Businessplan Komitee 265

1 Titel und thematischer Aufgabenbereich

1.1 Titel

de: Governance und Compliance
en: Governance and Compliance

1.2 Thematischer Aufgabenbereich

de:

- Entwicklung von Normen und Werkzeugen für die Planung, Einführung, Aufrechterhaltung und Überprüfung von regelkonformen Verhalten in Organisationen, unabhängig von deren Größe und Art.,
- Spiegelkomitee zu ISO/TC 309 Governance of organizations.

en:

- Development of standards and tools for planning, introducing, maintaining, and checking compliant behavior in organizations, regardless of their size and type.
- Mirror committee to ISO/TC 309 Governance of organizations.

2 Markt, Umfeld und Ziele des Komitees/Workshops

2.1 Marktsituation

2.1.1 Grundsätzliche Informationen über den Markt

In einem dynamischen und komplexen Geschäftsumfeld ist eine gute Unternehmensführung maßgeblich für die Erreichung der Unternehmensziele. Gute Governance ist der Grundstein für die Einhaltung gesetzlicher Vorschriften und ethischem Verhalten, für ein effektives Risikomanagement und eine effiziente Entscheidungsfindung, und damit für eine langfristige Nachhaltigkeit bei der Ausübung der Geschäftstätigkeit. Ebenso wird das Vertrauen von Eigentümern, Mitarbeiter und weiterer Stakeholder gestärkt. Darüber hinaus verschaffen sich Unternehmen, die für ihre gute Unternehmensführung bekannt sind, häufig einen Wettbewerbsvorteil in einem Umfeld, in dem Transparenz und verantwortungsvolles Handeln zunehmend geschätzt werden.

Als Beitrag für die Standardisierung von Governance in Bezug auf Leitung, Aufsicht und Rechenschaftspflicht von Organisationen wurde unter der Verantwortung des ISO/TC 309 der internationale *Standard ISO 37000:2021 Governance von Organisationen – Leitlinien* publiziert. Der Standard bildet einen integrierten organisatorischen Governance-Rahmen ab, um durch Stärkung von Kultur, Resilienz und Wertschöpfung die Zielerreichung voranzutreiben und eine nachhaltige Entwicklung der Organisation sicherzustellen. Compliance nimmt innerhalb dieses Governance-Rahmens eine zentrale Stellung ein.

Compliance bzw. regelkonformes Verhalten (auch Regelkonformität) ist in der Fachsprache der Begriff für die Einhaltung von Gesetzen und sonstigen verbindlichen Vorschriften, von organisationsinternen Vorgaben und freiwilliger Kodizes. Compliance bedeutet ebenso die Gestaltung des Verhaltens der Mitarbeiter der Organisation und ist weder ein branchenspezifisches noch ein größenabhängiges Thema. Mangelnde Compliance stellt nicht nur ein bedeutendes unternehmerisches Risiko dar, sondern kann zu einer Sanktionierung sowie zu sonstigen schwerwiegenden Konsequenzen sowohl für die Organisation an sich als auch zu straf- und zivilrechtlicher Verantwortung der Organisationsleitung führen. Ebenso drohen Reputationsschäden.

Abhängig von der Geschäftstätigkeit beziehen sich Compliance-Verpflichtungen gängiger Weise auf folgende (Rechts-)Materien (die nachfolgende Aufzählung erhebt nicht den Anspruch auf Vollständigkeit):

- Antikorruption,
- Datenschutz,
- Betrug (Fraud),
- Kartell- und Wettbewerbsrecht,
- Exportkontrolle,
- Sorgfaltspflicht in den Lieferketten,
- Geldwäsche,
- Menschenrechte,
- Hinweisgeberschutz,
- Kapitalmarkt,
- Aufsichtsrecht (z. B. Bankwesengesetz (BWG), Wertpapieraufsichtsgesetz (WAG) und Telekommunikationsgesetz (TKG))

Nicht effektive Compliance-Maßnahmenkönnen einer Organisation nachhaltig schaden bzw. diese unnötig in deren Geschäftsabläufen behindern. Kritische Elemente sind beispielsweise der Umgang mit Verdachtsfällen und der Einsatz von Überwachungsinstrumenten, die jedoch ihrerseits zu Verstößen von Rechtsvorschriften führen könnten. In Managementsystem-Normen wie Qualitätsmanagementsysteme (ISO 9001), Umweltmanagementsysteme (ISO 14001), Energiemanagementsysteme (ISO 50001), Informationssicherheits-Managementsysteme (ISO/IEC 27001), Managementsystem für Aufzeichnungen ISO 30300), Managementsysteme für die Lebensmittelsicherheit (ISO 22000) oder Risikomanagement (ISO 31000, ONR 49000ff) finden sich lediglich Teilelemente eines ganzheitlichen Compliance-Systems. So ist zum Beispiel grundsätzlich zwischen einem Compliance-Audit und einem System-Audit zu unterscheiden. Beispielsweise wird bei ISO 14001 auditiert, ob bei dem Umweltmanagementsystem in der Organisation Prozesse und Verfahren vorhanden sind, die die Konformität mit anwendbaren Rechtsvorschriften sicherstellen können. Wird bei einem ISO 14001-Audit eine rechtliche Non-Compliance festgestellt, weist dies auf ein mögliches System-Problem hin, zum Beispiel bei der Schulung, Führung von Aufzeichnungen, Überwachung und Messung.

Der Notwendigkeit einer ganzheitlichen, systemischen Sicht auf Compliance in einer Organisation Rechnung tragend wurden auf ISO-Ebene unter der Verantwortung des ISO/TC 309 mehrere Managementsystem-Normen veröffentlicht:

- *ISO 37001:2016 Managementsysteme zur Korruptionsbekämpfung – Anforderungen mit Leitlinien zur Anwendung.*
- *ISO 37301:2021 Compliance-Managementsysteme - Anforderungen mit Leitlinien zur Anwendung,*
- *ISO 37002:2022 Hinweismanagementsysteme – Leitlinien*
- *ISO 37008:2023 Internal investigation of organisation - Guidance*.

Compliance-Management Systeme bieten die Möglichkeit, für den jeweiligen Einsatzbereich (Compliance-Verpflichtung, Organisationseinheit) systematisch und strukturiert Anforderungen (der Kunden und aus

Rechtsvorschriften) zu identifizieren bzw. zu erheben, Maßnahmen zu deren Einhaltung zu entwickeln und deren Umsetzung organisationsweit zu kommunizieren bzw. dahingehend Bewusstsein zu schaffen, ihre Einhaltung zu messen bzw. regelmäßig zu auditieren und zu dokumentieren sowie bei Nichtkonformitäten gegenzusteuern.

Auch in dem Leitfaden zur gesellschaftlichen Verantwortung von Organisationen (ISO 26000) finden sich Teilaspekte eines Compliance-Systems, wobei in dieser Internationalen Norm der Schwerpunkt auf das, was überwacht werden sollte gesetzt wird, z. B. Anti-Korruption, fairer Wettbewerb u.dgl.

2.1.2 Interessensträger des Themas

Zu den interessierten Kreisen (Stakeholdern) zählen:

1. Organisationen des privaten Sektors jeglicher Größe und Art
2. Behörden, öffentliche Verwaltung
3. Branchenübergreifende Interessenvertretungen und Vereine, wie z. B. Wirtschaftskammer, Industriellenvereinigung
4. Nichtregierungsorganisationen (NGOs)
5. Zertifizierungsstellen
6. Forschung und Einrichtung der Wissenschaft, wie z.B. Universitäten

Folgende Funktionen der unter 1. bis 6. genannten Kreise sind beispielsweise relevant:

a. Organisationsleitung (z. B. Geschäftsführung, Vorstand),
b. Governance und Stakeholder Management,
c. Compliance und Rechtsabteilung,
d. Finanz- und Controlling,
e. Datenschutz- und Datensicherheitsbeauftragte, CIO
f. Interne Revision,
g. Personalwesen,
h. Rechtsabteilungen,
i. Risikomanager.

2.1.3 Marktstruktur

In Österreich sind die überwiegende Zahl der Unternehmen Klein- und Mittelbetrieb (KMUs). Gerade für diese Zielgruppe ist es erforderlich, geeignete, allgemein anerkannte Handlungsanleitungen für eine effektive und effiziente Unternehmensführung zur Verfügung zu haben. In jedem Unternehmen – selbst in den kleinsten – kann es zu Regelverstößen kommen. Wie sinnvoll die Implementierung eines umfassenden Compliance-Management-Systems (CMS) ist, hängt von mehreren Faktoren ab, u.a.: Branche, potenzielles Risiko, Unternehmensgröße, Unternehmenskultur, Eintrittswahrscheinlichkeit eines Compliance-Verstoßes-. In der Praxis sind es – laut einer Studie von LexisNexis aus dem Jahr 2021 – mehrheitlich Unternehmen aus den Branchen Industrie, Banken/Finanzen und Versicherungen sowie des öffentlichen Sektors, die professionelle Compliance-Systeme nutzen. Dies beinhaltet einerseits vorsorgliche Maßnahmen, wie die Aufklärung, Information und Schulung von Mitarbeiterinnen und Mitarbeitern, stellt aber auch andererseits die Überwachung unternehmensinterner Vorgänge sicher.

2.1.4 Europäische und internationale Perspektiven

Auf europäischer Ebene sind die Bereiche Governance und Compliance durch einen sich laufend entwickelnden Rahmen gekennzeichnet, der darauf abzielt, Geschäftspraktiken innerhalb der Europäischen Union (EU) zu harmonisieren und zu regulieren, um einen einheitlichen Markt mit einheitlichen Regeln und Standards zu schaffen, der die wirtschaftliche Integration zwischen den Mitgliedstaaten fördert. Umfassende Regulierungsrahmen gibt es u.a. betreffend:

- Umwelt-, Sozial- und Governance-Faktoren (ESG) – durch Vorschriften und Berichtspflichten haben Unternehmen ökologische und soziale Auswirkungen ihrer Geschäftstätigkeit sowie die ethischen Aspekte der Unternehmensführung zu berücksichtigen.
- Berichterstattung und Transparenz – die Richtlinie zur nichtfinanziellen Berichterstattung (NFRD) verlangt von bestimmten großen Unternehmen, in ihren Jahresberichten nichtfinanzielle Informationen, einschließlich Umwelt- und Sozialdaten, offenzulegen.
- Datenschutz und Privatsphäre – durch die Allgemeine Datenschutzgrundverordnung (DSGVO) werden Unternehmen erhebliche Compliance-Verpflichtungen in Bezug auf den Umgang personenbezogenen Daten auferlegt.
- Geldwäsche – die Richtlinien zur Bekämpfung der Geldwäsche (AMLD) verpflichtet Finanzinstitute und bestimmte andere Unternehmen zur Umsetzung von Maßnahmen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung.

Auf internationaler Ebene widmen sich zahlreiche Organisationen und Institutionen den Themen Governance und Compliance, wie zum Beispiel:

- UN Global Compact als eine freiwillige Initiative, die Unternehmen und Organisationen dazu ermutigt, Grundsätze in den Bereichen Menschenrechte, Arbeit, Umwelt und Korruptionsbekämpfung zu übernehmen.
- OECD Leitlinien für multinationale Unternehmen enthalten Empfehlungen für verantwortungsvolle Geschäftsführung und adressieren ebenso Bereiche wie Menschenrechte, Arbeit, Umwelt, Korruptionsbekämpfung und sowie Verbraucherschutz.
- OECD-Übereinkommen zur Bekämpfung von Bestechung verpflichtet als ein rechtsverbindliches internationales Instrument die Unterzeichnerstaaten, Bestechung ausländischer Amtsträger unter Strafe zu stellen und wirksame Durchsetzungsmechanismen einzurichten.
- Sarbanes-Oxley Act (SOX) als Regelung für in den USA börsennotierte Unternehmen enthält Vorschriften zu Corporate Governance, internen Kontrollen und Finanzberichterstattung.
- Übereinkommen der International Labor Organisation (ILO) legen Arbeitsnormen fest, die sich mit den grundlegenden Arbeitnehmerrechten befassen, darunter Vereinigungsfreiheit, Tarifverhandlungen, Kinderarbeit, Zwangsarbeit und Nichtdiskriminierung am Arbeitsplatz.
- Übereinkommen der Vereinten Nationen gegen Korruption (United Nation Convention Against Corruption, UNCAC) ist ein umfassender internationaler Vertrag zur Verhinderung und Bekämpfung von Korruption, Bestechung, Unterschlagung und Vermögensabschöpfung befasst.
- Transparency International: Business Principles for Countering Bribery.
- US Foreign Corrupt Practices Act (FCPA) verbietet bestimmten Gruppen von Personen und Organisationen Zahlungen an ausländische Regierungsbeamte zu leisten, um bei der Anbahnung oder Aufrechterhaltung von Geschäften behilflich zu sein.
- Seven Elements of an Effective Compliance Program des 2023 Guidelines Manuals (§8B2.1) der US Sentencing Commission.
- UK Bribery Act 2010 schafft in Abschnitt 7 den „weitreichenden und innovativen Straftatbestand“ des Versäumnisses kommerzieller Organisationen, Bestechung in ihrem Namen nicht zu verhindern.
- Richtlinien zum UK Bribery Act 2010 über Maßnahmen zur Vorbeugung von Bestechung (6 Principles for “Adequate Procedures)

3 Rahmenbedingungen

3.1 Faktoren

3.1.1 Politische Faktoren

Politische Entscheidungen prägen das regulatorische Umfeld und den rechtlichen Rahmen, in dem Organisationen tätig sind. In Rechtsvorschriften werden Anforderungen festgelegt zu deren Einhaltung Organisationen bzw. Unternehmen verpflichtet sind (legal compliance) – zum Teil wird auch erwartet, dass Unternehmen hierzu einen Nachweis führen. Um Risiken zu mindern und eine effektive und effiziente Unternehmensführung sowie eine kontinuierliche Compliance sicherzustellen, müssen Organisationen über politische Entwicklungen auf dem Laufenden bleiben, und Compliance-Programme an sich ändernde Anforderungen anpassen.

In Organisationspolitiken wird häufig angeführt, dass sich die jeweilige Organisation zur Einhaltung von Rechtsvorschriften und von freiwilligen Kodizes sowie von organisationsinternen Vorhaben verpflichtet.

3.1.2 Wirtschaftliche Faktoren

Der Fokus aller Organisationen sollte darauf liegen, ihren Zweck zu erfüllen, indem sie im Laufe der Zeit angemessene Werte für alle ihre Stakeholder schaffen. Wie eine Organisation diese Werte generiert, wird in ihrem Geschäftsmodell festgelegt, welches regelmäßig an dessen Zielerreichung gemessen wird.

Ein effektives und effizientes Compliance-System kann für eine Organisation nachhaltig von Vorteil sein. Hingegen stellt fehlende oder mangelnde Compliance ein bedeutendes unternehmerisches Risiko dar und kann zu einer Sanktionierung der Organisation und zu straf- und zivilrechtlichen Konsequenzen der Organisationsleitung führen. Sowohl für die Organisation selbst als auch für die Organisationsleitung (Geschäftsführung, Vorstand, Aufsichtsrat) ist daher ein wirksames Compliance-System essentiell. Strafverfolgungsbehörden verhängen zunehmend hohe Sanktionen gegen Organisationen und deren Organe, wenn sie nicht compliant arbeiten.

3.1.3 Gesellschaftliche Faktoren

Das Verhalten von Organisationen wird von der Gesellschaft kritisch beobachtet – dies betrifft sowohl die Einhaltung von Rechtsvorschriften als auch die Erfüllung von Erwartungen der Gesellschaft, zu deren Erfüllung manche Organisationen sich durch organisationsinterne Vorgaben oder freiwillige Kodizes Dritter selbstverpflichten. Ein Verstoß gegen diese Verpflichtungen kann zu Reputationsschäden für die Organisation und die Gesellschaft als Ganzes führen.

3.1.4 Umweltfaktoren

Die EU steht an der Spitze von Nachhaltigkeitsinitiativen, einschließlich des europäischen Grünen Deals, der darauf abzielt, die Region in eine CO2-neutrale Wirtschaft umzuwandeln. Unternehmen werden ermutigt, ihre Strategien an diesen Nachhaltigkeitszielen auszurichten.

Compliance ist Teil von Governance, somit Teil von ESG (Environmental, Social, and Governance) und damit für die Umwelt von Relevanz. Compliance ist in der Lage, die Erreichung der Sustainable Development Goals (SDGs) zu fördern.

3.1.5 Technische Faktoren

Während technische Innovationen (z. B. künstliche Intelligenz) erhebliche Vorteile im Bereich Governance und Compliance bieten können, müssen Unternehmen bei der Einführung dieser Technologien auch Herausforderungen im Zusammenhang mit Datenschutz, Sicherheit, Ethik und regulatorischer Ausrichtung bewältigen. Darüber hinaus ist es von entscheidender Bedeutung, mit den sich ändernden regulatorischen Anforderungen Schritt zu halten und sich an veränderte Compliance-Landschaften anzupassen, um technische Innovationen effektiv nutzen zu können.

3.1.6 Rechtliche Faktoren

In europäischen Ländern gibt es oft klar definierte Corporate-Governance-Kodizes, die Best Practices für Vorstände, Aktionärsrechte und Transparenz darlegen. Diese Standards zielen darauf ab, die Rechenschaftspflicht zu verbessern und die Interessen von Aktionären und Stakeholdern zu schützen.

Grundsätzlich sind im Rahmen der ganzheitlichen Compliance sowohl jegliche nationale Rechtsvorschriften zu berücksichtigen als auch in nationales Recht umzusetzende Europäische Richtlinien bzw. direkt anwendbare Europäische Verordnungen, aber auch extraterritorial wirkende ausländische Rechtsvorschriften. Ebenso sind Empfehlungen der OECD und von kompetenten NGOs wie Transparency International von Bedeutung.

3.1.7 Europäische und internationale Faktoren

Viele europäische Unternehmen sind grenzüberschreitend tätig, was die Einhaltung verschiedener nationaler und EU-Vorschriften erfordert. Diese Komplexität unterstreicht die Bedeutung robuster Governance- und Compliance-Rahmenwerke.

Das britische Antikorruptionsgesetz „Bribery Act 2010“ ist seit 1. Juli 2011 in Kraft und beinhaltet einen extraterritorialen Anwendungsbereich. Hiervon werden alle Unternehmen erfasst, die Geschäfte oder auch nur Teile des Geschäfts auf dem Hoheitsgebiet des Vereinigten Königreichs tätigen. Für die Zuständigkeit der britischen Strafverfolgungsbehörden und Justiz ist daher bereits eine geschäftliche/unternehmerische Tätigkeit ganz unabhängig von einer Niederlassung im britischen Hoheitsgebiet ausreichend, auch wenn die Korruptionshandlung im Ausland gesetzt wird.

Ebenso kommen die Bestimmung des Sarbanes-Oxley Act (SOX) zum Tragen, da dessen Vorschriften für inländische und ausländische Unternehmen gelten, deren Wertpapiere an US-Börsen gehandelt werden, deren Wertpapiere mit Eigenkapitalcharakter in den USA außerbörslich gehandelt werden, oder deren Wertpapiere in den USA öffentlich angeboten werden. Vergleichbares gilt für den Foreign Corrupt Practices Act (FCPA).

3.2 Zielsetzungen und Strategie des Komitees

3.2.1 Zielsetzungen des Komitees

Schaffung von ÖNORMEN auf den Gebieten Governance und Compliance, um Organisationen, unabhängig von deren Größe und Art, bewährte und anerkannte Instrumente auf freiwilliger Basis zur Verfügung zu stellen, damit die jeweilige Organisation ihre Rechtssicherheit systematisch, ganzheitlich und institutionalisiert sicherstellen und nachweisen kann. Damit tragen die Arbeiten des Komitees zur Haftungsminimierung und zur Professionalisierung von Compliance und den Akteuren bei.

3.2.2 Strategie zur Zielerreichung

Bei der Erstellung der ÖNORMEN trägt das Komitee Sorge, dass kein unnötiger Verwaltungsaufwand bzw. Parallelitäten in den Organisationen entstehen. Hierzu werden Erfahrungen aus der Praxis bei der Umsetzung und den Betrieb von Compliance-Systemen genutzt, um so angemessene, effiziente Instrumente, wie z. B. interne Guidelines, Schulungs- und Bewusstseinsbildungsprogramme, zu identifizieren.
Bei der Zusammensetzung des Komitees ist neben den in Abschnitt 2.1.2 genannten Kreisen auf eine angemessene Vertretung aus verschiedenen Branchen, z. B. Banken, Chemie, Energieversorgungsunternehmen, Handel und Dienstleistungsunternehmen, und Unternehmensgrößen, einschließlich KMUs, zu achten.

3.2.3 Risikoanalyse

Ein wesentliches Risiko ist, dass die im Komitee zu entwickelnden ÖNORMEN in der Praxis nicht angewendet und nicht akzeptiert werden. Um dieses Risiko zu minimieren, ist bei der Gestaltung die Erfahrung aus der Praxis bestehender Governance Maßnahmen und Compliance-Systeme zu nutzen und die Zweckmäßigkeit der Anforderungen durch Einbindung kompetenter Personen zu prüfen.

4 Arbeitsprogramm

Das Arbeitsprogramm des Komitees ist in https://www.austrian-standards.at/de/standardisierung/komitees-arbeitsgruppen/nationale-komitees/committees/35210/details dargestellt.