ISSN 2568-6380 Item no. 7465531

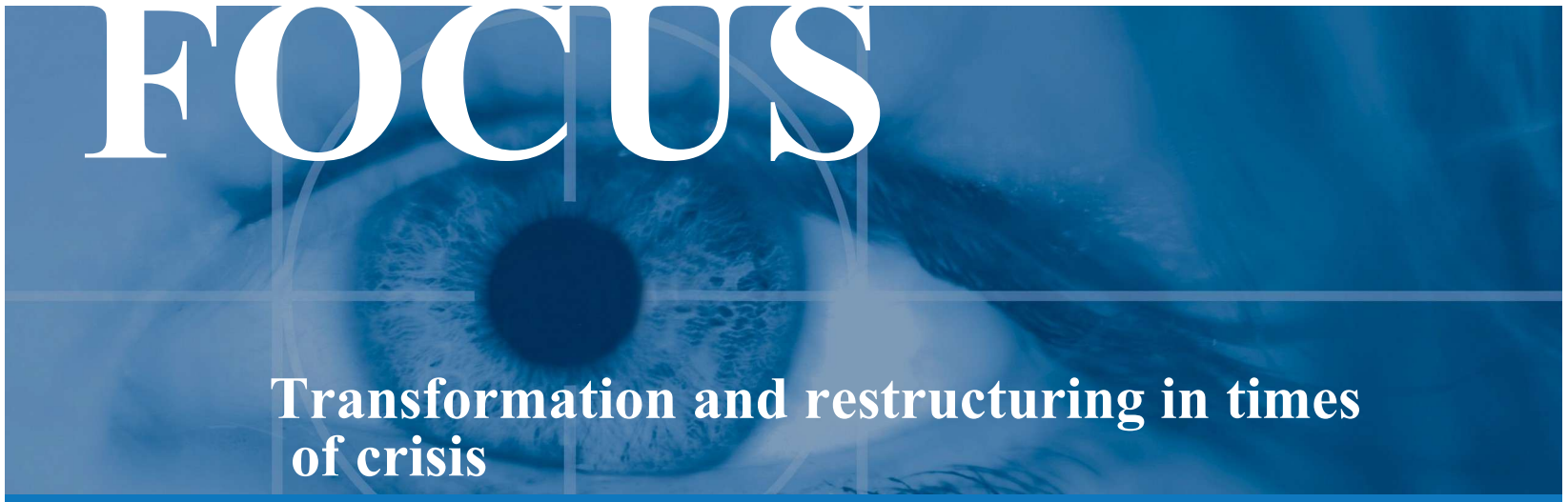
ZInsO 31

Journal for all aspects of insolvency and restructuring law

July 31, 2025

28th year · Pages 1489 to 1548

FOCUS



Transformation and restructuring in times of crisis

Josef Scherer/Sascha Seehaus

Governance obligation with early risk detection, resilience, and transformation as a cardinal duty of executive bodies and managers

Wolters Kluwer

Duty of governance with early risk detection, resilience, and transformation as a cardinal duty of executive bodies and managers[1]

Managing directors,[2] board members, supervisory board members, and executives are "sailing blindly into liability and insurance losses"[3]

by Professor Dr. Josef Scherer, Deggendorf* and Dr. Sascha Seehaus, Diez**

In times of multiple crises and transformation, managing directors, board members, supervisory board members, auditors, compliance and risk managers, ICS officers (and other lines of defense functions) often pay too little attention to the things that really matter. The current situation harbors great dangers and opportunities. Identifying and assessing these appropriately and deriving appropriate transformation measures to secure the long-term existence and resilience of the organization[4] is one of the essential governance duties that are often unknown or neglected. This frequently causes financial damage to the organizations concerned, often puts them in avoidable existential difficulties, and in most cases constitutes liable mismanagement[5].

In addition to the proven drastic increase in personal liability risk, there is a threat of loss of insurance coverage for managers due to the accumulation of "breach of cardinal duties" accepted by current case law and the resulting indication of "known breach of duty".

An examination of the annual reports of organizations often indicates major shortcomings in governance, risk, and compliance, i.e., economic sustainability. For example, there is still generally little understanding among the executive bodies (managing directors, executive board, supervisory bodies) and "lines of defense" regarding the content of so-called "cardinal duties" and "Risk-based governance compliance," even though this currently represents the top risk for almost all organizations. If the management body delegates leadership and monitoring (governance) in the area of resilience and transformation, the delegates are not effective, the question arises as to how to distinguish between faulty delegation and excessive employee involvement.

The following discussion highlights the role of the bodies, the "lines of defense" functions, including auditors and certifiers,[8] who, on the one hand, have to justify themselves when problems arise within their scope or audit area.

On the other hand, it shows that, conversely, "good, risk-based audits" can make an enormous contribution to resilience in difficult times.

It is not without reason that "governance" stands for economic sustainability in the sustainability acronym ESG. This, in turn, is a prerequisite for being able to operate in a socially and ecologically sustainable manner: "No money, no honey."[9]

---

* Prof. *Dr. Josef Scherer* is the founder and partner of the law firm Prof. Dr. Scherer & Partner mbB, which focuses on commercial law, compliance, risk, and governance. Since 1996, he has been teaching corporate law, risk and compliance management at the Deggendorf Institute of Technology. Prior to that, he was a public prosecutor and civil judge. As managing director of Governance Solutions GmbH, he supports companies in the digitalization and legally compliant design of their organizational and management systems.

** *Dr. Sascha Seehaus* is a specialist lawyer for insolvency and restructuring law, a certified ESGRC manager, and holds a master's degree in risk and compliance management (M.A.). He supports entrepreneurs in transformation and transition phases with a particular focus on sustainable corporate management, strategic restructuring, liability-avoiding management organization, and effective personnel and receivables management.

1 Note: Parts of this article correspond to the article *Scherer*: Kardinalpflicht fordert „risikobasierten Ansatz" (Cardinal duty requires a risk-based approach), published on RiskNET, available at: *https://www.risknet.de/themen/risknews/kardinalpflicht-fordert-risikobasierten-ansatz/.*

2 Gender note: Where specific gender forms are used in this article, they always refer to both genders.

3 Slightly modified quote from: OLG Frankfurt/M., decision of January 16, 2025 – 7 W 20/24, NJW-RR 2025, 731: "blindly sailing into crisis"; See also OLG Frankfurt/M., judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917, with a similar case (appeal lodged, BGH – IV ZR 66/25).

4 See ISO 37000:2021-09 "Governance of Organizations," chap. 6.11 "Viability and performance over time."

5 See *Scherer*, What interests investors: Antifragility and the Achilles heel of the prudent businessman, 2019, available at: *https://www.scherer-grc. net/publikationen/das-interessiert-kapitalgeber-antifragilitaet-und-der-achilleskoerper-des-ordentlichen-kaufmanns*.

6 Higher Regional Court of Frankfurt/Main, decision of January 16, 2025 – 7 W 20/24, NJW-RR 2025, 731: "blindly sailing into the crisis" and Higher Regional Court of Frankfurt/Main, judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917, with a similar case (appeal lodged, BGH – IV ZR 66/25).

7 According to the latest rulings of the Higher Regional Court of Frankfurt/Main (OLG Frankfurt/M., decision of January 16, 2025 – 7 W 20/24, NJW-RR 2025, 731; OLG Frankfurt/M., judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917) "*fundamental professional duties, knowledge of which can be assumed to be possessed by every member of the profession based on life experience*." Current case law (see above) has also established *cardinal duties in the context of governance (*conscientious management and supervision of organizations). Various case groups have already emerged in case law. Current case law now extends these case groups to the "*diverse duties relating to corporate management that are associated with registration as a managing director of a corporation*." *Governance compliance* is therefore rightly regarded as a fundamental professional duty of a managing director or board member.

8 Auditors work, for example, as internal auditors (see ISO Harmonized Structure Standard Section 9.2), third-party auditors, or auditors of external certification bodies.

9 Bavarian proverb.

I. Current situation: Best, real, and worst-case scenarios – urgent action required

1. Escalation of the risk situation in times of multiple transformations

The global geopolitical, economic, and ecological crises in times of fundamental transformation (technological, demographic, ecological, social, regulatory) are gradually coming to a head.

Appropriate risk management, including early risk detection[10], must also take worst-case scenarios into account, quantify and aggregate all risks appropriately, manage them and balance them against risk-bearing capacity (11).

2. Relevant empirical findings: Insolvency risks and risk perception

a) Increased probability of insolvency across the economy

According to a recent study on the financial situation of companies in Germany, approximately 318,000 companies, or one in ten, currently have an increased risk of insolvency.

However, insolvency figures had already risen to record levels before Trump's tariff capers. [13]

b) Risk awareness exists in capital market-oriented companies

A recent analysis[14] of the annual reports of the 134 largest German DAX, M-DAX, and S-DAX companies points to a huge increase in risks. The number of risks identified in the annual reports rose by 30% compared to 2023. In each case, 98% of risk reports cite *regulatory changes* and *cyber incidents* as the top risks, followed by *geopolitical developments, financial issues, competition*, and *legal and compliance issues.*

c) Credibility deficit due to communication gap at top management level

While risk reports have never before identified so many risks and threats at the same time, over 40% of CEO forewords make no mention of them. This undermines the credibility of the governance function. CEOs are thus failing in their leadership responsibilities.

3. Lack of risk orientation in management and supervision

a) Ignorance of realistic crisis scenarios

Although even the head of the Ifo Institute now considers a global economic crisis possible,[16] the current pressure to act has apparently not yet reached managing directors, board members, and supervisors (supervisory boards, auditors, lines of defense with internal audit, risk and compliance management, etc.), nor the various types of *auditors*.

Worst-case scenarios are often ignored, either deliberately or out of ignorance. [17]

b) Misguided use of resources and behavioral economic barriers

Instead, dwindling resources are often not pooled for important things, but spent on pure bureaucracy without adding any value.

This may have behavioral economic reasons, but it is often also due to the fact that, on the one hand, regulations such as Section 1 StaRUG (duty to identify risks at an early stage) or Section 93 (1) sentence 2 AktG (Business Judgment Rule) are not sufficiently known or understood by supervisory boards, executive boards, and management.
Section 93 (1) sentence 2 AktG (business judgment rule) are not adequately known or understood.

c) Knowledge gaps and lack of GRC expertise

There is often a lack of genuine governance, risk, and compliance expertise, and GRC experts are often not consulted or taken seriously when intuitive decisions are made by the governing bodies. [20] Instead, they are kept busy with operational tasks such as training and bureaucratic reporting.[21]

---

10 For more details, see *Scherer/Seehaus*, Governance and Compliance according to § 1 StaRUG, 2024, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*, and *Romeike,* IDW ES 16 – Early crisis detection and crisis management pursuant to Section 1 StaRUG, 2025, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-krisenmanagement-nach-1-starug/.*

11 See *Scherer/Romeike/Gursky*, Mehr Risikokompetenz für eine neue Welt (More risk competence for a new world), RiskNET.de, 2021, available at: *https://www.risknet.de/themen/risknews/ mehr-risikokompetenz-fuer-eine-neue-welt/* and *Pätzold*, ZInsO 2025, 605 ff.

12 See CRIF, One in ten companies in Germany is at risk of insolvency, 2025, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/ jedes-zehnte-unternehmen-in-deutschland-ist-insolvenzgefaehrdet/*.

13 See Tagesschau, "Number of insolvencies continues to rise," March 14, 2025, available at: *https://www.tagesschau.de/wirtschaft/insolvenzen-anstieg-100.html*.

14 See *Romeike*, What risk reports say – and what management boards conceal, 2025, with reference to Crunchtime Risk Monitor 2025, available at: *https://www.risknet.de/themen/risknews/was-risikoberichte-sagen-und-vorstaende-verschweigen/*.

15 See *i*bid.

16 See n-tv, Ifo chief considers new global economic crisis possible, ntv news, April 12, 2025, available at: *https://www.n-tv.de/wirtschaft/Ifo-Chef-haelt-neue-Weltwirtschaftskrise-fuer-moeglich-article25699556.html*.

17 See *Scherer/Romeike/Gursky*, Mehr Risikokompetenz für eine neue Welt (More risk competence for a new world), RiskNET.de, 2021, available at: *https://www.risknet.de/themen/risknews/* mehr-*risiko*kompetenz-fuer-e*ine*-neue-welt/.

18 See *Scherer*, Investing in governance in light of Basel IV and ratings, RiskNET.de, 2025, available at: *https://www.risknet.de/themen/risknews/* der-weg-zu-resilienz-und-rentabilitaet/.

19 See *i*bid.

20 Example: Appropriate business judgment rule opinions are often lacking *before* relevant decisions are made. Bayer is still suffering from the purchase of Monsanto while US product compliance proceedings are ongoing.

21 E.g., the LKSG report, which the BAFA did not seriously demand or sanction for not being submitted.

a) Inadequate implementation of the risk-based approach

The "*risk-based* approach," which involves prioritizing important issues based on an appropriate risk assessment, is also not well known or practiced:

The primary focus should be on avoiding danger to life and limb or personal sanctions against employees or third parties, as well as significant financial losses that impair risk-bearing capacity.

4. Conclusion: Strategic focus urgently needed

"*In challenging times, it is important to focus on the important issues. (...) A lot of management time and resources are still being spent on issues whose strategic relevance is questionable, at best*"[22]

II. Doing the important things right: Examples of things that tie up a lot of resources but deliver little value

Sustainability and data protection are, of course, very important. But here, too, the "risk-based approach" applies.

1. Example: Sustainability reporting and the Supply Chain Due Diligence Act

After years of high resource consumption, SMEs have now prepared for reporting with CSRD, ESRS, taxonomy, CSDDD, etc., the EU and the new coalition have recognized that a great deal of bureaucracy, redundancies, and analogies had crept into the regulation of existentially important sustainability issues and are now steering back with ESG omnibus packages and the abolition of LKSG. [23]

Nothing has been achieved except unpredictability, costs, bureaucracy, uncertainty, and annoyance among SMEs.

2. Example: Data protection and deletion of important documents

Since 2018, with the GDPR and the often-hysterical implementation of data protection measures involving the premature deletion of documents, a great deal of information has been lost that would subsequently be needed as exonerating or positive documentation for contractual partners, authorities, or courts.

In addition to complex tax regulations that cannot be avoided[24], there are numerous other bureaucratic monsters that small and medium-sized businesses have to endure.

III. Examples of cases in which risk management, but possibly also supervisory bodies, auditors, and lines of defense, including various auditors, may have failed

1. BayWa AG case: balance sheet audit, failure to provide information, and audit failure

On November 11, 2024, the media reported that Bafin had ordered an audit of BayWa's balance sheet. There were concrete indications of violations of accounting regulations. The presentation of the financial position and risks arising from the Group's financing was possibly incorrect. The international auditing firm PricewaterhouseCoopers (PwC) has audited the annual report. In its unqualified audit opinion on the 2023 annual report, PwC refrained from commenting on the company's strained financial situation, which had been known for some time. According to press reports, approximately €1 billion in fresh money had been provided in the meantime. [25]

2. Further cases: Wirecard, Helma AG, Creditshelf AG, and many more.

According to widely held opinion, it was not only at Wirecard where all supervisory mechanisms failed miserably. [26]

In the case of the insolvent companies Helma AG and Creditshelf AG, a subsequent review of the annual report concluded that, under certain circumstances, the "*statutory minimum requirements for the risk and early warning system had not been implemented*." [27]

"It is alarming that these are still not being audited by the auditors who follow IDW PS 340. The management board and supervisory boards should be aware of this, because it means that the audit is of little use. (...) it should be noted that the obligation to have an effective crisis and risk early warning system is incumbent on the management board and supervisory board and also holds the supervisory board liable in this regard."[28]

---

22 Quote from *Gleißner/Weissmann*, The strategic challenges facing German companies, Die Deutsche Wirtschaft, 2024, available at: *https://futurevalue.de/wp-content/uploads/2024/12/FA-2344-Strategische-Herausforderungen-deutscher-Unternehmen-2024.pdf.*

23 See *Scherer*, CSRD Implementation: What the Delay Means for SMEs, Lexware 2025, available at: *https://www.lexware.de/wissen/nachhaltigkeit/ c*srd-umsetzung/.

24 For liability limitation reasons, it is advisable to implement a tax compliance management system in accordance with Section 153 of the German Fiscal Code (AO).

25 See faz.net, Audit of Baywa's consolidated financial statements, available at: *https://www.faz.net/aktuell/wirtschaft/bafin-ordnet-pruefung-des-konzernabschlusses-von-agrarkonzern-baywa-an-110105059.html.*

26 See *Gleißner*, Wirecard: Weaknesses in risk management and auditing, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/ wirecard-schwaechen-bei-risikomanagement-und-abschlusspruefung/* and *Glaser*, And every day we hear about ... Wirecard!, available at: *https://www.risknet.de/ themen/risknews/und-taeglich-gruesst-wirecard/.*

27 See *Gleißner/Wolfrum*, ZfRM 2024, 116, 118.

28 See *Gleißner/Wolfrum*, ZfRM 2024, 116, 118.

3. Empirical shortcomings in annual reports and the role of supervisory boards

An examination of the information on risk management in the annual reports of German DAX and MDAX companies concludes that the requirements under
Section 1 StaRUG and FISG are hardly being observed. 83 annual reports evaluated according to various criteria achieved an average ~37% of the possible points:[29]

"Many management boards seem to be concerned only with what the auditor wants to see and not with aspects that are economically important and even required by law. There is a great need for action.

Supervisory boards are particularly called upon to act, as they are directly addressed in Section 1 Sta-RUG and Section 107 AktG and could also incur personal liability risks (...)" [30]

4. Systemic criticism of the role, structure, and independence of auditors

The world of supervisors [31] ppears unable, despite the high level of resources deployed, to effectively control and monitor the things that really matter. The role of auditors as an independent body responsible for ensuring the reliability of company financial statements is coming under increasing pressure. Cases such as that of BayWa AG, where the company's economic difficulties were inadequately reflected over a long period of time, once again raise questions about risk perception and the independence of auditors. Critics complain of structural proximity to the audited companies and economic dependencies that could impair the objective quality of the audit.

Quote: [32]

"(...) Pursuant to Section 317 of the German Commercial Code (HGB) and the principles of proper auditing (IDW PS 200 ff.), auditors are required to conduct risk-based audits. This means that, particularly in the case of companies with tight balance sheet ratios and increased risks to their continued existence, the risk management system must be the focus of the audit as a central element of a going concern assessment. (...)

Particularly in a group such as BayWa, which is highly dependent on external factors such as raw material prices,

interest rates or regulatory changes, such a simplistic view of risk is grossly negligent and leads to complete risk blindness. A simplistic view of risk is grossly negligent and leads to complete risk blindness.

It is therefore all the more irritating that auditors accept such a statement in the risk report. Unfortunately, BayWa (PWC) is no exception here.

This also applies to Wirecard (Ernst & Young), Lehman Brothers (Ernst & Young), Gerry Weber International (Ebner Stolz), Thomas Cook (Ernst & Young), Prokon Regenerative Energien (BDO), Luckin Coffee (Ernst & Young), Schlecker Drogeriemärkte (Grant Thornton, formerly Baker Tilly Roelfs), NMC Health (Ernst & Young), Greensill Capital (Grant Thornton), Carillion (KPMG), Steinhoff (Deloitte), Hypo Alpe Adria/HETA (KPMG) and many other corporate crises and bankruptcies, where the auditors were flying completely blind. (...)"

Michel Barnier, former EU Commissioner for Internal Market and Services, had already initiated ambitious reforms in the wake of the financial crisis to strengthen the independence of auditors.[33] Among other things, these included a strict separation of auditing and consulting, mandatory rotation of audit firms, and measures to promote competition in the highly concentrated audit market. However, many of these proposals were watered down or weakened in the further legislative process, partly due to considerable resistance from major market players and national interests.

The result is a regulatory framework that in practice is not sufficiently effective in preventing systemic conflicts of interest. The debate on reforming auditing therefore remains relevant, especially against the backdrop of growing demands for transparency, sustainability, and risk management in companies.

Note:

In the meantime, the Institute of German Auditors [IDW] *has published IDW ES 16 on the audit of the implementation of the requirements of Section 1 StaRUG. This draft still contains numerous weaknesses and falls significantly short of the requirements of the legislator and DIIR No. 2.*

From a legal perspective, it should be noted that the responsibility of the executive bodies (managing directors/executive board/supervisory board, etc.) and senior executives within the meaning of Section 9 (2) OWiG for legally compliant and appropriate risk and crisis early warning is primarily governed by law (e.g., Section 1 StaRUG, Section 91 (2) and (3) AktG, Section 43 GmbHG, Sections 93, 116, 107 AktG), case law, and the "recognized rules of technology," and that standards of private (professional) organizations such as IDW, DIIR, and DIN are only legally relevant if they reflect the requirements of these sources.

The task and responsibility of auditors with regard to their audit of risk or early crisis detection is also primarily based on

29 See *Jungesblut*, Corporate Finance, 2024, 274.

30 See *Jungesblut*, Corporate Finance, 2024, 274, 280 (quote).

31 See *Scherer*, FIRM Yearbook 2017, 79, available at: *https://www.gmrc.de/images/Docs/Publikationen/Scherer_Die_Welt_en_der_Ueberwacher.pdf*.

32 See *Romeike*, The Expectation Value Fallacy – Self-Deception in BayWa's Risk Report, 2025, RiskNET.de, available at: *https://www.risknet.de/themen/risknews*/der-erwart*ungswert*-irrtum/.

33 See *Romeike/Hager*, Financial crisis exposes weaknesses among auditors, *available at: https://www.risknet.de/themen/risknews/finanzkrise-legt-schwaechen-bei-wirtschaftspruefern-offen/*.

34 See *Romeike*, IDW ES 16 – Early crisis detection and crisis management pursuant to Section 1 StaRUG, 2025, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und-*krisen*management-nach-1*-starug/.

Requirements arising from legislation (e.g., HGB) and case law, and not from "instructions for use" or auditing standards prescribed by their own professional association, insofar as these contain a negative in this regard. It should be a concern of the profession to be supported only by auditing standards of the professional association that comply with legislation, case law, and recognized rules of technology. Ignorance of the legal situation with reference to compliance with a standard that lags behind the legal situation would not exculpate auditors.

Unfortunately, only sporadic and not necessarily prominent references to current requirements arising from legislation, case law, and recognized technical rules always take precedence over the contents of the standards and must be observed can be found in DIN and IDW standards.

IV. Important examples: Risks in governance, early risk detection, IT with AI

1. Current global risk situation and cyber threat scenarios

Due to developments in artificial intelligence (AI), the number one medium-term risk in the Global Risks Report 2024 was "disinformation and manipulation."[35]

Cyber risks ranked first among the biggest concerns of CEOs worldwide. [36] These risk assessments have hardly changed in 2025. [37]

The continuing escalation of cyber threats, including potential threats from the use of artificial intelligence, is the dominant concern for most companies/organizations. In connection with the associated tightening of regulations, the risks of disputes over insurance policies and cyber compliance along the value chain are growing.

2. Governance and risk requirements in the context of regulatory uncertainty

The expanding and diverse risk landscape – including outside IT and AI – requires the highest level of timeliness and quality in early risk detection and management as well as *governance, i.e., the "sustainable compliance- and risk-based, conscientious management and monitoring of organizations*." [38]

The fact that there is a lack of legal definitions and therefore uncertainty regarding the definition, content, and specific requirements of governance in science and practice makes it even more difficult to meet governance compliance requirements.

As a result, the above-mentioned responsible parties, including auditors, interpret the requirements arbitrarily and differently, which, as will be shown below, leads to disastrous results.

Those responsible for management systems (occupational safety, environmental, information security, quality, sustainability, energy efficiency, etc.), along with their auditors and certifiers, should have realized long ago that appropriate compliance and risk management is also a primary and indispensable requirement for the systems they oversee.

3. Risk understanding and the need for action in organizations

As a rule, it is not individual risks that threaten the existence of a company, but rather the cumulative effect of many individual risks; therefore, a methodologically sound aggregation of risks is important. [39]

4. Interim conclusion on governance competence

In order to ensure resilience in organizations, the necessary governance competencies that are currently lacking among managers and their supervisors should be brought up to an appropriate level in a timely manner and then implemented, controlled, and monitored accordingly.

V. Governance compliance

1. Concept and system of governance

Governance can be legally defined as the "*sustainable, compliance- and risk-based, conscientious management and monitoring of organizations, including interaction with relevant* stakeholders."

The governance compliance management system is a structural and procedural organization consisting of components (e.g., roles, objectives, resources, processes, delegations, and interactions, etc.) with the purpose of supporting an organization in decision-making, setting objectives and planning, implementation, control, and monitoring to achieve *mandatory and optional goals in the area of governance*.

35 See WEF, Global Risks Report 2024, available at: *https://www.weforum.org/publications/global-risks-report-2024/*.

36 See PWC, CEOs' Global Survey 2024, available at: *https://www.pwc.de/de/ceosurvey.html*.

37 See WEF, Global Risks Report 2025, available at: *https://www.weforum.org/publications/global-risks-report-2025/* and PWC, CEOs' Global Survey 2025, available at: *https://www.pwc.de/de/ceosurvey.html*.

38 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) According to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Chapter Introduction.

39 See *Romeike*, Qualitative Methods for Risk Aggregation Are a Fiction, 2019, available at: *https://www.risknet.de/themen/risknews/qualitative-methoden-zur-risikoaggregation-sind-eine-fiktion/* and *Romeike*, Risk Aggregation Becomes Mandatory, 2025, available at: *https://www.risknet.de/themen/risknews/risikoaggregation-wird-zur-pflicht/* and *Scherer,* Sustainable management and monitoring of organizations (governance) according to DIN ISO 37000 – successful implementation, auditing, and reporting, DIN Media, 2025, Chapter 6.9.

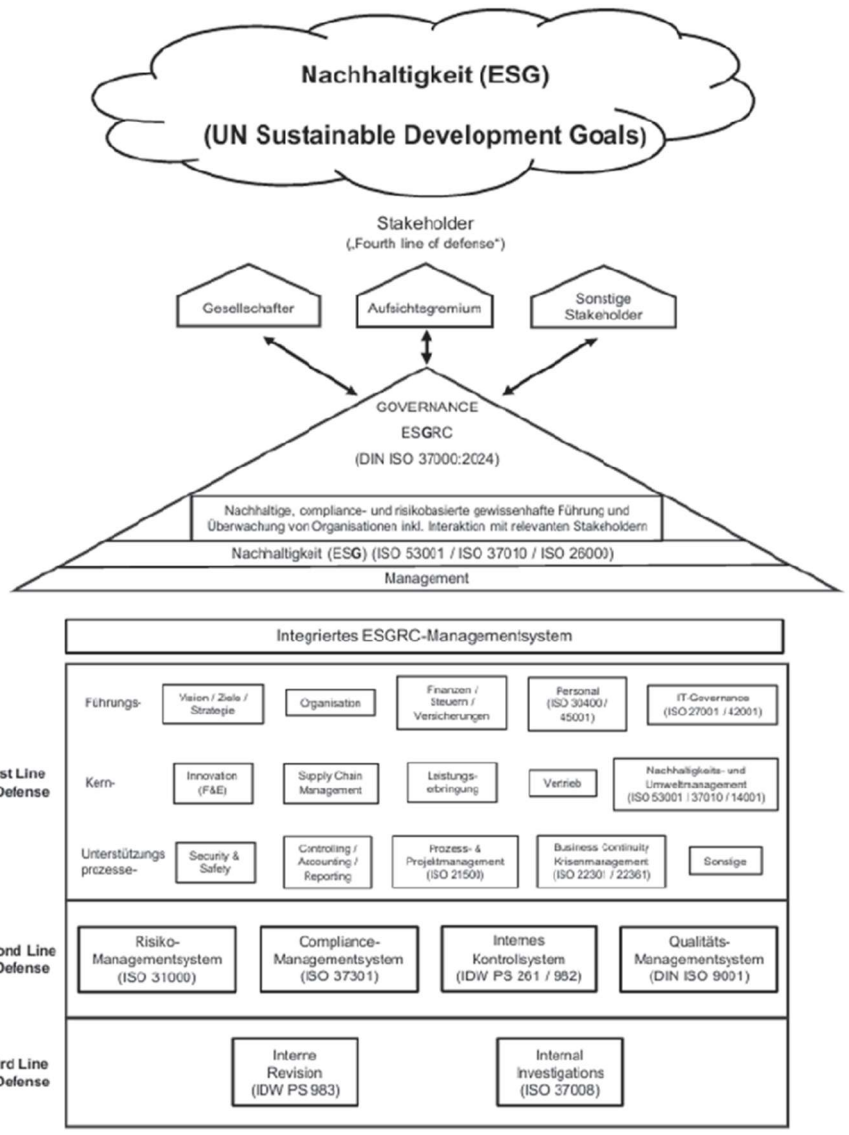


Fig. 1: The "ESGRC House," representation from Scherer, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025

Governance encompasses all relevant areas/functions/processes of an organization.

2. Interdisciplinarity and the example of IT governance

Each individual area in turn consists of various *interdisciplinary* components, which is why governance requires not only specialists but also, more often, generalists:

Example of IT (AI) governance:

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

IT compliance management (this is the top priority!), IT risk management, IT strategy, IT planning, IT implementation, IT processes, IT ICS, IT auditing, IT control and monitoring, IT reporting, IT management (the management [P/D/C/A] of IT, e.g., everything related to hardware and software), IT security management, information security management, data protection, digitization including the use of AI, IT social engineering, etc.

Whether, for example, the IT department head is suitable for IT governance depends on whether they have sufficient affinity and generalist expertise for the many non-IT disciplines that IT governance encompasses. Alternatively, a committee solution could also be considered here.

3. Obligation to use AI in business decisions

ISO 37000 (Governance of Organizations) deals with this in section 6.8, "Data and decisions":

The use of AI – in compliance with legal (e.g., AI compliance with AI Act, NIS 2, DORA, and export controls)[40] and ethical requirements as well as risks – is now not only an opportunity but also an obligation in the context of early risk detection, governance assessment, business decisions (business judgment rule), and much more:

(...) "In order to fulfill information obligations, all available sources of factual and legal information must be exhausted in the specific decision-making situation in order to carefully assess the advantages and disadvantages of the existing options for action on this basis and to take the identifiable risks into account[41] *(...)"*

This now also includes AI.[42]

4. OT risks and new challenges posed by IoT

It should be noted at this point that a risk analysis that only takes traditional information technology (IT) into account is no longer sufficient. Operational technology (OT) must increasingly be included – i.e., those systems that control, regulate, and monitor physical processes, for example in industrial plants, energy supply, or transportation infrastructure. While IT systems are typically geared toward processing and protecting data, OT directly affects the physical security, stability, and availability of operational processes.

However, this separation is becoming less important: as OT systems become increasingly networked via the Internet of Things (IoT), the attack surface is also growing. Modern sensors, control devices, and networked production systems are increasingly connected directly or indirectly to the Internet—often without the protection against external threats that was originally intended. This creates new and complex risk situations at the interface between IT and OT.

The IEC 62443 series of standards have established itself as an internationally recognized standard for the structured evaluation and protection of these systems. It provides a systematic approach to risk analysis, segmentation, access control, and security certification for industrial automation and control systems. The standard is aimed at operators, manufacturers, and system integrators alike and requires, among other things, the implementation of comprehensive security lifecycle management and the inclusion of zone and conduit models for risk assessment.

VI. Regulation: New rules of the game – healthy pressure instead of bureaucracy?

1. Legal basis for preventive corporate management

Sections 91 (2) and (3), 107 of the German Stock Corporation Act (AktG) and Section 1 of the German Act on the Strengthening of the Supervisory and Management Functions of Supervisory Boards of Companies with a Significant Public Interest (StaRUG) with the liability-based duty to identify risks at an early stage with

Quantification, aggregation, control, comparison with risk tolerance and business continuity and crisis management (see IDW ES 16, [43]IDW PS 340 and DIIR Auditing Standard No. 2) refer to governance risks in the same way as case law. This requires a managing director or board member to always be aware of the financial and economic situation (continuous risk identification in real time) and to take appropriate measures in the event of signs of a crisis.

The obligation to establish an early warning system that complies with StaRUG specifies the guiding principle of preventive corporate management. Section 1 StaRUG requires the establishment of a continuous, real-time early warning system. The benchmark is not the formal existence of a system, but its suitability for the timely detection and control of developments that threaten the continued existence of the company. The time dimension of early risk detection is often underestimated in practice. The determination of the forecast period for the probability of insolvency (p1) within the meaning of Section 1 StaRUG is based on the insolvency law *going concern forecast,* not on the commercial law *going concern forecast.* InsO and StaRUG both address the *continued existence of the legal entity,* whereas the "going concern" (continuation forecast) under the German Commercial Code (HGB) refers to the *continuation of the business model*.

The InsO legislator has (unfortunately) given us two forecast periods:

- In the over-indebtedness test pursuant to section 19 (2) sentence 1 InsO, solvency must be forecast for 12 months. Solvency is required because, under current law, insolvency determines over-indebtedness. This means that if, at the time of the over-indebtedness test, insolvency is forecast within the next 12 months, the company is generally considered to be over-indebted.
- When assessing imminent insolvency, it should be noted that Section 18 (2) sentence 1 has been amended by the SanInsFoG to the effect that, as a rule, a forecast period of 24 months must be used. From an insolvency law perspective, the company may file for insolvency due to imminent insolvency if

40 See *Scherer*, AI responsibility and the liability-exempting effect of an AI compliance management system for management (executive board, managing directors, officers), supervisory board, and other executives, 2023, available at: *https://www.risknet.de/themen/risknews/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/.*

41 See Federal Court of Justice, judgment of October 12, 2016 – 5 StR 134/15, margin note 34, ZInsO 2017, 25, 30 – HSH Nordbank.

42 See *Scherer*, The liability-based obligation to use AI in business decisions – also in the context of transformation, risk and crisis management, 2024, available at: *https://www. risknet.de/themen/risknews/ki-verantwortung-und-enthaftende-wirkung-eines-ki-compliance-managementsystems/*.

43 See *Romeike*, IDW ES 16 – Early crisis detection and crisis management pursuant to Section 1 StaRUG, 2025, RiskNET.de, available at: *https://www.risknet.* de/*themen/risknews/krisenfrueherkennung-und*-krisen*management-nach-1-*starug/.

44 See, for example: Federal Court of Justice, default judgment of June 19, 2012 – II ZR 243/11, ZInsO 2012, 1536 and Federal Court of Justice, judgment of July 23, 2024 – II ZR 206/22, ZInsO 2024, 1980.

Its occurrence is predicted for a date within the next 24 months.

Since insolvency and thus the occurrence of material insolvency is not excluded with regard to Section 60 (1) No. 4, 5 GmbHG and Section 262 (1) No. 3 4 AktG, and the obligation to initiate countermeasures pursuant to § 1 (1) sentence 2, 1st alternative StaRUG takes effect at the latest upon the occurrence of imminent insolvency and an early warning system must therefore sound the alarm at the latest at this point in time, the forecast period must be set at 24 months in accordance with § 18 para. 2 InsO, the forecast period is generally to be set at 24 months.

"In principle" because the law itself refers to "as a rule." This allows for the specific characteristics of the company to be considered: e.g., whether the company has short-term (e.g., seasonal business) or long-term (e.g., manufacturing and trading in a cement plant) goods turnover. In the case of short-term/long-term turnover, the forecast period generally ends at the end of the turnover. (45) According to the correct interpretation, it is therefore not possible to rely on a fixed forecast period. In the absence of specific indications, however, a forecast period of 24 months should generally be used in accordance with the legal requirement.[46]

In summary, it can be stated that, based on Sections 18 and 19 InsO, the plan must cover a period of at least 12 months and no more than 24 months.[47] The planning horizon should fall within this time frame and be based on the size and complexity of the company, as this will determine the relevant variables and influences that need to be taken into account in the planning.

2. Legal standard: Continuous real-time monitoring

The Higher Regional Court of Nuremberg ruled in the case of a small company and added that the managing director had a duty to ensure an appropriate and effective compliance, risk management, and internal control system.

This case concerned an employee at a small gas station with few employees who apparently ignored or circumvented some of the credit limits set for business customers, resulting in payment defaults.

When this came to light, the damage amounted to approximately €3.75 million. The managing director (leaseholder of the gas station) was personally ordered to pay damages to the company in this amount for breach of duty.

The Higher Regional Court of Nuremberg stated that he had failed in his duty to ensure an appropriate and effective compliance and internal control management system.

A managing director always has a duty to be aware of the financial and economic situation (continuous real-time risk identification) and to take appropriate measures in the event of signs of a crisis.

The managing director's excuse was that he had just advertised a position for a controller who would have been responsible for this, but that he had been unable to find anyone due to a shortage of skilled workers, was not accepted by the court: as managing director, he was responsible for taking care of this himself.

Important: This case was not about avoiding insolvency or crisis, but about the general duty to prevent damage.

VII. Liability risks increase in proportion to growing regulation

1. Increasing personal liability for executives and officers

In proportion to regulatory requirements, the liability risks for executive bodies (supervisory boards, management boards, managing directors), exposed functions such as department heads, risk or compliance officers, and companies are increasing enormous:

Between 1986 and 1995, there were as many convictions for manager liability in Germany as in the entire previous 100 years. In the following decades, 1996–2005 and 2006–2015, this number doubled again, as current analyses show. No complete data is currently available for the period 2016–2025. However, trends such as the increase in ESG-related lawsuits and stricter regulatory requirements indicate that the number of manager liability cases will continue to rise.

2. International trends and rising settlement amounts

The average settlement amount of the 50 largest US liability court judgments from 2014 to 2018 almost doubled from $28 million to $54 million.

"Top jobs are becoming riskier – more lawsuits are expected"

"Top positions also come with a growing risk of becoming the target of a lawsuit."

[...]

45 See *Schwerdtfeger/Scheuffele*, 4th edition, 2025, section 18 InsO, margin number 14 et seq.

46 See AG Cologne, decision of March 3, 2021 – 83 RES 1/21, ZInsO 2021, 868.

47 See dissenting opinion *Bea/Dressler*, NZI 2021, 67, 70 – generally for planning over 24 months.

48 See OLG Nuremberg, judgment of March 30, 2022 – 12 U 1520/19, NZG 2022, 1058.

49 See in detail: *Scherer/Seehaus*, Governance and Compliance under Section 1 StaRUG, 2024, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/kontinuierliche-risikoueberwachung-in-echtzeit/*.

50 See beck-aktuell, Allianz: Liability risks for companies are increasing, 2020, available at: *https://rsw.beck.de/aktuell/daily/meldung/detail/allianz-haftungsrisiken-fuer-unternehmen-steigen*.

"*We are seeing regulatory authorities around the world scrutinizing corporate behavior more closely, making corporate leaders more vulnerable to investigations, penalties, and lawsuits.*"[51]

3. Developments in D&O insurance

"D&O insurance: Managers are being asked to pay up more often

(...) Insurers expect claims for damages against managers to increase in the future. This is due to the economic situation and higher legal requirements. According to the latest D&O statistics from the GDV, the number of claims rose for the second year in a row. At the same time, claims are rising faster than premium income.

Manager liability insurers operating in Germany had to settle more claims again in 2023. The number of cases rose to 2,200, almost seven percent more than in the previous year. D&O or manager liability insurance pays compensation claims against managers if they have breached their duties. Each claim cost the insurers an average of almost €100,000.

Insurers attribute this development to the economic situation and higher legal requirements. The number of insolvencies has risen significantly recently. This often results in high claims for damages from insolvency administrators against those responsible.

In addition, compliance requirements are constantly growing. Managers are personally liable if they have not established a functioning compliance system. (...)" [52]

4. Requirements for personal suitability

The Federal Fiscal Court (BFH) established "managing director liability due to incompetence":

"[...] anyone who cannot meet the requirements of a conscientious managing director must refrain from taking on the position of managing director or resign from this position. [...]" [53]

Note:

The new DIN ISO 37301:2021(CMS) contains around 60 BGH decisions on legally compliant organization.[54]

VIII. Increased liability due to recent "Cardinal duty" case law: "Sailing blind in liability and insurance loss"

1. Liability risk: Cardinal duty

In addition to the proven drastic increase in personal liability risk, managers face the threat of losing their insurance coverage due to the latest ruling by the Higher Regional Court of Frankfurt/Main (OLG Frankfurt/M.), which accepted the allegation of *a "breach of cardinal duty*" and the resulting indication of a "*known breach of duty*."

According to the latest rulings of the OLG Frankfurt/M., "cardinal duties" are "basic professional duties whose knowledge can be assumed to be possessed by every professional based on life experience."

2. Forms of cardinal duties and case law

a) Cardinal duties in contractual relationships

These duties relate, on the one hand, to contractual relationships (*"duties whose fulfillment is essential for the proper execution of the contract and on whose fulfillment the contractual partner* may *regularly rely*")[56]

b) Cardinal duties in the area of governance

On the other hand, current case law also establishes *cardinal duties within the framework of governance (conscientious management and supervision of organizations*).

Various case groups have already emerged in case law.

Case groups:[57]

"(...) For a managing person (executive board member of a stock corporation, managing director of a limited liability company or other company, senior executive), these cardinal duties should include:

- *not granting themselves or third parties any advantages from the company's assets to which they are not entitled,*[58]

---

51 Quote from: beck-aktuell, Allianz: Top jobs are becoming riskier – more lawsuits expected, 2024, *https://rsw.beck.de/aktuell/daily/meldung/detail/allianz-chefposten-risiko-klagen-versicherung-manager*.

52 Quote from: GDV-Gesamtverband der Deutschen Versicherer (German Insurance Association), D&O insurance: Managers are being asked to pay up more often, 2024, available at: *https://www.gdv.de/gdv/themen/schaden-unfall/d-and-o-versicherung-manager-kosten-182564*.

53 Quote from: BFH, decision of November 15, 2022 – VIII R 23/19, LS, margin number 35, BFHE 278, 392.

54 See *Scherer*, Compliance Management System According to DIN/ISO 37301: Successful Implementation, Integration, Auditing, and Certification, DIN Media Verlag, 2022, 40, footnote 96 with reference to *Rack*, CB 2021, 433.

55 See OLG Frankfurt/M., decision of January 16, 2025 – 7 W 20/24, NJW-RR 2025, 731: "blindly sailing into the crisis." See also OLG Frankfurt/M., judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917, with a similar case (appeal lodged, BGH – IV ZR 66/25).

56 Quote from: BGHZ 164, 11 (BGH, judgment of January 20, 2005 – V III ZR 121/04).

57 Quote from: Wikipedia, Cardinal duty/cardinal obligations in business management, available at: *https://de.wikipedia.org/wiki/Kardinalpflicht*.

58 See BGH, judgment of January 10, 2023 – 6 StR 133/22, BGHSt 67, 225, (*"Ver-VW works council members*") and Federal Court of Justice, judgment of February 10, 2022 – 3 StR 329/21, ZInsO 2022, 765 (*"Liability of management board members for breach of trust in decisions based on inadequate information*"). Both decisions deal with the criminal liability of management board members for breach of trust (Section 266 of the German Criminal Code (StGB)) if they initiate/make *payments that are unjustified or not justified in the specific amount*. In terms of tax (criminal) law, *tax evasion* is also often an issue. If convicted, the board member/managing director faces a fine or imprisonment and, as a further consequence, civil liability for damages, termination, etc., and personal/professional loss of reputation. ➔

- *not to use the company's assets for purposes unrelated to the company,*[59]
- *to file for insolvency in good time in the event of insolvency,*
- *to ascertain the economic situation of the company at any time*[60] and *to examine in detail whether insolvency is imminent: anyone who recognizes that the company is unable to meet its due and demanded liabilities in full on a specific date must check its solvency on the basis of a liquidity balance sheet (OLG Frankfurt, judgment of March 5, 2025 – 7 U 134/23 (...).*

c) Extension of the case groups of cardinal duty violations to governance compliance

Current case law now extends these case groups

- to include the obligation to identify risks and crises at an early stage and to implement crisis management.
- crisis management and
- to the "*diverse duties relating to corporate management associated with registration as a managing director of a corporation*."

Quote from the Higher Regional Court of Frankfurt/Main:[61]

"In principle, the assumption of a cardinal duty violation presupposes that the (...) violated

legal norm is one of the central, fundamental rules of a specific area of regulation."

"The generally recognized (...) duty of early crisis detection and crisis management for limited liability companies already existed before the entry into force of Section 1 (1) StaRUG under Section 43 (1) GmbHG."

d) Digression: Early risk detection as a necessary component of early crisis detection

Insofar as Section 1 StaRUG and the current case law refer to refer to "early crisis detection" rather than "early risk detection," it should be noted that early risk detection is an indispensable preliminary step in early crisis detection.

Early risk detection as a mandatory element of a monitoring system for "early detection of developments that could jeopardize the company's continued existence" was already established in 1998 with the KonTraG in Section 91 AktG as a legal obligation for AGs and (by analogy) for large GmbHs (see the legislative materials on the KonTraG and the FiSG).

- Discharge of the management board due to inadequate risk management system

Case law quickly followed suit and extended the obligation to risks that do not threaten the existence of the company:[62]

The Munich Regional Court [63] ruled in 2007 that the discharge of the management board of a Munich-based company was void.

because the documentation of the process flows and the responsibilities of the risk management system were omitted. Since discharge resolutions based on material deficiencies can only be successfully challenged in the event of serious violations of the law or the articles of association, it can be concluded that the court assumed a correspondingly serious violation in this case.

The LG's decision also contains statements that can be interpreted to mean that the risk management system to be established and documented (!) must deal not only with risks that jeopardize the company's existence, but also with general risks.[64]According to its reasoning, the court required that not only the management, but all relevant departments, such as the areas and hierarchical levels affected, down to the level of the individual employees, must be informed about the existing risks – not only those that threaten the existence of the company – in the area and field of activity concerned in order to "get these risks under control."

---

etc. Note: If the *supervisory board* were responsible for such unjustified payments, the members of the supervisory board would be accused of violating Section 116 of the German Stock Corporation Act (AktG), as this refers to Section 93 (1) sentence 2 AktG. *In practice*, unjustified (over)payments are often made in order to part ways "quietly" on the basis of a termination agreement/settlement/etc. instead of a legal dispute, or to "buy" favorable treatment (e.g., from works councils) through excessive remuneration/bonus payments. In practice, it is often not checked whether there is any need for the service to be commissioned or whether the service provided justifies its price, or loss-making investments are made or maintained without applying the BJR. The case groups "unauthorized payments" are incredibly numerous in practice and thus represent considerable liability potential for executive boards/managing directors and supervisory boards if they are either unaware of the BJR or do not comply with it despite being aware of it. The 6th Senate of *the Federal Court of Justice (BGH*) (dated January 6, 2023 – 6 StR 133/22) emphasizes that "*the question of whether this violation is serious or evident is irrelevant for criminal liability for breach of trust*." Even the "*consent of the* asset owners" (e.g., shareholders of an AG or GmbH) "*does not preclude a breach of duty*," and any advantage gained through the unauthorized performance cannot be compensated for by the unauthorized outflow of assets. Even a *waiver of repayment* is problematic under criminal law. For more details, see *Sche-rer,* Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Section 6.8.

59 See Federal Court of Justice, judgment of July 10, 2018 – II ZR 24/17, BB 2018, 2369: Particularly with regard to the public interest concerns mentioned in governance standards, such as sustainability and social responsibility, compliance requirements must be observed in the area of conflict between integrity and ethics. For example, managing directors, executive boards, and supervisory boards cannot simply incorporate stakeholder or public welfare interests, such as sustainability (ESG) or social responsibility (CSR), into their strategic goals that need to be adapted to the transformation requirements. Rather, in order to avoid sanctions, they must comply with numerous legal requirements.

60 See BGH, default judgment of June 19, 2012 – II ZR 243/11, ZInsO 2012, 1536, and BGH, judgment of July 23, 2024 – II ZR 206/22, ZInsO 2024, 1980, and OLG Nuremberg, judgment of March 30, 2022 – 12 U 1520/19, NZG 2022, 1058.

61 See OLG Frankfurt/M., judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917, with a similar case (appeal lodged, Federal Court of Justice – IV ZR 66/25).

62 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) According to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Section 6.9.

63 See LG Munich I of April 5, 2007 – 5 HK O 15964/06, NZG 2008, 319; *Theusinger/Liese*, NZG 2008, 289; LG Berlin v. 3.7.2002 – 2 O 358/01, AG 2002, 682: this already considered inadequate risk management to be an important reason for the extraordinary termination of a board member in 2002.

64 See *Theusinger/Liese*, NZG 2008, 290.

Since it is usually not a single risk that threatens the existence of a company, but rather many individual risks that aggregate, early risk detection with quantification and aggregation and comparison with risk-bearing capacity must also be considered in the context of early crisis detection (which means that, due to the general duty of conscientious management – Section 43 of the German Limited Liability Companies Act (GmbHG) and Section 93 of the German Stock Corporation Act (AktG) – even risks below the threshold of a threat to the continued existence of the company must be managed appropriately).[65]

- *Inadequate risk management and aggregation of numerous individual risks as the main cause of insolvency*

The management report for an insolvency administered by the author, which was audited by a recognized auditing company, states:

"*Description of the situation: [...] One of the main reasons is the lack of risk management, which led to an uncontrolled accumulation of numerous business risks that were too many for the size of the company*"[(66)]

A functioning risk management system would have prevented significant damage in this case: approximately €73 million in claims were filed by the group's creditors, of which approximately €50 million were confirmed by the insolvency administrator. To date, approximately €17 million (€) have been returned to creditors through company continuation, transferable restructuring, separations, liquidation, etc. The remainder is likely to be irretrievably lost.

Quote from the Frankfurt/M. Higher Regional Court: [67]

"In principle, the assumption of a breach of a cardinal duty requires that the (...) legal norm that has been violated is one of the central, fundamental rules of a specific area of regulation."

"The generally recognized (...) duty of early crisis detection and crisis management for limited liability companies already existed before the entry into force of Section 1 (1) StaRUG under Section 43 (1) GmbHG."

The current court ruling rightly considers Section 43 of the German Limited Liability Companies Act (GmbHG) (duty of the managing director of a limited liability company to conduct business with due diligence) to be a legal norm that "*belongs to the central, fundamental basic rules of a specific area of regulation*."

Consequently, § 93 AktG (duty of the executive board of an AG to conduct business conscientiously), including § 93 (1) sentence 2 with the obligation to comply with the so-called business judgment rule, is a corresponding legal norm for executive boards that is considered a cardinal duty.

And for supervisory boards, Section 116 AktG, which refers to Section 93 AktG, is relevant.

Thus, governance compliance is rightly regarded as a fundamental professional duty of a managing director, executive board member, or supervisory board member.

In the event of any breach of duty within the meaning of Section 43 of the German Limited Liability Companies Act (GmbHG) or Sections 93 and 116 of the German Stock Corporation Act (AktG), it will certainly be necessary to examine whether the fundamental rules of the regulatory matter have been violated. This will again be closely related to the respective risk situation with regard to this regulatory matter in relation to the specific organization.

Early risk and crisis detection and management are fundamental for all organizations because they are intended to protect the existence of the organization. Currently, IT governance, including information security, is likely to be of similar importance for all organizations. Sustainability risks are also likely to become increasingly important in these risk areas.

In general, an appropriate (compliance) risk analysis[69] within the individual organization would provide information on which (legal) areas with the associated obligations are to be classified as cardinal obligations. The risk-based approach considers requirements aimed at avoiding danger to life and limb, significant civil or criminal penalties, or significant financial losses that impair risk-bearing capacity to be particularly important.

3. Legal obligation as a cardinal duty

The principle of legality,[70] or the duty of compliance, i.e., the duty of all to comply with binding rules such as laws or case law, has also become established in case law in recent years:

Starting with the famous "new citizen" ruling of the Munich Regional Court of December 10, 2013[71] in the Siemens compliance scandal,

---

65 See *Scherer/Seehaus*, Governance and Compliance under Section 1 StaRUG, 2024, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/* kontinuierliche-risikoueberwachung-in-echtzeit/.

66 See the published management report of N.N. Raumexklusiv GmbH for the financial year from January 1 to December 31, 2012.

67 See OLG Frankfurt/M., judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917, with a similar case (appeal lodged, Federal Court of Justice – IV ZR 66/25).

68 See the contents of governance compliance: *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025.

69 See DIN ISO 37301 standard section 4.6 Compliance risk analysis and ISO IEC 31010 Risk Assessment.

70 See Federal Court of Justice, judgment of August 27, 2010 – 2 StR 111/09, ZCG 2010, 285 (RWE-Tochter: Waste disposal and slush funds"), commented on in *Scherer*, What interests investors: Antifragility and the Achilles heel of the ordinary businessman, 2019, available at: *https://www.scherer-grc.net/ publikationen/das-interessiert-kapitalgeber-antifragilitaet-und-der-achilleskoerper-des-ordentlichen-kaufmanns.*

71 The so-called "Siemens/Neubürger ruling" of the Munich Regional Court I, ruling of December 10, 2013 – 5 HK O 1387/10, NZG 2014, 345, is considered a landmark ruling on the organizational liability of executive boards in stock corporations. The main question was whether former Siemens board member *Dr. Uriel J. Neubürger* had breached his duty of care under Section 93(1) of the German Stock Corporation Act (AktG) by failing to adequately improve deficient compliance structures within the group. The court affirmed personal liability and clarified that members of the management board are also liable if they violate organizational duties, in particular in the case of inadequate control of corruption risks and internal control systems.
risks and internal control systems. It was emphasized that the obligation to establish a functioning compliance ➔

The Düsseldorf Regional Labor Court (LAG) the Frankfurt Labor Court (ArbG), the Federal Court of Justice (BGH) and, most recently, the Nuremberg Higher Regional Court (OLG) have all ruled that it is the duty of the managing director or executive board to establish an appropriate and effective compliance management system.

In addition, the Federal Court of Justice ruled in the "Buchhändler judgment"[77] that a professional must have the necessary knowledge regarding the compliance requirements relevant to their work or obtain it from experts. Furthermore, they must also fulfill these requirements. According to the BGH in the "ISION decisions," following the expert's recommendation can have a binding effect. [78)]

From the continuous repetition of this case's law over many years, it can be concluded that compliance and legal obligations are a self-evident cardinal duty of the organs:

Anyone who knowingly disregards legal requirements (dolus eventualis, i.e., "considering it possible and accepting it") is therefore in breach of fundamental professional duties.

It should come as no surprise that intentional violations of the law are severely punished in almost all areas of law (criminal law, insurance law, contract law, etc.).

Contrary opinions, which indirectly argue that a board member or managing director is not a profession that requires specific qualifications, are refuted by the Federal Court of Justice (BGH)[(79)] which states that a managing director who wishes to leave the company without liability must resign from office.

The Federal Fiscal Court (BFH) takes the same view, stating:

"[...] anyone who cannot meet the requirements of a conscientious managing director must refrain from taking on the position of managing director or resign from this position. [...]"

It is certainly not easy to always meet all compliance requirements. However, with regard to cardinal duties, comprehensive compliance is not required, but only compliance obligations are not intentionally violated.

In parallel, case law[81] developed the *corrective measure of the exonerating effect of a compliance management system*: in the event of breaches of duty below management level, the accusation of organizational fault in the sense of a breach of supervisory duty may be waived if a compliance management system is in place.

This development in case law and at least the *risk* of a breach of cardinal duty being assumed in the event of intentional compliance violations (even in cases of dolus eventualis) can have enormous implications for executive bodies and managers and should be appropriately reflected in risk and compliance management.

IX. Corrective measures for the exonerating effect of an appropriate compliance management system, breach of supervisory duties, and employee misconduct

1. Responsibility despite delegation – principal liability and structural requirements for governance

When executive bodies delegate their governance tasks to managers, established case law stipulates that at least supervisory duties and ultimate responsibility remain with the executive body.

This also applies in light of what is known as employer liability, which—although German company law does not recognize general liability for results—establishes criminal, administrative, and civil liability for breaches of duty by employees in the course of their work. The basis for this is a position of guarantor within the meaning of Section 13 of the German Criminal Code (StGB), specified in Section 43 of the German Limited Liability Companies Act (GmbHG), Section 93 of the German Stock Corporation Act (AktG) and Section 130 of the German Administrative Offenses Act (OWiG).[(82)]

The tasks of risk and crisis detection, compliance, information security, and business continuity, as well as relevant areas of transformation such as digitalization and organizational development, are often delegated to the corresponding staff units or lines of defense functions.

This division of labor makes good business sense, but it does not alter the original responsibility of the management (business owner responsibility).

---

or risk management system cannot be delegated and is one of the central management tasks of a board of directors. Merely relying on subordinate bodies does not relieve them of their responsibility.

72 See LAG Düsseldorf, judgment of November 27, 2015 – 14 Sa 800/15, para. 242 (rail cartel judgment).

73 See Frankfurt Labor Court, judgment of September 11, 2013 – 9 Ca 1541/13 (Libor manipulation).

74 See Federal Court of Justice, judgment of January 15, 2013 – II ZR 90/11, NJW 2013, 1958 marginal no. 22 (derivative transactions contrary to the purpose of the company) and Federal Court of Justice, judgment of May 9, 2017 – 1 StR 265/16, NJW 2017, 3798 (tank howitzer case).

75 See OLG Nuremberg, judgment of March 30, 2022 – 12 U 1520/19, NZG 2022, 1058.

76 See *Scherer*, Compliance Management System According to DIN/ISO 37301: Successful Implementation, Integration, Auditing, and Certification, DIN Media Verlag, 2022, 39.

77 See Federal Court of Justice, judgment of November 18, 2020 – 2 StR 246/20, wistra 2021, 355.

78 See *Scherer*, Compliance Management System According to DIN/ISO 37301: Successful Implementation, Integration, Auditing, and Certification, DIN Media, 2022, 233: "Who is supposed to know all this?"

79 Decision of May 21, 2019 – II ZR 337/17.

80 See Federal Fiscal Court, decision of November 15, 2022 – VIII R 23/19, LS Rn. 35, BFHE 278, 392.

81 BGH 2017: (KMW), judgment of May 9, 2017; BGH 2022: (self-cleaning), judgment of April 27, 2022; BGH 2023 (distribution of business), judgment of November 9, 2023; ECJ 2023: (Deutsche Wohnen), judgment of December 5, 2023; ECJ 2023: (hacker attack), judgment of December 14, 2023; ECJ 2024: (VAT fraud), judgment of January 30, 2024; ECJ 2024: Judgment of April 11, 2024 – C-741/21, NJW 2024, 1561; Higher Regional Court of Stuttgart 2025: (employee excess), decision of February 25, 2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279.

82 See Federal Court of Justice, judgment of July 17, 2009 – 5 StR 394/08 (2), NJW 2009, 3173; Federal Court of Justice, Judgment of October 20, 2011 – 4 StR 71/11, BGHSt 57, 43.

According to Section 43 GmbHG and Section 93 (1) AktG, the management is obliged to ensure that delegated functions:

- methodologically suitable,
- are adequately staffed and organized,
- systematically integrated, and
- continuously monitored.

These requirements are also reflected in international standards: ISO 37301 (No. 5.3) requires continuous review of the integrity, adequacy, and effectiveness of the compliance management system, [83] ISO 37000 (No. 5.1) emphasizes management's responsibility for governance structures.[84]

If one of these elements is missing, the possibility of exculpation is ruled out, especially if there are indications of overload, understaffing, or structural deficiencies.

If the delegates, i.e., the managers responsible by virtue of delegation, do not perform their duties or do not perform them properly, thereby causing damage to the organization or third parties, the question arises as to the (liability) responsibility of the executive bodies and delegates.

In the event of breach of duty or omission on the part of the delegates in the course of their operational activities, there may be a supervisory fault on the part of the organs, but an appropriate compliance management system may have an exonerating effect[85]

2. Excessive conduct by employees – definition, attribution, and limits of liability transfer

If the delegates fail to act in accordance with their duties due to the pursuit of their own goals unrelated to the company, the question arises as to whether the organs are also responsible for so-called "Employee excess."

> ***Example in the context of fulfilling supervisory duties***
>
> *For example, this "exonerating argument of employee excess" would be conceivable if, despite proper delegation to a fundamentally properly selected, competent, instructed, adequately resourced, and also monitored line of defense function*
>
> *their meta-surveillance tasks in an inappropriate manner in order to avoid compromising third parties, e.g. primarily responsible colleagues.*
>
> *Or, in other words: Is there staff excess if, despite knowledge of relevant and risky weaknesses in the organization, the lines of defense function deliberately examine and report on other issues without the knowledge or even instruction of the executive bodies?*

Staff excess is behavior in which an employee acts outside the scope of their employment contract obligations.

and is objectively no longer working for the employer. There is no functional connection to the operational task. Typical these are actions motivated exclusively by private or non-business reasons, such as personal enrichment or for the benefit of third parties.

The Federal Court of Justice clarifies that such excesses cannot, in principle, be attributed to the organization, as they lie outside the sphere of influence of the company. Although the position of business owner or superior may give rise to a duty to prevent criminal offences committed by subordinate employees, this duty is limited – according to the official guiding principle – to business-related criminal offences and does not include acts committed by employees merely in the course of their work.

Dogmatically speaking, cases of employee misconduct involve conduct that is outside the scope of the employer's authority and the employment contract. The company and its managers are then generally not liable as "responsible parties" within the meaning of Art. 4 No. 7 GDPR, § 831 or § 278 BGB.

The decisive factor for attribution is whether the action still falls within the scope of the tasks assigned by the employer – which is usually determined by job descriptions, employment contracts, work instructions, or specific individual orders. If an employee acts within this framework – even if contrary to instructions – the behavior remains attributable to the company. Only when the scope of action is objectively exceeded and the connection to the company's purpose is completely lost is there a genuine case of excess. The threshold for excess is therefore crossed when the formal task commitment is abandoned and replaced by subjective, selfish interests.

A look at case law shows that excess generally leads to personal responsibility on the part of the employee.

> ***Example case (1) from the Higher Regional Court of Stuttgart: Police officer as data thief – no attribution to the employer in the case of complete reversal of purpose:***[87]
>
> *During the night, a police officer used his official access to the police information system out of pure curiosity to retrieve personal data of a colleague who was in custody without any official reason. If the employee deliberately misuses*

83 See *Scherer*, Successful Implementation, Integration, Auditing, and Certification of a Compliance Management System According to DIN ISO 37301, DIN Media, 2022, Chapters 5.1 and 5.2.

84 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) According to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Section 5.2.

85 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) According to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Section 4.2 "Governance and Delegation."

86 Federal Court of Justice, judgment of October 20, 2011 – 4 StR 71/11, BGHSt 57, 42.

87 See OLG Stuttgart, decision of February 25, 2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279.

If he acts on his own initiative, i.e. without official instructions, he no longer acts as an agent bound by instructions (Section 278 BGB), but on his own responsibility (here within the meaning of Art. 4 No. 7 GDPR). He thus becomes the "responsible party" himself, with all the resulting consequences in terms of liability and fines. The private use of work-related access rights constitutes what is known as "employee misconduct" – i.e., conduct that is completely outside the scope of the employee's legitimate duties and can therefore only be attributed to the employee and not to the employer.

Example case (2) from the Schwerin Regional Court: Criminal energy of a practice employee – employee excess exonerates contract doctor: [88]

In medical practice, a medical assistant and a pharmaceutical employee manipulated the prescription system. Without the doctor's knowledge, they issued prescriptions, ordered medicines at the expense of the statutory health insurance funds, and then sold the goods in the bodybuilding scene. A health insurance fund then made a recourse claim.

The plaintiff claimed approximately $68,000 (€) against the contract doctor. The Social Court dismissed the claim, stating that the doctor could not be proven to be at fault. In particular, it had not been proven that the prescriptions used were based on blank prescriptions signed by him. The abuse by the employees therefore constituted an independent act outside the scope of their official duties, with the result that the doctor was not liable for the conduct of his employees.

Key points for practice:

If an employee deliberately acts outside the scope of their duties with criminal intent and deliberately conceals their actions, there is much to suggest that this constitutes an act of their own responsibility – and not something that can be attributed to management. Exemption from liability requires that the breach of duty was not objectively recognizable and not controlled by the management.

Note on employee misconduct with criminal intent:

The pharmacy case of the Schwerin Regional Court illustrates that, in the event of significant criminal intent, deliberate concealment, and a lack of control, damaging employee behavior must be classified as an act of personal responsibility. Whether a breach of duty by an employee is attributable to the organization or management depends largely on two criteria: the functional connection with the operational area of responsibility and the objective controllability by the management level. If conduct is formally carried out within the scope of official access rights but serves exclusively irrelevant, self-serving purposes—such as personal gain or the gain of third parties—and is also deliberately designed to deceive and conceal, there is much to suggest that it is attributable to the individual.

Staff excess. The likelihood of exemption from liability increases with high criminal energy and low control options. This increases in particular if the employee creates a control environment that systematically makes it difficult to detect their actions – for example, by circumventing internal processes, manipulating documents, abusing special positions of trust, or deliberately withholding information from control bodies. In such constellations, the internal operational context breaks down to such an extent that attribution to the organization is regularly ruled out—even if the employee has formally acted within existing powers.

A controversial example (3): The VW emissions scandal – employee excess or structural control failure?

In 2018, the public prosecutor's office in Braunschweig imposed a fine of €1 billion on Volkswagen AG for a breach of its supervisory duties pursuant to Section 130 of the German Administrative Offences Act (OWiG), after the US Environmental Protection Agency (EPA) revealed in September 2015 that VW had manipulated the emissions values of diesel vehicles using software (defeat devices). The allegation: failure to take adequate organizational precautions to prevent unlawful conduct. The fine consisted of a formal fine of €5 million and a skimming of economic benefits amounting to €995 million. As Volkswagen accepted this, there was no judicial review. – The defeat devices were developed by VW employees acting within the scope of their operational functions. Whether this conduct is to be classified as unauthorized employee excess or whether there were structural causes, failure to supervise, or even shared responsibility at management level remains unclear to this day. [89]

Note:

The VW emissions scandal is a case that remains unresolved and exemplifies how challenging and difficult it can be to clarify the facts and legal issues in complex organizations. The case has been examined in numerous proceedings, investigative committees, and publications; however, due to the complexity of the case and the large number of unresolved issues, it has not yet been legally classified as excessive behavior on the part of individual employees, in which the threshold of personal responsibility has been crossed, or as employee behavior that is (still) attributable to the organization.

---

88 See SG Schwerin, judgment of June 14, 2023 – S 6 KA 15/20.

89 See LG Munich II, judgment of June 27, 2023 – W5 KLs 64 Js 22724/19 (see press release 38/20, available at: *https://www.justiz.bayern.de/gerichte-und-behoerden/oberlandesgerichte/muenchen/presse/2023/38.php)*; cf. tagesschau, Former VW managers sentenced to prison in diesel scandal, 2025, available at: *https://www.tagesschau.de/wirtschaft/volkswagen-diese laffaere-urteil-100.htm;* WirtschaftsWoche, Former VW managers sentenced to prison for diesel scandal, 2025, available at: *https://www.wiwo.de/ unternehmen/auto/betrugsprozess-fruehere-vw-manager-wegen-dieselskandal-zu-haft-verurteilt/100130305.html.*

10 years of "Dieselgate." The case thus prompts further discussion.

3. Liability consequences of control failures and requirements for an effective CMS

a) Delegation and organizational obligation

In corporate law, the decisive factor in terms of liability is whether the management adequately fulfills its responsibilities for management, control, and intervention. The Higher Regional Court of Frankfurt/Main has clarified that a managing director is personally liable if he grants powers of attorney without ensuring effective control.[90] In such cases, even an initially arbitrary act by an employee can turn into a structurally induced organizational failure—with full attribution to the management level.

Given the size of the company and the division of labor, managers are regularly unable to personally fulfill all of their duties, in particular selection, supervision, and traffic safety duties. Therefore, there is a legally binding obligation to delegate, in particular to specialist departments such as human resources, compliance, or auditing.[91]However, this delegation is only exempt if it is properly structured, tailored to the risks, and effectively monitored. Over time, case law has developed a tiered system of organizational duties under the heading of "decentralized proof of exemption. This includes, in particular, the obligation to systematically identify all operational legal obligations, delegate them to suitably qualified employees in a manner commensurate with the risk involved, provide clear instructions on tasks and risks, establish effective control and monitoring mechanisms, and actively intervene in the event of identified breaches of duty. In addition, the organizational structure must be continuously reviewed and adapted to changes in the legal and operational environment.

The following example shows that mere delegation without an effective control and monitoring structure does not have the effect of exempting liability

> ***example (4) – OLG Nuremberg:***[93]
>
> *A long-standing employee was able to manipulate fuel card statements to a considerable extent because there was neither a functioning dual control principle nor random checks. Although the tasks had been formally delegated to the controlling department, the monitoring system failed completely in practice.*

Comment:

The Higher Regional Court of Nuremberg saw this as an organizational and supervisory failure on the part of management. It made it clear that there is a legal obligation to set up an effective compliance system. Delegation does not release you from the duty to monitor and intervene immediately. A purely formal CMS is not enough—structured, risk-appropriate supervision is required. The ruling emphasizes that without systemic integration and ongoing monitoring, even well-intentioned delegations can give rise to liability.

b) Obligations for prevention and control

Delegation is permissible – but does not absolve liability. Those who delegate must monitor, document, and correct any deviations that occur. Particularly in the context of employee misconduct, it must be examined whether the organization could have prevented such misconduct, for example by:

- Defined rules of conduct (Code of Conduct)
- training on the limits of duties,
- effective reporting systems and whistleblower protection,
- and documented monitoring of the limits for excessive intervention.

c) Excess and control failure: limits of exemption from liability in the event of system deficiencies

Exemption from liability for employee misconduct is not unlimited. It requires that the company's management has effectively fulfilled its organizational, selection, and monitoring obligations. If effective control or compliance structures are lacking or remain merely formal, excessive conduct can still be attributed to the company—because there is then a structural organizational failure.

However, the reverse also applies: the applicable liability law does not require complete omnipotence of control. There is no obligation to achieve the impossible (impossibilium nulla obligatio est). A duty of supervision can only be breached where such supervision would have been feasible in the specific case (see Section 130 OWiG), because the person responsible for supervision must have committed the breach culpably (reprehensibly).[94]This basic rule, which has been confirmed by case law, takes into account the practical circumstance that a company cannot prevent all conceivable breaches of duty by individual employees—especially if they act with a high degree of criminal energy and deliberate deception.

The limit of exemption from liability is therefore reached when a company cannot demonstrate that it has an effective control system in place. In such cases, individual excesses take a back seat to an attributable systemic deficiency. The decisive factor is the dogmatic distinction between the subjective arbitrariness of the perpetrator and objective organizational responsibility. At the same time, a structurally functioning

---

90 See OLG Frankfurt/M., judgment of May 23, 2019 – 5 U 21/18, ZIP 2018, 1132; see also OLG Nuremberg, judgment of 30 March 2022 – 12 U 1520/19 (fuel card case), DB 2022, 2153.

91 See *Rack*, CB 2013, 231.

92 See *MünchKomm-BGB/Wagner*, 9th ed. 2024, § 831 marginal no. 56 et seq.

93 See OLG Nuremberg, judgment of March 30, 2022 – 12 U 1520/19, NZG 2022, 1058.

94 See OLG Jena, decision of November 2, 2005 – 1 Ss 242/05, NStZ 2006, 533.

of the system does not always apply – for example, if early indicators are ignored, whistleblowers are disregarded, or control mechanisms are implemented incompletely. In such cases, the excess becomes organizational negligence.

Example case (4) of the ECJ: Falsified invoices by employees – excess exonerates if a control system is in place[95]

A gas station employee in Poland issued more than 1,600 fake invoices totaling around 320,000 Polish zlotys (PLN) over a long period of time on behalf of her employer—without their knowledge and without any actual goods being moved. The fictitious invoices were not entered into the system. The recipients used these invoices to obtain VAT refunds unlawfully. The tax authorities demanded VAT from the company on the grounds that it had violated its supervisory obligations.

The ECJ (judgment of January 30, 2024 – C-442/22) ruled that such conduct can be considered an independent act of an employee – but only if the employer can prove that it took all reasonable measures to prevent, control, and detect such violations. The decision emphasizes that a formally existing compliance or control system is not sufficient. The decisive factor is whether the system functioned in a lively, effective, and verifiable manner in the specific case. However, this requirement does not mean that misconduct that has remained hidden for years automatically disqualifies the entire system and that responsibility must be attributed to the business owner. Rather, even a structured and active control system can be circumvented, for example, through particular criminal energy, deliberate deception, and exploitation of structures of trust. In such an exceptional case, the focus of the breach of duty no longer lies in the organizational sphere, but exclusively with the employee who acted—thereby relieving the company and its principal of liability.

Case example (5) – OLG Jena: No duty of omnipotence – duty of supervision ends with criminal energy[96]

In a company, waste material was deposited near a river without permission. Whether this was done intentionally by employees in violation of instructions remained unclear to the authorities and the lower courts. In any case, there was no instruction from management. Due to allegedly inadequate supervisory measures, a fine was imposed on the limited liability company and its managing director pursuant to Section 130 of the German Administrative Offenses Act (OWiG).

The Higher Regional Court of Jena (decision of November 2, 2005 – 1 Ss 242/05, NStZ 2006, 533) overturned the decision and clarified that Section 130 OWiG does not establish any liability on the part of the company's management. The mere position of managing director is not sufficient for attribution. Rather, the Allegation of a breach of supervisory duty presupposes that specific, feasible control measures were omitted—and that this was done culpably. Liability only arises if the person responsible for supervision is actually in a position to recognize, stop, or prevent the behavior.

Note:

The court thus confirms a fundamental standard of liability: there is no obligation to perform the impossible – "impossibilium nulla obligatio est." This is important to note in cases where employees act with considerable criminal intent and deliberately circumvent internal structures or conceal their conduct. In such cases, it may be objectively impossible to fulfill the duty of supervision in individual cases. In such constellations – for example, in the case of employee misconduct – accountability ends where management actions have reached their structurally feasible limits.

Case study (6) – Vodafone data scandal: Excess or structural control failure?[97]

At the beginning of June 2025, Vodafone was fined of €45 million – the highest ever imposed by the Federal Commissioner for Data Protection and Freedom of Information in Bonn. The accusation: insufficient control of partner companies, inadequate IT security, and lack of oversight of processes that enabled the misuse of customer data. Among other things, employees in partner shops had systematically manipulated mobile phone contracts and used internal IT structures without authorization.

Even though individual actions indicate arbitrary behavior with considerable criminal energy, the authority apparently did not consider the conditions for liability exclusion due to excessive behavior to be met in the area of GDPR fines. The decisive factor was probably that Vodafone had not structurally established effective control mechanisms, such as those for monitoring processors. In such a case, breaches of duty are not just individual missteps, but the result of a systemic failure of supervision.

The proceedings concerning the (criminal) liability of the organs and executives were discontinued. [98]It is unclear whether this decision was made in favor of the organs (in dubio pro reo).

---

95 See ECJ, judgment of January 30, 2024 – C-442/22, available at: *https://curia.europa.eu/juris/document/document.jsf?text=&docid=282265&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1*.

96 See Higher Regional Court of Jena, decision of November 2, 2005 – 1 Ss 242/05, NStZ 2006, 53.

97 See Federal Commissioner for Data Protection and Freedom of Information, BfDI imposes fines on Vodafone, press release 6/2025, available at: *https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/06_Geldbu%C3%9Fe-Vodafone.html*.

98 See InvestmentWeek, 45 million for the cloak of silence – what Vodafone would rather keep quiet about, 2025, available at: *https://www. investmentweek.com/45-millionen-fur-den-mantel-des-schweigens-was-vodafone-lieber-verschweigen-wurde/*.

and executives were accused of having staff excesses.

d) Criteria for liability-relevant control failures

As already explained, in the case of staff excesses, it is crucial whether this was foreseeable by the company management and whether existing risk signals were ignored. The mere formal existence of a CMS is not sufficient if the system has not been effectively implemented in the company or has structural weaknesses. The decisive factor is whether there were concrete indications that a duty to react arose, for example, through systematic deviations, information from the workforce, or critical risk reports.

The following points must be examined critically:

- Were there early indicators that were ignored or downplayed?
- Was the compliance management system (CMS) that was set up unrealistic, understaffed, inadequately equipped, or methodologically unsuitable?
- Was reliance placed on aggregated risk reports or positive self-disclosures without questioning their validity or checking their plausibility?

If the answer to even one of these questions is yes, the exemption does not apply. In this case, there is a warning signal that requires control and to which no appropriate response was made – with the result that the excess can no longer be attributed to the employee alone but is attributable to a structural control failure on the part of the organization under liability law. The central question is then no longer whether the CMS was in place, but how it was actually implemented and checked for effectiveness.

e) Excess as a failure of management duty? Often yes, but not always!

Ignorance is no excuse – it is a liability: managers who cite a lack of information must ask themselves why they failed to fulfill their duties to inquire and obtain information. It is not only what was known that matters, but what should have been known. Management is obliged to establish and enforce a functioning reporting system. This includes obliging employees to report risks and breaches of duty in their respective areas of responsibility. Only those who actively manage such a reporting system fulfill their legal obligations.

The case law presented above makes it clear that a misguided belief in protection through delegation or reports does not lead to exoneration, but rather to strict liability, especially in cases of foreseeable deviations from behavior and inadequate systemic structures.

Rack sums it up (actually) when he writes:

"Those who delegate must monitor or be held accountable." Employees with particular criminal energy who deliberately evade monitoring take this maxim, which is true in itself, to its dogmatic extreme.

Therefore, the following applies: Excess is not an argument for exoneration, but rather a magnifying glass for systemic leadership failure, especially if:

- there was no effective CMS in place,
- whistleblowers were ignored,
- sanction systems were lacking,
- risks were not aggregated or validated,
- delegation took place without control,
- the purpose of the action did not correspond to the employee's duties as defined in the job description, and
- No systematic distinction was made between conduct contrary to instructions and excessive conduct.

Case study (7): A somewhat different case from practice – Attribution despite excess on the part of a (former) vicarious agent with criminal intent[102]

The Munich Regional Court I ordered a financial services provider to pay immaterial damages pursuant to Art. 82 GDPR and clarified that the excess of a (former) vicarious agent does not exonerate if control obligations are violated. After the termination of the contract, an IT service provider used access data that had not been blocked for months to gain unauthorized access to sensitive customer data of a financial services provider, including tax IDs, copies of ID cards, and deposit data. The management had failed to revoke the rights of the former IT service provider in a timely manner. The access took place entirely outside the company's organizational structure, as in the case of employee misconduct. Nevertheless, the financial services provider was liable because no effective access control or audit-proof authorization management had been implemented. Although a compliance system formally existed, the court ruled that it was structurally inadequate and effectively non-functional.

---

99 In specialist literature, this is dealt with under the term "criminal organizational responsibility," see *Momsen/Grützner*, Wirtschafts-und Steuerstrafrecht (Commercial and Tax Criminal Law), 2nd edition 2020, § 16 Rn. 42 ff.

100 For details, see: OLG Stuttgart, judgment of February 19, 2012 – 20 U 3/11, ZCG 2012, 167, on the so-called "Sardinia statement" of the supervisory board; Federal Court of Justice, judgment of June 19, 2012 – II ZR 243/11, ZInsO 2012, 1536, 1538 [Insolvency – knowledge does not protect].
ignorance does not protect].

101 Worth reading: *Rack*, Manfred: Wer delegiert, muss kontrollieren oder haften – Die Haftung der Betriebsleiter, Abteilungsleiter und Führungskräfte des mittleren Managements mit ausdrücklichem Auftrag (Those who delegate must monitor or be liable – The liability of plant managers, department heads, and middle managers with explicit instructions), download at: *https://xn--rack-rechtsanwlte-3qb.de/upload/downloads/aufsaetze/Wer_delegiert.pdf*.

102 See LG Munich I, judgment of December 9, 2021 – 31 O 16606/20, openJur 2021, 46734.

What was special about this case was that it did not involve active misconduct on the part of current employees, but rather a failure to revoke authorizations after an external service provider left the company, in other words, excessive access by a former vicarious agent. Nevertheless, the company was held liable for the third party's breach of duty. The decision shows that, contrary to popular belief, the excess (in this case by a third party) does not automatically lead to exemption from liability if the company violates its control, monitoring, and organizational obligations.

4. Summary

A look at case law shows that excessive staffing raises fundamental questions of liability law—its dogmatic classification has so far only been partially addressed. Neither case law nor legal literature has yet developed a consistent set of criteria that sufficiently outlines the dogmatic prerequisites, scope, and limits of attribution in cases where individual employees exceed their duties. Whether the threshold for exemption from liability has been reached has therefore always requires a careful and differentiated analysis of the individual case. The dogmatic dividing line runs between delegated responsibility and structural failure – not between formal competence and actual control.

In the authors' view, the doctrine of excessive employee involvement is closely linked to the requirements of modern governance, preventive risk monitoring, and functional compliance structures. Excessive employee conduct terminates attribution—but not the obligation to exercise structural control through governance, CMS, and preventive system oversight. It is therefore always necessary to consider each case individually to determine whether excess actually leads to a release from liability. An effective CMS does not provide absolute protection, but it does establish the possibility of exemption from liability. If there are no mechanisms in place to fulfill the duty of supervision, responsibility remains with the company – even in the case of individual misconduct, unless the employee undermines the system with criminal intent through manipulation or deception.

The mere establishment of roles, powers, and responsibilities within an organization does not automatically lead to exemption from liability in the event of misconduct by individual employees. The decisive factor is whether a functioning control and monitoring system has been established that is suitable for preventing misconduct.

Recognizing and effectively preventing the misuse of rights, systems, or authority.
and effectively prevent them. Lack of control, failure to respond to warning signs, or
"trust organization without oversight" can lead to a finding of structural organizational failure in the fulfillment of supervisory duties and thus to attribution despite employee excesses. This must be prevented by appropriate structures. If, in turn, the employee circumvents these structures, it will be necessary to investigate the intention and manner in which this was done, as liability law recognizes

either guarantee liability based on the position of a manager or an obligation in cases of impossibility. Particularly in cases involving significant criminal energy and deliberate circumvention of the system, it may be objectively impossible to fulfill the duty of supervision, with the result that attribution is ruled out.

Employee excess liability relief applies where not only formal but also substantive mechanisms for supervision, control, and prevention are established and verifiably practiced (CMS), but also where these mechanisms are manipulated or circumvented with criminal intent—in all other cases, personal liability may apply.

X. Basel IV: New requirements and challenges for banks and financed organizations

The revision of Capital Requirements Regulation III (CRR III) came into force on January 1, 2025. The aim is to strengthen the resilience and stability of the banking sector through stricter rules for credit risk assessment and capital adequacy. This has implications for financed companies and increases the importance of a reputable rating: Organizations with a reputable external (good) rating generally receive better terms. A good rating should be established as a strategic goal, although there is still room for improvement: Only one in ten large companies (at least €500 million) has an external rating.

XI. New approaches to "ratings"/assessments based on information in sustainability, governance, or annual reports[104]

1. Indicator-based assessment of governance, resilience, and insolvency risk using AI

Approaches to assessing the probability of insolvency, resilience, future viability, and much more can be found in the Z, O, and Q score concepts developed by academics.

In the future, more comprehensive governance reporting in a uniform digital format, possibly via sustainability reports, will make organizations more transparent and enable new types of *indicator-based governance rating or scoring* using AI.

103 See Risknet editorial team, The role of risk management under Basel IV, 2024, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/* die-rolle-des-risikomanagements-unter-basel-iv/.

104 See *Gleissner/Wolfrum/Moecke*, The Supervisory Board, 2024, 110.

105 See Wikipedia – The Free Encyclopedia, Altmann Z-score, May 28, 2024, Wikipedia.de, available at: *https://en.wikipedia.org/w/index.php?title=-Altman_Z-score&oldid=1226107836* and Wikipedia – The Free Encyclopedia, Ohlsen O-score, December 8, 2024, Wikipedia.de, available at: *https:// en.wikipedia.org/w/index.php?title=Ohlson_O-score&oldid=1261889479.* See *Gleissner/Weissmann,* Das zukunftsfähige Familienunternehmen (The Future-Proof Family Business), Springer 2024, available at: *https://link.springer.com/content/pdf/10. 1007/978-3-658-42787-0.pdf.*

Targeted questions or prompts for the AI tools appropriate to the problem at hand help to evaluate key topics, requirements, key figures, etc. found in the information contained in the documents examined (e.g., annual reports) in a qualitative and/or (semi-)quantitative manner.

These results can provide indicators that trigger an in-depth, audit-proof investigation. For governance scoring, quantitative assessments—including those of business partners' annual reports—should be preferred over qualitative statements: "If you can't measure it, you can't manage it."[106]

2. Truthfulness and consistency check in reporting as a risk indicator

The accuracy of the statements in the documents/reports examined should also be checked: Do the qualitative statements correspond to the quantitative data? Are there any contradictions?

Appropriate AI-supported assessments enable risks to be identified at an early stage.

This is – especially in times of crisis and transformation – the duty of a conscientious body (Section 43 GmbHG, Sections 91, 93, 116 AktG, Section 347 HGB) and also a cardinal duty, the violation of which leads to the loss of (D&O) insurance coverage.

3. Truthfulness in annual reports

Strict compliance standards must also be applied to the accuracy of annual reports:

The new Green Claims Directive, whose abolition is already being discussed again, tightens many existing requirements.

Reporting – including with the help of AI – is accounting law and compliance, not marketing.

At the same time, the probability of compliance violations being detected in reporting in the context of green, white, and pink washing is increasing due to the establishment of whistleblowing.

a) Risks jeopardizing the continued existence of the company and lack of auditing

Management reports often state something along the lines of:

"As a result of the analysis of opportunities and risks, countermeasures, safeguards, and precautions, and in the opinion of the Management Board, based on the current risk assessment and our medium-term planning, there are no risks that could individually or collectively impair the assets, financial position, and earnings of the ... Group to an extent that would jeopardize its continued existence."

However, according to renowned risk management experts, this statement has not been verified at all in many companies, for example with the help of stress scenarios or similar and is therefore a potentially inaccurate – and often consequential – statement in the management report. No company is immune to risks that threaten its existence. Regardless of industry, size, or market experience, every organization has the potential to find itself in a situation that threatens its existence due to the occurrence of serious risks, such as market disruptions, regulatory changes, reputational damage, or operational crises.

b) Structural crises and latent threats to existence

Even highly profitable companies can find themselves in trouble in the short term due to external shocks or internal mismanagement if they do not have sufficient risk buffers, early warning systems, or resilience mechanisms in place.

This is particularly evident in companies that regularly rely on government subsidies or aid (see Meyer Werft, statutory health insurance funds, etc.) to ensure their continued operations. These companies are structurally exposed to a persistent latent threat to their existence, as their business model is not viable on its own under market conditions.

In the authors' view, it is also one of the tasks of the many supervisory functions, including *governance compliance* auditors, to scrutinize this appropriately.

Tip

Try to optimize your governance structures in order to meet the mandatory requirements of the relevant stakeholders you are assessing.

Evaluate your relevant stakeholders/business partners in order to identify their risks at an early stage.

106 This quote, often attributed to Peter Drucker or W. Edwards Deming, cannot be found in either of their works. W. Edwards Deming warned against purely number-driven management and counted pure management "by visible numbers" among the "seven deadly diseases." Peter Drucker also saw measurement as an important tool, but emphasized that good management always relies on judgment, experience, and intuition. Not everything that counts can be measured. According to the authors, good governance is essential as the core of ESGRC. However, data collection and analysis are also necessary, which are already part of ESGRC.

107 See Tagesschau, the convictions of DWS based on greenwashing allegations in the fund description, available at: *https://www.tagesschau.de/wirtschaft/finanzen/dws-millionenstrafe-greenwashing-100. html* and FuW, complaint against Shell for possible misleading of shareholders, 2023, available at: *https://www.fuw.ch/beschwerde-gegen-shell-wegen-moeglicher-irrefuehrung-der-aktionaere-445996836231.*

108 See *Romeike*, IDW ES 16 – Early crisis detection and crisis management pursuant to Section 1 StaRUG, 2025, RiskNET.de, available at: *https://www.risknet.de/themen/risknews/krisenfrueherkennung-und*-krisen*management-nach-1-*starug/.

4. Regulation of ESG ratings

It should be noted that ESG rating/scoring/certification is becoming increasingly important and strictly regulated:

On November 19, 2024, the EU adopted the *ESG Rating Regulation*,[109] which came into force 20 days after publication and will take legal effect 18 months later, i.e. *in mid-2026*, for the organizations concerned (rating providers, insurers, fund companies, and credit institutions that offer their customers free ratings).

The regulation stipulates that rating providers based in the EU must be authorized by ESMA, transparency, conflicts of interest, complaint mechanisms, and third-country authorization.

XII. Digression: Audit committees in public-interest entities within the meaning of Section 316a sentence 2 HGB (capital market-oriented companies, credit institutions, and insurers)

1. Rights to information and risk-based disclosure requirements

Pursuant to Section 107 (4) sentence 4 AktG, each member of the audit committee in companies of public interest may obtain information directly from the heads of the company's central departments, such as risk management, compliance management, accounting, auditing, internal control system, and internal audit, via the chairperson.

This right may, due to the supervisory board's duty to supervise the management board, develop into a *duty to obtain information*, whereby the *important* information must also be obtained on a risk-based basis.

This, in turn, requires an appropriate risk assessment or serves as a basis for risk assessment.

2. Compliance tasks of the audit committee

"(...) The compliance-related tasks of the audit committee have grown significantly in recent years. This is due to increasing legalization in the area of ESG and cyber issues, but also to a heightened awareness of the compliance relevance of these 'trend topics' within the company. The range of compliance issues that audit committees deal with intensively is now much broader than when the audit committee was introduced.

With the right to question managers at subordinate levels, the audit committee gains 'investigative powers' in compliance matters. (...)

(...) The annual reports of the DAX 40 companies from 2023 provide some indications that audit committee members are making use of this new right to information regarding compliance in practice. (...)" [111]

3. Expansion of monitoring duties

The measurable "tightening of the compliance obligations of the Management Board due to external and internal developments" would also increase the monitoring obligations of the Supervisory Board and the audit committees.

On the one hand, this involves an increase in new regulations in familiar areas of law. On the other hand, more and more new topics that were not previously regulated are being "legalized." For example, the technical topics of AI and information security are becoming the legal topics *of* AI and *information security compliance*. Similarly, decades ago, the field of corporate governance and supervision was essentially business-oriented and not subject to legal assessment or standardization. [112] This has now changed fundamentally, and *governance compliance* [113] has become one of the most relevant areas of law for corporate bodies and executives.

4. Trend topics, legal obligations, and competence requirements

"(...) General trends such as cybersecurity, data protection, climate risks, pandemics, and geopolitical uncertainties must now also be taken into account by the audit committee in its responsibility for monitoring compliance-relevant systems and structures.

Many of the areas of action mentioned have undergone increasing legalization in recent years, which has redefined the legal obligations of the management board in the context of its responsibility for the company. (...)" [114]

It is positive that annual reports increasingly mention that supervisory boards obtain information directly from the lines of defense functions in order to fulfill their monitoring role.

It should be noted here, however, that the Management Board and Supervisory Board are not responsible for addressing "trend topics," but rather issues that present relevant opportunities and risks for their organization. It is correctly stated that this requires training and continuing education as well as sound compliance expertise on the part of the executive bodies.

---

109 Regulation (EU) 2024/3005 of the European Parliament and of the Council of November 27, 2024, on transparency and integrity of environmental, social, and governance (ESG) rating activities and amending Regulations (EU) 2019/2088 and (EU) 2023/2859 was published in the EU Official Journal on December 12, 2024, available at: *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202403005.*

110 ESMA is the European Securities and Markets Authority.

111 See *Arnold/Reinhardt*, CCZ 2025, 60.

112 See *Scherer/Fruth*, Governance Management, Vol. I, 2015, 134: "Compliance dominates business administration."

113 The content on governance compliance can be found in *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025.

114 See *Arnold/Reinhardt*, CCZ 2025, 60.

XIII. Special case: Qualification matrix for executive board and supervisory board competence in annual reports

1. Significance and shortcomings of the qualification matrix

The qualification matrix in the annual report is intended to reflect the competencies of the individual members of the executive board and supervisory board.

Competencies in sustainability, governance, digitalization, and AI are increasingly being communicated.

However, an analysis of the qualification matrices from the 2023 annual reports of all companies listed on the DAX, MDAX, and SDAX stock indices revealed weaknesses:[115]

These may be purely self-assessments, and there is generally no information on the methodology used to determine the results, nor is there any external validation in accordance with "Fit & Proper."

Competence levels such as "basic knowledge, good knowledge, expert knowledge" and benchmarks/industry comparison analyses are also mostly missing.

This is therefore a useful tool that is not (yet) being implemented appropriately, as the accuracy of the information provided cannot usually be verified or checked.

2. Governance compliance audits and resilience scores: especially important in times of crisis

Here is a selection of audit check questions on the topics of governance compliance, resilience, and capital market viability:[116]

a) Understanding of the (legal) definitions in the area of governance[117]

- Are the relevant definitions for governance, risk management, and compliance in times of transformation with digitalization and sustainability (ESG) known, understood, and used consistently by the relevant body (lines of defense functions, managers, etc.)?
- Do the relevant addressees (bodies, lines of defense functions, managers, etc.) have adequate knowledge of "sustainable compliance and risk-based, conscientious management and supervision of organizations (governance)"? ([118])

b) Legal basis (compliance) for governance[119]

- Are the legal foundations for governance (management and supervision of organizations), digitalization, and sustainability known and is compliance with them ensured?
- Are the mandatory provisions (compliance) of corporate governance (ISO 37000:2021) observed?
- Are the *cardinal duties* of the executive bodies and senior executives known and is compliance with them ensured?
- Is there an effective legal department and compliance function?

c) Relevant benchmarks including standards for governance[121]

- In addition to the binding regulatory requirements for governance (see above), are relevant standards for governance, risk management, compliance, information security, etc. also used as benchmarks?

d) Bodies[122]

aa) Roles, tasks, rights, and duties

- Are there up to date, documented "role descriptions," business distribution plans, rules of procedure for the respective bodies, etc., and are the respective members of the governing bodies aware of their tasks and (liability) responsibilities and do they fulfill them?
- Are the members of the governing bodies regularly and effectively trained?

bb) Interaction

- Are appropriate governance structures (management and supervision of the organization)/interactions between shareholders, supervisory bodies, and management, as well as with department heads, ensured?

cc) Competencies

- Is the composition of the management (supervisory bodies/executive board/management/extended management) appropriate?

---

115 See ECBE Governance Perspectives 2024, Qualification Matrix & Supervisory Board Competence – An Analysis of the 2023 Annual Reports from the DAX Index Family, 2024, available at: *https://www.ecbe.com/assets/qualifikationsmatrix-und-aufsichtsratskompetenz-ecbe-governance-perspectives-2024.pdf.*

116 The questions were selected based on legal requirements, requirements of the German Federal Court of Justice (BGH) case law, *Achleitner/Kaserer/Günther/Volk*, Die Kapitalmarktfähigkeit von Familienunternehmen – Unternehmensfinanzierung über Schuldschein, Anleihe und Börsengang (The Capital Market Suitability of Family Businesses – Corporate Financing via Promissory Notes, Bonds, and IPOs), 2011, 59 ff., available at: *https://papers.ssrn.com/sol3/papers.cfm?-abstract_id=1791526,* and ISO Harmonized Structure: 2021.

117 See DIN ISO 37000, section 3.

118 The content on governance compliance can be found in *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, published by DIN, DIN Media-Verlag, 2025.

119 See DIN ISO 37000, standard section 1.

120 See the contents of governance compliance: *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025.

121 See DIN ISO 37000, section 2.

122 See DIN ISO 37000, section 4.3.

management) positively evaluated by competent and objective parties?

- Are the positions in the organization's management and supervisory bodies adequately filled?
- Is the first management and supervisory level adequately supported and, if necessary, represented by the second management level (staff positions/department heads)?

The complete list contains many more important governance compliance audit check questions.

Ideally, the answers to these questions should be found in the relevant sections of the *Integrated Corporate* Governance Report. A governance compliance audit could then be carried out in stage 1 with little effort to check whether the annual report contains the relevant information.

Audit stage 2 would then focus on verifying the reported information and on relevant topics not covered in the reports.

XIV. Governance compliance certifications

1. Accredited certification bodies and reference to standards

A certification body accredited for compliance management systems now offers CMS certification in accordance with DIN ISO 37301 with a special scope of the audit on (IT/AI) governance compliance based on DIN ISO 37000 and ISO/IEC 38500.

2. Certification successes in practice

Four of the clients we support in the area of compliance are among the first seven companies in Germany to be certified by the only certification body accredited for ISO 37301 (CMS) and 37001 (anti-corruption):

a) Hitzler Ingenieure GmbH & Co. KG

"Thanks to the expert, practical advice and support, we were able to introduce and certify our CMS quickly and efficiently – thank you very much for your commitment!"

– Ernst Neumann, Chief Financial Officer, Hitzler Ingenieure GmbH & Co. KG –

b) Congatec GmbH

"Preparing for CMS certification by GovSol was a significant step for our governance. The collaboration was professional, efficient, and, unlike the standard solutions offered by large consulting firms, tailored precisely to our needs. We are delighted with this milestone and the benefits it will bring to our company. Certification is the safest way to test the effectiveness of a CMS without having to wait for an emergency situation to arise.

– Stefan Markovic, Director Global Quality & Compliance Officer, Congatec GmbH –

c) Karl Group

"Due to the important governance compliance issues, the certification demonstrated the value contribution of the integrative function of a compliance management system in terms of QM, environment, etc. – a valuable investment."

– Quote from André Karl, Management Karl Group –

d) LASCO Umformtechnik GmbH

"The consulting services provided by GovSol and the internal audit it conducted prepared our employees optimally for the external certification audit. The in-depth analysis and practical measures helped us to successfully achieve ISO 37001 certification. This is a decisive step for our company."

– Lothar Bauersachs, Chairman of the Management Board, LASCO Umformtechnik GmbH –

XV. Value contributions

Investments in digitalization with AI, governance, risk, and compliance initially cost money. But they strengthen resilience and mean sustainable increases in company value and future viability. The empirical study by Gleißner, Günther, and Walkshäusl (2022)[125] shows that companies with high financial sustainability – measured against four key criteria (growth, probability of survival, acceptable risk exposure, and attractive risk/return profile) – achieve significantly higher risk-adjusted capital market returns. Companies that met all four criteria generated a monthly excess return of 0.39% compared to the market average between 1990 and 2019, while also taking on less risks.

Another currently indispensable value contribution of a governance compliance management system is its *exempting effect for the executive board, supervisory board, management, and shareholders*, in accordance with established supreme court rulings[126].

123 About *Governance Solutions GmbH.*

124 As of May 2025.

125 See *Gleißner/Günther/Walkshäusl*, Financial sustainability: measurement and empirical evidence, in: Journal of Business Economics, 2022, 467, as well as *Gleißner/Romeike*, FIRM Yearbook 2023, 125.

126 See, among others, BGH 2017: (KMW), judgment of May 9, 2017; BGH 2022: (Selbstreinigung), judgment of 27 April 2022; BGH 2023 (distribution of business), judgment of 9 November 2023; ECJ 2023: (Deutsche Wohnen), judgment of 5 December 2023; ECJ 2023: (hacker attack), judgment of December 14, 2023; ECJ 2024: (VAT fraud), judgment of January 30, 2024; ECJ 2024: (juris), judgment of April 11, 2024; OLG Stuttgart, decision of February 25, 2025 – 2 ORbs 16 Ss 336/24, NJW 2025, 1279 (employee ex
).

Department heads, compliance and risk managers, and other employees. [127]

XVI. Outlook and conclusions for practice

The countless serious daily events that pose a threat to life and limb, personal liability risks for executives and all employees of an organization, or significant financial losses, even leading to insolvency, show that the topic of governance cannot be treated with enough sensitivity.

The mandatory requirements and measures derived from governance may seem overwhelming, but they are not. If governance is used as an umbrella for the integrated management system (IMS), there will be numerous overlaps with elements already present in the IMS, and the tasks that need to be performed correctly will be distributed among many people.

Governance is primarily a matter for top management, i.e., it is the primary and ultimate responsibility of the company's management (e.g., managing director, executive board). Only through legally compliant delegation of duties can tasks and responsibilities be delegated to other competent functions.

However, governance also means that the supervisory board is responsible for monitoring management and that the shareholder has the power to issue instructions.

Everything that needs to be done in the area of governance must (!) be done. This is pure compliance without any discretion as to "whether" and thus bound decisions and, under certain circumstances, *"cardinal obligations*." There is also no risk appetite and no Pareto principle.

There is only the "risk-based approach": instead of doing everything at once – which is impossible – do the most important things first!

In order to avoid falling into the trap of personal liability due to accusations of a legally non-compliant organization, a *governance compliance management system that provides exemption from liability* is essential.

New developments in the business environment require new skills from management bodies and employees, but also from supervisory functions.

Training and continuing education should not miss out on this megatrend. The way in which these transformation requirements are being addressed is reflected in the non-financial business or sustainability reports of an increasing number of organizations.

Governance means, but not limited to, successfully guiding the organization and its people through the transformation as part of an effective change process despite scientifically proven "deliberate ignorance" [129] and typical human resistance.

Economic booster and systemic error: a bias that has hardly been questioned to date:[130]

The causes of insolvency, closures, and strategic failure often lie not in the external environment, but in internal company deficits—particularly in the area of legally standardized management responsibility. Even companies that should objectively benefit from the economic "boost" are stumbling when serious management mistakes are overlooked, mismanagement is tolerated, or early warning systems are not implemented in the first place.

The belief that economic stimulus measures such as the draft law passed by the German federal cabinet on June 4, 2025, dubbed the "investment, growth, or economic booster," which is an immediate tax investment program aimed at strengthening Germany as a business location, could compensate for structural deficiencies is an expression of a certain naivety and a bias that has hardly been questioned to date in the form of a cognitive distortion: the stability illusion is an expression of a certain naivety and a bias that has hardly been questioned to date in the form of a cognitive distortion: the stability illusion. As long as serious management errors – such as "management by blind flight [131]– persist and are not recognized, questioned or even implicitly covered up by supervisory bodies such as supervisory boards, auditors or the functions of the lines of defense, any external impetus will remain ineffective. Substantial improvement can only occur where governance structures are in place, early warning systems are effective, and information relevant to management is not only collected but also understood and used.

Under the impression of the illusion of stability created by an economic booster, there is a risk that managers will continue to

---

127 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Section 4.2 "Governance and Delegation."

128 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) According to DIN ISO 37000 – Successful Implementation, Auditing, and Reporting, DIN Media, 2025, Section 4.2 "Governance and Delegation."

129 See *Dörr*, Deliberate ignorance: On the obstacles to digital transformation and Schrödinger's cat, beck-aktuell, 2025, available at: *https://rsw.beck.de/aktuell/daily/meldung/detail/vorsaetzliche-ignoranz-justiz-behoerden-digitale-transformation-studie*.

130 See: The Federal Government, Growth boosters to strengthen Germany as a business location, 2025, available at: *https://www.bundesregierung.de/breg-de/aktuelles/kabinett-beschliesst-wachstumsbooster-2351752*; See BMF, Growth boosters approved by the cabinet: Planning security and incentives for private investment, press release 5/2025, available at: *https://www.bundesfinanzministerium.de/Content/DE/Pressemitteilungen/Finanzpolitik/2025/06/2025-06-04-kabinett-beschliesst-wachstumsbooster.html;* that., Draft law for an immediate tax investment program to strengthen Germany as a business location, available at: *https://www. bundesfinanzministerium. de/ Content/ DE/ Gesetzestexte/ Gesetze_ Gesetzesvorhaben/Abteilungen/Abteilung_IV/20_Legislaturperiode/2025-06-04-steuerliches-Investitionssofortprogramm/0-Gesetz.html.*

131 Based on: OLG Frankfurt/M., decision of January 16, 2025 – 7 W 20/24, NJW-RR 2025, 731: "blindly sailing into the crisis" and OLG Frankfurt/M., judgment of March 5, 2025 – 7 U 134/23, DStR 2025, 917, with a similar case (appeal lodged, Federal Court of Justice – IV ZR 66/25).

be aware that Section 1 StaRUG has established a non-delegable obligation to establish effective risk and early warning systems since 2021. This obligation is an expression of the duty of legality and has direct relevance under liability law via Section 43 GmbHG and Section 93 AktG. In its ruling of March 5, 2025 [132], the Higher Regional Court of Frankfurt/Main clarified that anyone who fails to comply with this obligation is regularly acting "knowingly in breach of duty" and runs the risk of being excluded from liability under Section 81 (2) VVG. Managing directors who, despite internal indications, external signals, or reliable key figures, act in "management by blind flight" mode are acting outside the scope of protection of the business judgment rule.

Governance without control, compliance without monitoring, and risk management without aggregation do not lead to resilience but rather to the illusion of legal protection in the event of actual control failure. Without preventive corporate management in the sense of an integrated ESGRC approach, any economic booster remains a flash in the pan—economically ineffective and dangerous in terms of liability law. [133]

132 Ref. 7 U 134/23.

133 See *Scherer*, Sustainable Management and Monitoring of Organizations (Governance) according to ISO 37000, DIN Media 2025, 92 ff.; *ibid.*, ESGRC, Gabler Business Dictionary (online edition), 2024, (The ESGRC model combines ecological, social, and legal-normative requirements with an internal corporate management logic in which governance acts as a connecting link and, as a normative control framework, ensures the connection between risk, compliance, and sustainable corporate management), available at: *https://wirtschaftslexikon.gabler.de/definition/ esgrc-126420/version-390788.*