FIRM
Frankfurter Institut für Risikomanagement und Regulierung

Resilienz, Zielerreichung und Nachhaltigkeit im Zeitalter der Transformation

Von Josef Scherer

Die revisionierten *Leitlinien zur internen Governance* der *Europäischen Bankenaufsicht* (EBA) und die *Leitlinien zur Beurteilung der Eignung von Mitgliedern des Leitungsorgans und von Inhabern von Schlüsselfunktionen* der *EBA* und der *Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA, European Securities and Market Authority*) gelten seit dem 31.12.2021. Beim Studium der Leitlinien wird der Bedarf an einer modernen, den Zeiten der Transformation angepassten Governance deutlich. Ebenso bekommen die Adressaten ein Gefühl, was alles zum Bereich Governance zählt und welche regulatorischen Anforderungen zu erfüllen sind. Eine grundlegende Auseinandersetzung mit dem Begriff und dem rechtlichen Umfang von Governance insgesamt findet sich in den Leitlinien nicht, so dass insoweit noch weiterer Diskussions-, Qualifizierungs- und Handlungsbedarf besteht.

DIE „SUSTAINABLE FINANCE STRATEGIE“ DER *BAFIN*

Governance (als das G in ESG) spielt auch in der „Sustainable Finance Strategie“ der *BaFin* eine erhebliche Rolle. Mangels vertiefter Auseinandersetzung, was die nicht legal-definierten Begriffe *Governance, Governance-Compliance* und *Governance-Reporting-Compliance* konkret bedeuten, lohnt sich eine Differenzierung und juristisch greifbare Herleitung dieser Themen auf Basis (internationaler) Referenzgrößen.

Möglicherweise hilft hierbei die neue DIN ISO 37000 für die Governance von Organisationen.

DIN ISO 37000:2024 ANLEITUNG FÜR DIE GOVERNANCE VON ORGANISATIONEN

Im 3. Quartal 2024 wird die ***DIN ISO 37000:2024*** (als deutsche Übersetzung der englischen, international anerkannten Norm) erscheinen.

ZIELGRUPPE

Dieser nicht zertifizierbare Leitfaden für alle Arten und Größen von Organisationen, also auch Finanzakteure, wie Kreditinstitute und Versicherer, ist gerade in Zeiten von multiplen Krisen und Transformation ein wichtiger Ratgeber für Organe (Geschäftsführer, Vorstände, Bei- oder Aufsichtsräte etc.), Führungskräfte und Stakeholder.

Gesellschafter, Investoren, Kreditgeber und Business Partner beziehen die in dieser Norm behandelten Themen, die auch in Geschäfts- und Nachhaltigkeitsberichten im Fokus stehen, in ihre Bewertungen (Rating, Scoring, Due Diligence) ein.

GOVERNANCE ALS COMPLIANCE-ANFORDERUNG

Governance ist nicht legal-definiert. Der Begriff lässt sich juristisch hergeleitet als „*nachhaltige, compliance- und risikobasierte gewissenhafte Führung und Überwachung von Organisationen inklusive Interaktion mit relevanten Stakeholdern*“ definieren.

Die sinnvollen Empfehlungen der ISO 37000:2021 bzw. der DIN ISO 37000:2024 gehen kaum auf rechtlich zwingend zu beachtende Anforderungen an Governance ein. Diese haben jedoch Vorrang vor den Empfehlungen von Standards (Legalitätsprinzip und Pflicht zur Compliance).

Um auch hierbei zu unterstützen, veröffentlicht die DIN im Herbst 2024 eine Kommentierung der DIN ISO 37000: Scherer, Nachhaltige Führung von Organisationen (Governance) nach DIN ISO 37000, 2024.

TRANSFORMATIONS-GOVERNANCE

Ökonomische, soziale und ökologische Nachhaltigkeit (ESG), Regulierung mit Governance, Risikomanagement (vgl. ISO 31000) und Compliance-Management (vgl. DIN ISO 37301), sowie Digitalisierung und Künstliche Intelligenz (vgl. ISO 42001) sind die neuen Megatrends der Transformation.

Die *Nachhaltigkeitsziele der Vereinten Nationen* (17 UN Sustainable Development Goals, 2016) haben kein geringeres Ziel als das nachhaltige und menschenwürdige Überleben der Menschheit. Um diese Ziele zu erreichen, sind angemessene Beiträge durch Nationen, Privatpersonen, aber vor allem auch *jegliche Arten von Organisationen mit angemessener Governance* und nachhaltigen Mission Statement / Purpose (Abschnitt 6.1, *Zweck*) erforderlich.

Nachhaltige Existenzsicherung („Financial Governance" – Abschnitte 6.2, *Wertschöpfung*) und 6.11 („Viability") erfordern die erfolgreiche Umsetzung eines strukturierten Konzeptes in diesem noch sehr unbekannten Terrain.

Das überwiegend juristisch geregelte „Governance-G" spielt dabei die Schlüsselrolle in ESGRC und Nachhaltigkeitsberichterstattung und zeigt, wie sich Nachhaltigkeits-, Compliance-, Qualitäts-, Risiko-, Informationssicherheits- und weitere Managementsysteme unter dem Dach „Governance" integrieren lassen (Normabschnitt 4.2.1 enthält den Ansatz eines *Integrierten Governance-Managementsystems*).

Im Abschnitt 4.2.2 *Governance und Delegation* spielt das Thema der ordnungsgemäßen bzw. *rechtssicheren Übertragung von Unternehmerpflichten (Pflichtendelegation)*:

Unlängst verurteilte der *Bundesfinanzhof* einen Geschäftsführer wegen fehlerhafter Delegation und riet, bei unzureichenden Kompetenzen für das Amt eines Leitungsorgans, dieses gar nicht anzutreten oder schleunigst niederzulegen.

Abschnitt 4.2.4 *Governance und Nachhaltigkeit* thematisiert neue Anforderungen, Regularien und Berichtspflichten im Bereich *ESG.* Nachhaltigkeits-Compliance geht weit über die Erfüllung der Berichtspflichten aus CSRD (Corporate Sustainability Reporting Directive), LKSG (Lieferkettensorgfaltspflichten-Gesetz), Taxonomie-Verordnung, CSDDD (Corporate Sustainability Due Diligence Directive), Green Claims Directive etc. unter Vermeidung von *Green-, Blue- und White-Washing* hinaus.

In den Abschnitten 4.3 (*Das Oberste Organ)*, 4.3.1 (*Zusammensetzung)* und 4.3.2 (*Kompetenzen)* wird auf angemessene Interaktion der relevanten Organe, die mit den aktuellen Anforderungen gerecht werdenden Kompetenzen („Fit & Proper") ausgestattet sein müssen, eingegangen. Ohne diese wird eine Organisation kaum ihre Ziele erreichen.

Eine aktuelle Studie von PWC (vgl. Pressemitteilung vom 26.6.2024: Beiräte in Familienunternehmen sind heute noch zu sehr von gestern für ein erfolgreiches Morgen) moniert, dass derzeit nur etwa 25 % der Beiräte von Familienunternehmen mit den zum Meistern der Transformation erforderlichen Kompetenzen ausgestattet sind.

Darüber hinaus haben Wirtschaftsnobelpreisträger, wie beispielsweise Daniel Kahneman („Thinking fast and slow" und „Noise") und Richard Thaler („Nudge"), bewiesen, dass der Mensch an sich beim Denken, Entscheiden und Handeln vielen kognitiven Verzerrungen, Heuristiken, Mustern etc. unterliegt.

Abschnitt 6.3 (*Strategie)* zeigt die besondere Bedeutung der Ableitung angemessener Strategien in einem höchst volatilen Umfeld als haftungsbewehrte Pflicht der Organe auf. Die „Grundsätze ordnungsgemäßer Planung" sollten hier Beachtung finden. Bereits an dieser Stelle kommt auch Abschnitt 6.9 (*Risk Governance)* zum Tragen, da ohne angemessene Risk Governance weder die richtigen Ziele gesetzt noch erreicht werden können.

Bezeichnend ist in diesem Zusammenhang, dass der *Bundesrechnungshof* immer wieder moniert, dass strategische Konzepte (z.B. Reform des Gesundheitswesens) Worst-Case-Szenarien vermissen lassen.

Im Abschnitt 6.5 (*Verantwortung)* wird die zivil-, straf- und bußgeldrechtlichen (Haftungs-) Verantwortung der Organisation, von Organen, Führungskräften und sonstigen Beschäftigten erläutert, ebenso wie die haftungsbeschränkende Wirkung von Lines-of-defense-Systemen, die im Normabschnitt 6.4 (*Aufsicht)* behandelt werden.

Hierzu gab es in jüngster Zeit zahlreiche Urteile des *Bundesgerichtshofes (BGH)* und *des Europäischen Gerichtshofes (EuGH)*, die die enthaftende Wirkung von Governance-Systemen (Compliancemanagement, Risikomanagement, IKS) für Organe anerkennen, wenn Pflichtverstöße von Beschäftigen unterhalb der Leitungsebene begangen wurden.

Im Abschnitt 6.8 (*Daten und Entscheidungen)* werden Data-Governance, IT- und KI-Governance als Basis für „gute unternehmerische Entscheidungen" („Business Judgment Rule") und Zielerreichung angesprochen. Die Sicherstellung von *risikobasiertem Denken, Entscheiden und Handeln* in der Organisation hat dabei in Zeiten von Cyber Crime, Hackerangriffen und terroristischen Attacken auf kritische Infrastruktur nicht nur mit Informationssicherheit zu tun. Die neue *ISO 38500:2024 IT-Governance* ist analog zu den Abschnitten 6.1 bis 6.11 der DIN ISO 37000 aufgebaut.

Abschnitt 6.10 (*Soziale Verantwortung)* zeigt den Zusammenhang zwischen Governance und Corporate oder Public Social Responsibility (vgl. DIN ISO 26000) und Nachhaltigkeits-Berichterstattung im Bereich *Soziale Nachhaltigkeit und Menschenrechte* gemäß den European Sustainability Reporting Standards ESRS S 1 bis S 4. Hierbei spielt auch das Betriebliche Gesundheitsmanagement (vgl. DIN EN ISO 45001) eine wesentliche Rolle.

Im Abschnitt 6.11 (*Nachhaltige Existenzsicherung und Wirtschaftlichkeit)* werden Themen, wie Risiko-Früherkennung (vgl. § 1 des Gesetzes zur Stabilisierung und Restrukturierung von Unternehmen, StaRuG), Business Continuity-Management (vgl. DIN ISO 22301) und Krisen-Governance (vgl. DIN EN ISO 2236) zur Sicherstellung von Resilienz und Finanzierung der Transformation behandelt.

FAZIT

Angemessene und wirksame Governance ist in den aktuellen Zeiten der Transformation und Krisen die Voraussetzung zur Erreichung der Ziele der Finanzakteure, aber auch der Nachhaltigkeitsziele der Vereinten Nationen und damit nicht nur überlebenswichtig für alle Arten von Organisationen, sondern auch für die Menschheit an sich.

AUTOR

Prof. Dr. Josef Scherer

Mitglied des Beirats

PROF. DR. SCHERER DR. RIEGER & MITTAG PARTNERSCHAFT MBB