FIRM
Frankfurter Institut für
Risikomanagement und Regulierung

IT (AI) governance compliance for managing the top risks in 2026 and for defense capability

Authors

Prof. Dr. Josef Scherer
Fabian Pothorn

The current situation in times of multiple crises, various transformations due to numerous megatrends [see Zukunftsinstitut 2025] and numerous armed conflicts is full of risks, as the *Global Risks Report 2026* [see World Economic Forum 2026], *CEO's Annual Survey 2026* [see PwC 2026] or the *Allianz Risk Barometer 2026* [see Allianz 2026] show almost unanimously. - Many new opportunities are the flip side of this coin if the so-called future skills [see Zukunftsinstitut 2025] are developed at an early stage.

According to the *Allianz Risk Barometer 2026*, *cyber risks, business continuity, regulation and AI* are in the top four positions.

Quote: "(...) *In Germany, cyber attacks and business interruption remain in 1st and 2nd place - in view of political and regulatory uncertainties, changes in legislation and regulation jump to 3rd place, while AI risks now enter the ranking in 4th place.* (...)" [Allianz 2026].

Obligations arising from IT/AI governance compliance

In connection with stricter regulation, the risks of disputes over D&O and cyber risks insurance policies [see Scherer, Seehaus 2025, p.1515 ff. and Scherer, Seehaus 2026] and cyber compliance in the supply chain [see Beck 2025] are also growing.

As the hybrid war on the part of various nations against Germany and Europe is no longer merely a "threat", but an actual event [cf. Federal Office of Civil Protection and Disaster Assistance 2025], the following statements are also a *contribution to the military and defence capabilities of organizations and nations*.

Numerous IT incidents with high amounts of damage show that board members, managing directors, CISOs, CIOs, information security officers, supervisory bodies, auditors, lines-of-defense functions, auditors and certifiers do not always take the decisive measures. The current case law of the Higher Regional Court of Frankfurt and the Federal Court of Justice on the denial of D&O insurance cover in the event of intentional breach of duty will also become relevant in the future in the event of breaches of the mostly neglected legal obligations arising from IT/CI governance compliance [see Scherer, Seehaus 2026].

Consistent compliance with IT and AI governance is therefore essential. An integrated IT/AI governance management system supports managers and employees in complying with legal and technical requirements through clear organizational structures and processes. The relevant standards - DIN ISO 37000 (governance of organizations), ISO 38500 (IT gov-

ernance), ISO 42001 (AI management), DIN ISO 22301 (business continuity management), DIN ISO 22361 (crisis management guidelines) and DIN ISO 27001 (information security management) - supplement the legal requirements and create the basis for an effective compliance framework.

1. Digital literacy, legal basis and objectives

There is no statutory definition for ”IT or AI governance”. Instead, the terms must be derived from the relevant legal provisions, the state of the art and recognized standards, whereby the Federal Constitutional Court defined the terms ”recognized rules of technology” and ”state of the art” in the Kalkar decision [see Scherer, Fruth 2019]. In legal terms, IT and AI governance can be described as the ”sustainable, compliance- and risk-based, conscientious management and monitoring of organizations, including interaction with relevant stakeholders in the IT (AI) sector” [cf. Scherer 2025, pp. 16, 169].

The integrated IT/KI governance management system comprises compliance and risk management, strategy, planning, divisional organization and processes, implementation, internal control system (ICS), auditing, controlling, reporting, IT (service) management, IT security and information security management, data protection, digitalization including AI, social engineering and supply chain management.

AI governance is a sub-area of IT governance, which in turn is embedded in higher-level corporate governance. These structures must not be organized as isolated ”silos”. Compliance forms the basis, meaning that the implementation of an integrated management system first requires the fulfillment of all legal requirements (e.g. Sections 43 GmbHG 93, 116 AktG, 130 AktG, 30 OWiG etc.) [see Scherer 2022, Chapter 1] and compliance with the state of the art [see Scherer, Fruth 2019].

Courts have confirmed the obligation to maintain risk and compliance management systems and internal control systems [see Munich Regional Court I 2013 and Nuremberg Higher Regional Court 2022]. Failure to do so is considered a breach of organizational duties, while implemented systems have a discharging effect according to supreme court rulings (BGH, ECJ) [see Scherer, Seehaus 2025, p. 1515 et seq.]

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

In order to record, evaluate and control the legal requirements in IT/AI governance compliance management, a process-related legal register must be created and maintained on an ongoing basis. The requirements should be translated into comprehensible formulations and implemented in the organizational and operational structure so that the governance system is seamlessly linked to compliance management in accordance with DIN ISO 37301 [see Scherer 2022, section 4.5].

In November 2025, the EU presented the ”Digital Omnibus for Data Protection and AI”, which aims to reduce the regulatory burden [see KPMG 2025].

Modern tools enable the real-time recording and implementation of new or amended regulations - a procedure that corresponds to the current state of the art.

3. IT (AI) governance *compliance* risk management

The IT (AI) governance compliance risk management process [see Scherer 2025, Chapter 4.6] is used for the early identification, assessment and management of threats and opportunities that could influence the achievement of an organization's objectives. A business continuity management system is required for relevant residual risks that cannot be controlled [see Scherer 2025, p.180].

Regulated organizations in particular, which fall under the regulations of the new BSIG (amended by the NIS2 Implementation Act) or the Digital Operational Resilience Act (DORA), have special requirements for IT governance risk management.

4. New roles and responsibilities

As part of the ongoing trend of increasing digitalization, many new roles are emerging that organizations need to consider. In particular, AI management is increasingly being integrated into the area of IT. The transitions are fluid and therefore closely interwoven with IT governance.

In addition to the "classic" roles, such as Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Risk Officer (CRO), IT Administrator, Programmer, etc., new roles and job profiles are currently emerging.

These include, for example, AI Architects, Chief AI Officers (CAIO), AI Risk Managers, Prompt Engineers and many more [cf. Gartner 2024].

5. Operations - operationalization of IT governance compliance and process management

All elements of the (IT/AI) governance management system must be integrated into the operational processes. ISO/IEC 20000-1:2018 defines central process topic areas for this, which are taken up by best practice standards such as COBIT, ITIL or FitSM [see Pilorget 2025, p. 38 ff.] In ITIL 4, 34 process topic areas are described, with the focus shifting from specific processes to process-related requirements and KPIs - an approach that enables individual process design and better IT-business alignment.

Implementation primarily takes place in the "first line" (IT department). Without a functioning IT service management system (e.g. in accordance with ITIL, FitSM or ISO 20000), it is not possible to establish an effective management system structure for the second line (e.g. information security, business continuity, AI management). The strength of the interaction between IT service management and these management systems varies depending on the size and scope of the IT department.

6. Monitoring and evaluation

The IT/AI governance management system is primarily monitored internally by bundled functions - controlling, compliance, risk, ISM, BCM, KIM, ICS and internal audit - according to the "three lines of defense" principle, but can also be supplemented externally by the supervisory board, authorities or second/third party audits. ISO/IEC 27004:2016 provides suitable KPIs and measurement methods for the ISMS, while ISO 42001:2023 (Annex B) provides corresponding KPI topic areas for the evaluation of AI management systems.

7. outlook

The requirements to be derived from IT/AI governance may seem overwhelming at first, but they are not. If IT/AI governance is correctly embedded in corporate governance and thus in the integrated management system (IMS), there are numerous overlaps with existing IMS elements and the tasks can be distributed across several shoulders. At the same time, a compliance management system that removes liability is essential in order to avoid personal liability risks [see Scherer 2023].

New technological developments require new skills. According to the Boston Consulting Group, companies need algorithms, technology, people and processes - with people and processes accounting for the largest share at 70% [see BCG 2024, p. 15]. Education and training must address this megatrend. The corresponding transformation activities can increasingly be found in non-financial business and sustainability reports [see SGL Carbon 2024, p. 41-42].

Last but not least, governance means successfully leading the organization and its people through the transformation as part of an effective change process despite scientifically proven ”wilful ignorance” [cf. Dörr 2025] and typical human inertia.

In times of hybrid warfare, IT/AI governance compliance is ultimately an essential prerequisite for the defence capability of civilian and military organizations and systems.

Sources

[Zukunftsinstitut 2025] Zukunftsinstitut [2025]: The Future of Work megatrend, 01.01.2025, available at: https://www.zukunftsinstitut.de/zukunftsthemen/megatrend-future-of-work accessed on 25.01.2026.

[World Economic Forum 2026] World Economic Forum [2026]: Global Risks Report 2026, 14.01.2026, available at: https://www.weforum.org/publications/global-risks-report-2026/ accessed on 25.01.2026.

[PwC 2026] PwC [2026]: PwC's 29th Global CEO Survey, 19.01.2026, available at: https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html accessed on 25.01.2026.

[Allianz 2026] Alliance Commercial [2026]: Allianz Risk Barometer 2026, 14.01.2026, available at: https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026/de.html accessed on 25.01.2026.

[Scherer, Seehaus 2025] Scherer, J. and Seehaus, S. [2025]: Duty of governance with early risk detection, resilience and transformation as a cardinal duty of boards and executives, ZInsO 2025.

[Scherer, Seehaus 2026] Scherer, J. and Seehaus, S. [2026]: Manager liability, D&O insurance and early risk detection in the light of current case law.

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

[Federal Office of Civil Protection and Disaster Assistance 2025] Federal Office of Civil Protection and Disaster Assistance [2025], Hybride Bedrohungen, available online at: https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen accessed on 13.12.2025.

[Scherer, Fruth 2019] Scherer, J. and Fruth, K. [2019]: Technik-Governance, special publication of the German Association of Compliance Managers.

[Scherer 2022] Scherer, J. [2022]: Successfully implementing, integrating, auditing and certifying a compliance management system according to DIN ISO 37301:2021, DIN Media, 2022.

[Scherer 2025] Scherer, J.: Sustainable management and monitoring of organizations (governance) according to DIN ISO 37000, DIN Media, 2025.

[LG Munich I 2013] LG Munich I [2013]: Judgment of 10.12.2013, (Ref. 5 HK O 1387/10 - "Neubürger").

[OLG Nuremberg 2022] OLG Nuremberg [2022]: Judgment of 30.03.2022, (Ref. 12 U 1520/19 - "Gas station tenant").

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

[Gartner 2024] Gartner [2024]: *AI Is Creating New Roles and Skills in Data & Analytics*, 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).

[Pilorget 2025] Pilorget, L. [2025]: Managing IT in a digital world, Springer Vieweg.

[Scherer 2023] Scherer, J. [2023]: AI responsibility and liability-reducing effect of an AI compliance management system for management (board of directors, managing directors, officers), supervisory body and other executives, available at https://www.risknet.de/elibrary/paper/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/ accessed on 30.11.2025.

[SGL Carbon 2024] SGL Carbon [2024]: CSR report, available online at https://www.sglcarbon.com/news/user-upload/SGL-Carbon-2023-CSR-Bericht-DE-22-03-2024-s.pdf accessed on 25.01.2026.

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

[Dörr 2025] Dörr, S. [2025]: Willful Ignorance: On the Obstacles of Digital Transformation and Schrödinger's Cat, available online at: https://rsw.beck.de/aktuell/daily/meldung/detail/vorsaetzliche-ignoranz-justiz-behoerden-digitale-transformation-studie accessed on 25.01.2026.

Authors

Prof. Dr. Josef Scherer
Member of the Advisory Board
Deggendorf Institute of Technology

Fabian Pothorn
Information Security Officer
Deggendorf Institute of Technology

Scan to read online
https://firm.fm/?p=11099