS, Auditing (see also the "Three lines of defense")), but can also be the subject of external monitoring (supervisory board, authorities, "second party" and "third party" (certification) audits, etc.).

The degree of maturity, effectiveness (achievement of targets) and efficiency (cost-effectiveness) of the management system landscape must be continuously analyzed, evaluated and observed by the responsible authorities. This includes the collection and evaluation of relevant information and the development and implementation of (value-oriented) key figures that help to measure the objects of "surveillance".[89]

ISO/IEC 27004:2016 *Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation* proposes various key figures for the ISMS and provides guidance on how they can be measured and provided. ISO 42001:2023 lists in Annex B topics from which key figures for the management system evaluation with regard to AI management can be derived.

What tools support the topic of "*monitoring and evaluation of the IT (AI) governance compliance management system*" in practice?

A KPI system should be set up to control and evaluate the IT (AI) governance management system.

The implementation of (internal) audits reveals many opportunities for improvement. Therefore, an audit program should be put together that includes both internal and external audits. The resulting audit reports are

[89] Cf. *Scherer*, Compliance management system according to DIN ISO 37301 – successfully implementing, integrating, auditing, certifying, Beuth, 2022, Chapter 9.

essential components for the analysis of potential for improvement of the IT (AI) governance management system.

Management reviews help assess the maturity of the IT (AI) governance management system. This can be used to determine whether and to what extent certification is ready – in line with the defined strategic goals.

Questions for (internal) audits:

Are there regular reviews of the IT (AI) governance management system, including evaluation of target achievement and effectiveness?

Is there an (internal) audit program that covers the relevant standard requirements and risks?

10. Improvement and corrective action

The (IT/AI) governance management system must be adequately monitored and regularly evaluated. If necessary, control measures must be implemented.[90]

Due to continuous changes in the organization and environment, the (IT/AI) governance management system must be continuously adapted and improved in order to remain appropriate and effective. With the help of a process for detecting target deviations and the appropriate responses to them, target deviations can be detected and controlled at an early stage. The same breaches of duty must not occur repeatedly under any circumstances, because this would be a significant indication that the compliance management system contained in governance *is not* (!) effective. Case law[91] and academia demand *appropriate* responses to relevant changes and compliance incidents.[92]

Questions for (internal) audits:

Is there a documented plan for controlling, monitoring and continuously improving the IT (AI) governance system?

Is the system regularly monitored and improved?

Are governance structures regularly adapted to changes?

Is there a process for dealing with non-conformities?

[90] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.246.

[91] Cf. *Federal Court of Justice,* judgment of 09.05.2017 (Az. StR 265/16 – "KMW" 1 para. 190).

[92] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.248.

11 Outlook

The countless serious daily hazards and damage from the IT world (up to dangers to life and limb in the event of failure of life-protecting systems or up to the causation of insolvency) show that the topic of IT / AI governance cannot be treated sensitively enough. The mandatory requirements and measures to be derived from IT / AI governance can appear overwhelming, but they are not.

If IT / AI governance is correctly integrated into corporate governance and managed as part of the Integrated Management System (IMS), there will be numerous overlaps with elements already present in the IMS and the tasks to be completed will be distributed more evenly.

IT / AI governance is primarily a "*top priority*", i.e. as part of corporate governance by the company management (e.g. *managing director, board of directors)* in primary and ultimate responsibility, as well as all tasks of the management. Only through *legally secure delegation of duties* can tasks and responsibilities be delegated to others, e.g. the head of IT. However, IT / AI governance also means that the topic lies in the *supervisory board's responsibility* with regard to the management and the *shareholder's authority to issue instructions*.

Everything that needs to be done in the field of IT / AI governance must (!) be done. This is pure compliance without discretion as to whether or not it is required and thus a binding decision.

Example: In the meantime, the use of AI as an additional source of information within the framework of the so-called Business Judgment Rule. Even the duty of decision-makers in the safe application of AI must be done in accordance to the principles established in case law by the German Federal Court[93] of Justice.

When it comes to IT (AI) governance compliance, there is also no risk appetite and no Pareto principle. There is only the "*risk-based approach*".[94] Instead of everything at the same time – which is impossible in practice: *First things first*!

In order not to stumble into the *personal liability trap* due to the accusation of an organization that is not legally compliant*, an exempt* IT / AI compliance management system is indispensable[95].

[93] Cf. *Scherer*, The liability-reinforced duty to use AI in entrepreneurial decisions – also in the context of transformation, risk and crisis management, 2024, available at https://www.risknet.de/elibrary/paper/die-haftungsbewehrte-pflicht-zur-verwendung-von-ki-bei-unternehmerischen-entscheidungen/, accessed on 30.11.2025.

[94] Cf. *Scherer*, Sustainable Leadership and Monitoring of Organizations (Governance) according to DIN ISO 37000, DIN Media, 2025, p.17.

[95] Cf. *Scherer*, AI Responsibility and Liability of an AI Compliance Management System for Management (Board of Directors, Managing Directors, Officers), Supervisory Board and Other

Certifiers accredited *for compliance management systems* now offer CMS certifications according to DIN ISO 37301 with a special scope of the audit for IT (AI) governance compliance based on DIN ISO 37000 and ISO / IEC 38500.

New technical developments *require new competencies among executive bodies and employees*: The unemployment rate in the US IT sector rose to 5.7 percent in January 2025. Industry analysts attribute this to automation through artificial intelligence. Job advertisements for software developers fell by 8.5 percent compared to the previous year. Large IT companies such as Meta and Workday in particular are reducing their workforces[96]. At the same time, many new fields of activity are emerging in the field of IT and AI[97].

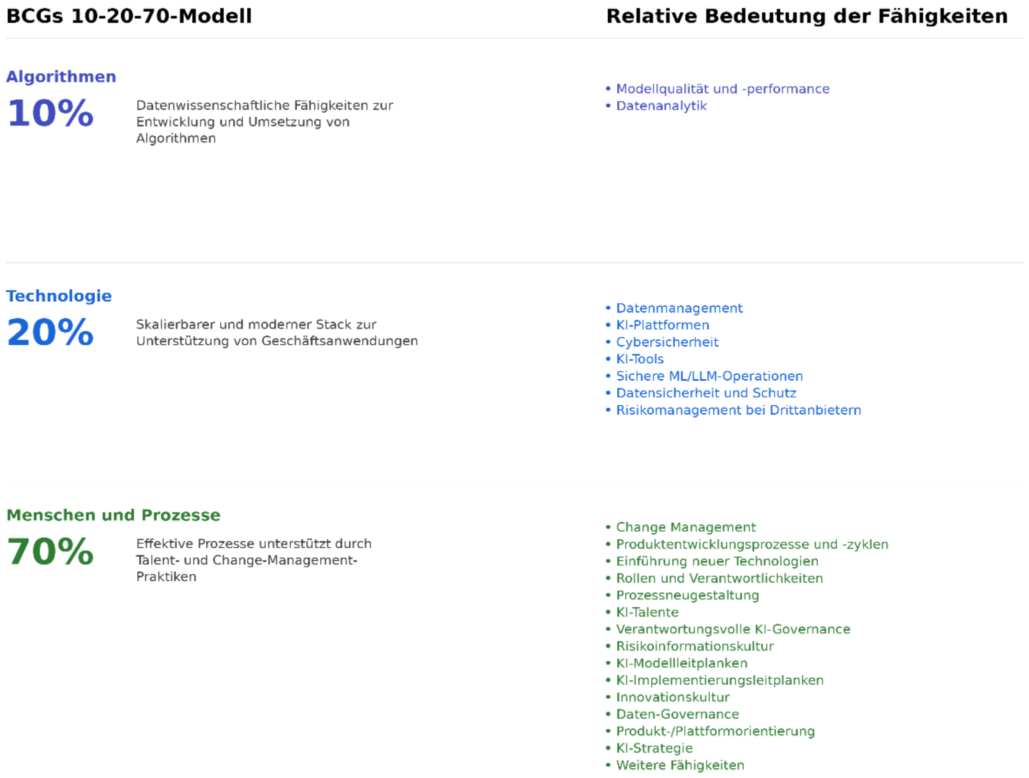
Skills required to manage IT (AI) transformation

According to the Boston Consulting Group*, the following figure shows* the percentage distribution of skills required between algorithms, technology, people and processes to meet the demands of IT (AI) transformation. *People and processes* take up the largest space here at 70%.

Executives, 2023, available at https://www.risknet.de/elibrary/paper/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/, accessed on 30.11.2025.

[96] Cf. *Linden*, Unemployment in the IT sector rises - also because of AI?, golem.de, 10.02.2025, available at https://www.golem.de/news/tech-branche-anstieg-der-arbeitslosenquote-im-zuge-der-ki-nutzung-2502-193189.html, accessed on 30.11.2025.

[97] Cf. *World Economic Forum,* The Future of Jobs Report 2025, 07.01.2025, available at https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf, accessed on 30.11.2025.



BCGs 10-20-70-Modell	Relative Bedeutung der Fähigkeiten
Algorithmen **10%** Datenwissenschaftliche Fähigkeiten zur Entwicklung und Umsetzung von Algorithmen	• Modellqualität und -performance • Datenanalytik
Technologie **20%** Skalierbarer und moderner Stack zur Unterstützung von Geschäftsanwendungen	• Datenmanagement • KI-Plattformen • Cybersicherheit • KI-Tools • Sichere ML/LLM-Operationen • Datensicherheit und Schutz • Risikomanagement bei Drittanbietern
Menschen und Prozesse **70%** Effektive Prozesse unterstützt durch Talent- und Change-Management-Praktiken	• Change Management • Produktentwicklungsprozesse und -zyklen • Einführung neuer Technologien • Rollen und Verantwortlichkeiten • Prozessneugestaltung • KI-Talente • Verantwortungsvolle KI-Governance • Risikoinformationskultur • KI-Modellleitplanken • KI-Implementierungsleitplanken • Innovationskultur • Daten-Governance • Produkt-/Plattformorientierung • KI-Strategie • Weitere Fähigkeiten

Figure 10: The "BCG 10-20-70 model"[98]

Education and training should not miss this megatrend. The activities to address these transformation requirements can be found *in the non-financial annual or sustainability reports* of more and more organizations.[99]

Governance means, not least, *successfully leading the organization and its people through the* transformation as part of an effective [100]change process, *despite scientifically proven "deliberate ignorance"* and typical human forces of inertia .

In times of hybrid war, **IT (AI) governance compliance is an essential *prerequisite for the defense capability of civilian and military organizations and systems*.**

[98] Based on *BCG*, Where is the value in AI, 2024, p.15, available online at: https://web-assets.bcg.com/a5/37/be4ddf26420e95aa7107a35aae8d/bcg-wheres-the-value-in-ai.pdf (accessed on 29.12.2025).

[99] *SGL Carbon*, CSR Report, 2024, pp. 41-42, available at https://www.sglcarbon.com/news/user-upload/SGL-Carbon-2023-CSR-Bericht-DE-22-03-2024-s.pdf, accessed on 30.11.2025.

[100] Cf. *Dörr*, Intentional Ignorance: On the Obstacles of Digital Transformation and Schrödinger's Cat, 13.01.2025, available at https://rsw.beck.de/aktuell/daily/meldung/detail/vorsaetzliche-ignoranz-justiz-behoerden-digitale-transformation-studie, accessed on 30.11.2025.

Prof. Dr. jur. Josef Scherer

Prof. Dr. jur. Josef Scherer is a lawyer and consultant, founder (2012) and head of the International Institute for Governance, Management, Risk and Compliance Management and head of the ESGRC staff unit at Deggendorf University of Applied Sciences (DIT). Since 1996 he has been Professor of Corporate Law (Compliance), Risk and Crisis Management, Restructuring and Insolvency Law at DIT. Previously, he worked as a public prosecutor at various regional courts and as a judge at the regional court in a civil chamber.

In addition to his work as a senior partner at the law firm Prof. Dr. Scherer & Partner mbB, which specializes in commercial law and governance, risk and compliance management (GRC), he prepares scientific legal opinions and acts as a judge in arbitration proceedings.

From 2001 to 2024, he also worked as an insolvency administrator in various district court districts.

Prof. Dr. Scherer works in various companies and corporations as a compliance ombudsperson or external compliance officer. He is a sought-after speaker at management training courses in well-known companies as well as in the continuing education program of the broadcaster BR-alpha and the Virtual University of Bavaria (VHB).

In cooperation with TÜV, he designed the part-time Master's degree program in Risk Management and Compliance Management at DIT, which has been renowned and accredited for over 15 years, and leads the certificate course "Sustainability and GRC" as well as the part-time Bachelor's degree in "Sustainability, Governance and Digitalization".

Since 2015, Prof. Dr. Scherer has been a member of the Advisory Board of the Institute for Risk Management and Regulation (FIRM), Frankfurt (www.firm.fm).

Since 2016, he has been a member of the DIN Standards Committee Services (Working Committee Human Resources Management NA 159-01-19 AA) for the development of ISO/DIN standards in human resources management and since 2017 a member of the delegation ISO TC 309 Governance of Organizations (Working Committee Governance and Compliance

NA 175-00-01-AA) for the development of ISO/DIN standards in the area of corporate governance, compliance and whistleblowing.

Since 2016, Prof. Dr. Scherer has been the technical director of the "User Group Sustainable Corporate Management (ESG/CSR/GRC) and Compliance" of Energieforen Leipzig, since 2018 he has been a member of Working Group 252.07 of Austrian Standards International for the development of an ÖNORM D 4900 et seq. (Risk Management System Standards) and since 2021 a member of DICO (German Institute for Compliance).

His research and practice focus on sustainability (ESG), integrated ESGRC management systems, manager liability, governance, risk and compliance management, integrated human workflow management systems and digitalization as well as contract, product liability, restructuring and insolvency law, employment law and human resources management.

In the field of applied research and solutions / tools in the field of ESG/GRC, digitization and integrated workflow management systems, Prof. Dr. Scherer is a shareholder-managing director of Governance-Solutions GmbH and a member of the supervisory board of various companies and foundations.

www.scherer-grc.net

Linkedin: Prof. Dr. Josef Scherer
The author regularly publishes current rulings, laws, articles, etc. on ESGRC topics via LinkedIn.

Fabian Pothorn

Fabian Pothorn studied administrative informatics (Diplom-Verwaltungswirt (FH)) and then risk and compliance management (M.A.). Since 2024, he has been the information security officer at Deggendorf University of Applied Sciences.

Fabian Pothorn is a lecturer in the fields of information security, business continuity management, AI management and process management.
In addition, he works as a management consultant and supports organizations in setting up and optimizing IT governance and information security management systems.