FIRM
Frankfurter Institut für Risikomanagement und Regulierung

Resilience, goal achievement and sustainability in the age of transformation

The revised *guidelines on internal governance* of the *European Banking* Authority (EBA) and the *guidelines on the assessment of the suitability of members of the management body and key function holders* of the *EBA* and the *European Securities and Market Authority (ESMA*) have been in force since December 31, 2021.

When studying the guidelines, the need for modern governance adapted to the times of transformation becomes clear. The addressees also get a feeling for what is included in the area of governance and which regulatory requirements need to be met. There is no fundamental discussion of the concept and legal scope of governance as a whole in the guidelines, meaning that there is still a need for further discussion, qualification and action in this respect.

BAFIN'S "SUSTAINABLE FINANCE STRATEGY"

Governance (as the G in ESG) also plays a significant role in *BaFin* 's "Sustainable Finance Strategy". In the absence of an in-depth discussion of what the non-legally defined terms *governance, governance compliance* and *governance reporting compliance* mean in concrete terms, it is worth differentiating and legally deriving these topics on the basis of (international) reference values.

The new DIN ISO 37000 standard for the governance of organizations may help here.

DIN ISO 37000:2024 GUIDANCE FOR THE GOVERNANCE OF ORGANIZATIONS

In the 3rd quarter of 2024, the ***DIN ISO 37000:2024*** (as the German translation of the English, internationally recognized standard) will be published.

TARGET GROUP

This non-certifiable guide for all types and sizes of organizations, including financial players such as credit institutions and insurers, is an important guide for executive bodies (managing directors, board members, supervisory board members, etc.), managers and stakeholders, especially in times of multiple crises and transformation.

Shareholders, investors, lenders and business partners include the topics covered in this standard, which are also the focus of annual and sustainability reports, in their assessments (rating, scoring, due diligence).

GOVERNANCE AS A COMPLIANCE REQUIREMENT

Governance is not legally defined. In legal terms, the term can be defined as "*sustainable, compliance- and risk-based conscientious management and monitoring of organizations, including interaction with relevant stakeholders*".

The sensible recommendations of ISO 37000:2021 and DIN ISO 37000:2024 barely address legally binding governance requirements. However, these take precedence over the recommendations of standards (principle of legality and duty of compliance).

To help with this, DIN is publishing a commentary on DIN ISO 37000 in autumn 2024: Scherer, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, 2024.

TRANSFORMATION GOVERNANCE

Economic, social and environmental sustainability (ESG), regulation with governance, risk management (see ISO 31000) and compliance management (see DIN ISO 37301), as well as digitalization and artificial intelligence (see ISO 42001) are the new megatrends of transformation.

The *United Nations Sustainable* Development Goals (17 UN Sustainable Development Goals, 2016) have no less a goal than the sustainable and humane survival of humankind. Achieving these goals requires appropriate contributions from nations, private individuals, but above all from *all types of organizations with appropriate governance* and a sustainable mission

statement/purpose (Section 6.1, *Purpose*).

Sustainable livelihoods ("Financial Governance" – sections 6.2, *Value Creation*) and 6.11 ("Viability") require the successful implementation of a structured concept in this still very unfamiliar terrain.

The predominantly legally regulated "Governance-G" plays the key role in ESGRC and sustainability reporting and shows how sustainability, compliance, quality, risk, information security and other management systems can be integrated under the umbrella of "governance" (standard section 4.2.1 contains the approach of an *integrated governance management system*).

Section 4.2.2 *Governance and delegation* deals with the proper and *legally compliant transfer of entrepreneurial duties (delegation of duties)*:

Recently, the *Federal Fiscal Court* condemned a managing director for incorrect delegation and advised not to take up the office of a management body at all or to resign as soon as possible if one did not have sufficient powers to do so.

Section 4.2.4 *Governance and sustainability* addresses new requirements, regulations and reporting obligations in the area of *ESG*. Sustainability compliance goes far beyond the fulfillment of reporting obligations under the CSRD (Corporate Sustainability Reporting Directive), LKSG (Supply Chain Duty of Care Act), Taxonomy Regulation, CSDDD (Corporate Sustainability Due Diligence Directive), Green Claims Directive, etc. while avoiding *green, blue and white washing*.

Sections 4.3 (*The supreme body)*, 4.3.1 (*Composition)* and 4.3.2 (*Competencies)* deal with the appropriate interaction of the relevant bodies, which must be equipped with competencies ("fit & proper") that meet current requirements. Without this, an organization will hardly achieve its goals.

A recent study by PWC (see press release dated 26.6.2024: Advisory boards in family businesses are still too yesterday's news for a successful tomorrow) criticizes the fact that only around 25 percent of advisory boards in family businesses are currently equipped with the skills required to master the transformation.

In addition, Nobel Prize winners in economics, such as Daniel Kahneman (“Thinking fast and slow” and “Noise”) and Richard Thaler (“Nudge”), have proven that humans are subject to many cognitive distortions, heuristics, patterns, etc. when thinking, deciding and acting.

Section 6.3 (*Strategy)* highlights the particular importance of deriving appropriate strategies in a highly volatile environment as a duty of the executive bodies that gives rise to liability. The “principles of proper planning” should be observed here. Section 6.9*(Risk governance)* also comes into play at this point, as the right objectives can neither be set nor achieved without appropriate risk governance.

In this context, it is significant that the German *Federal Court of Audit* repeatedly complains that strategic concepts (e.g. reform of the healthcare system) lack worst-case scenarios.

Section 6.5 (*Responsibility)* explains the civil, criminal and administrative liability of the organization, governing bodies, managers and other employees, as well as the liability-limiting effect of lines-of-defense systems, which are dealt with in section 6.4*(Supervision)*.

In this regard, there have recently been numerous rulings by the *German Federal Court of Justice (BGH*) and *the European Court of Justice (ECJ)* which recognize the discharging effect of governance systems (compliance management, risk management, ICS) for executive bodies if breaches of duty have been committed by employees below management level.

Section 6.8 (*Data and decisions)* addresses data governance, IT and AI governance as the basis for “good business decisions” (“business judgment rule”) and the achievement of objectives. In times of cybercrime, hacker attacks and terrorist attacks on critical infrastructure, ensuring *risk-based thinking, decisions and actions* in the organization is not just about information security. The new *ISO 38500:2024 IT governance* is structured in the same way as sections 6.1 to 6.11 of DIN ISO 37000.

Section 6.10 (*Social responsibility)* shows the connection between governance and corporate or public social responsibility (see DIN ISO 26000) and sustainability reporting in the area of *social sustainability and human rights* in accordance with the European Sustainability Reporting Standards ESRS S 1 to S 4. Corporate health management (see DIN EN ISO 45001) also plays a key role here.

Section 6.11 (*Securing sustainable existence and profitability)* deals with topics such as early risk detection (see Section 1 of the Act on the Stabilization and Restructuring of Companies, StaRuG), business continuity management (see DIN ISO 22301) and crisis governance (see DIN EN ISO 2236) to ensure resilience and financing of the transformation.

CONCLUSION

In the current times of transformation and crises, appropriate and effective governance is the prerequisite for achieving the goals of financial players, but also the sustainability goals of the United Nations, and is therefore not only vital for the survival of all types of organizations, but also for humanity itself.

AUTHOR

Prof. Dr. Josef Scherer

Mitglied des Beirats
PROF. DR. SCHERER DR. RIEGER & MITTAG PARTNERSCHAFT MBB