İNÖNÜ ÜNİVERSİTESİ HUKUK FAKÜLTESİ DERGİSİ
INONU UNIVERSITY LAW REVIEW
ISSN: 2146-1082 e-ISSN: 2667-5714
İnÜHFD - InULR
Araştırma Makalesi / Research Article

COMPLIANCE KAVRAMI VE YÖNETİM ORGANLARININ HUKUKİ SORUMLULUĞU

THE CONCEPT OF COMPLIANCE AND THE LEGAL RESPONSIBILITY OF GOVERNING BODIES

Tayfun ERCAN[*] & *Ayşe Nur TİRYAKİ*[**]

Makale Bilgi

Gönderi: 11/08/2025
Kabul : 31/08/2025

Anahtar Kelimeler

Compliance Yönetimi, Hukuki Sorumluluk, Kurumsal Yönetişim, ISO 37301, Uyum, Yönetim Organları

Özet

10.21492/inuhfd.1762801

Bu çalışma, günümüzün dinamik ve giderek karmaşıklaşan iş dünyasında "compliance" kavramının kurumsal yönetişim içerisindeki kritik rolünü ve yönetim kurulu üyelerinin bu çerçevede üstlendikleri hukuki sorumlulukları kapsamlı bir bakış açısıyla ele almaktadır. İlk olarak, uyumun salt hukuka riayet etmekten öte, etik kültürün inşası, kapsamlı politika ve prosedürlerin oluşturulması, etkin risk değerlendirmesi, sürekli eğitim ve iç denetim mekanizmalarının birbirini tamamlayan beş temel unsur olarak ele alındığı ISO 37301 PDCA döngüsü çerçevesinde açıklanmaktadır. Akabinde, Türkiye'de SPK, Türk Ticaret Kanunu, BDDK, Rekabet Kurumu ve KVKK düzenlemeleri ile Avrupa Birliği'nin GDPR, Kara Para Aklama Direktifleri ve Whistleblower Direktifi gibi uluslararası normlar karşılaştırmalı olarak incelenmektedir. Daha sonra, yönetim kurulu üyelerinin sözleşmesel, tazminî ve cezaî sorumlulukları ayrıntılı şekilde tartışılmakta; yetki aşımı, özenli yönetici standardı, rüşvet ve kara para aklama suçları gibi örneklerle açıklanmaktadır. Uyum programı eksikliklerinin yol açtığı ağır idari para cezaları, tazminat davaları, hisse senedi değer kayıpları ve itibar sorunlarını ortaya konulmaktadır. Çalışma, yönetim kurullarına entegre uyum programı tasarımı, bağımsız denetim fonksiyonunun güçlendirilmesi, erken uyarı göstergeleri, şeffaf raporlama ve sürekli iyileştirme kültürü tesisine yönelik somut öneriler sunmaktadır.

Article Info

Received: 11/08/2025
Accepted: 31/08/2025

Keywords

Internet Domain Names, Arbitration, Reverse Domain Name Hijacking, Dispute Resolution Service Provider, World Intellectual Property Organisation

Abstract

In today's rapidly evolving and increasingly complex business environment, compliance has emerged as a cornerstone of corporate governance, with board members bearing significant legal liabilities. This paper provides an integrated analysis of compliance's strategic role and the multifaceted duties of board directors. Drawing on the PDCA cycle of ISO 37301, it delineates the five pillars of an effective compliance program—ethical culture, policies and procedures, risk assessment, training and communication, and monitoring and improvement. A comparative examination of Turkey's regulatory framework (SPK, Turkish Commercial Code, BDDK, Competition Authority, KVKK) alongside the EU's GDPR, AML Directives, and Whistleblower Directive highlights overlapping and divergent obligations. The paper details contractual, tortious, and criminal liabilities of directors, including ultra vires acts, breach of the duty of care, bribery, and money laundering offences. Antitrust violations and Enron's accounting fraud illustrate the severe administrative sanctions, civil damages, stock price collapses, and reputational damage resulting from compliance failures. The study concludes with actionable recommendations for boards: integrated compliance governance, strengthened independent audit functions, key risk indicators, transparent reporting, and a culture of continuous improvement.

[*] Doç. Dr., Gaziantep Üniversitesi, Hukuk Fakültesi, Ticaret Hukuku Anabilim Dalı.
[**] Yüksek Lisans Öğrencisi, Gaziantep Üniversitesi, Sosyal Bilimler Enstitüsü, Ekonomi Hukuku Tezsiz Yüksek Lisans Programı

Atıf Şekli | **Cite As**: ERCAN, Tayfun/TİRYAKİ, Ayşe Nur, "Compliance Kavramı ve Yönetim Organlarının Hukuki Sorumluluğu", İnÜHFD, 16(2), 2025, s.350-364. **İntihal** | **Plagiarism:** Bu çalışma intihal programında kontrol edilmiş ve en az iki hakem incelemesinden geçmiştir. | This article has been controlled via plagiarism software and reviewed by at least two blind referees.

EXTENDED SUMMARY

The globalizing business environment, increasing competition, and rapidly changing regulatory frameworks are forcing businesses to go beyond focusing solely on profits and also strictly adhere to ethical and legal obligations. In this context, the concept of "compliance" refers to the obligation for organizations to conduct their activities in accordance with both international standards and national legislation. Compliance is not simply about adhering to the law; it also encompasses a multifaceted management approach, including the adoption of internal policies and procedures, the establishment of risk management processes, employee training, and the establishment of internal audit mechanisms. Starting from internationally recognized ISO standards, a comprehensive framework is defined that encompasses OECD and UN guidelines, legal regulations such as the FCPA and UK Bribery Act, and extends to the European Union's AML directives and GDPR, outlining the technical, legal, and ethical dimensions of modern compliance management in a holistic manner. These standards and guidelines not only ensure that organizations comply with regulations; they also position the compliance function as a strategic management tool within the framework of ethical principles and social responsibility.

The history of compliance can be traced back to the late 1970s, when regulations such as the Foreign Corrupt Practices Act (FCPA) were enacted in the US to combat bribery and corruption. Later, the Sarbanes–Oxley Act mandated publicly available data, internal control, and financial reporting transparency (Sarbanes-Oxley Act, 2002). In Europe, the first guidance text on compliance management systems emerged through the OECD's published guidelines for multinational corporations and the ISO 19600 standard in 2014. In 2021, this guidance was formalized into a documentable structure with the ISO 37301 standard (ISO, 2021). These international regulations paved the way for the adoption of financial compliance functions as a management tool, redefined the role of compliance departments from "controllers" to "advisors and guides." The primary objective of this study was to examine the importance of the concept of "compliance" within corporate governance in today's rapidly changing and complex business environment, and the legal responsibilities of board members within this framework, from a holistic perspective.

At the international level, standards such as ISO 19600 and ISO 37301, the OECD Guidelines for Multinational Enterprises, the United Nations Global Compact Initiative, the U.S. FCPA and the UK Bribery Act regulations, EU Anti-Money Laundering Directives, GDPR, and Whistleblower Directives have transformed compliance management from merely an internal control function into a strategic management tool. Within this framework, international norms encourage the top leadership of companies to embrace a culture of compliance; they provide a comprehensive structure ranging from risk assessment to policy-procedure documentation, from training-communication activities to monitoring-auditing-continuous improvement cycles. In particular, the PDCA approach of ISO 37301 requires a cyclical approach to policy revisions, performance measurements, and resource allocation, ensuring that the compliance management system remains dynamic.

Today, it is critical for companies to have an effective compliance program to protect their reputation, achieve corporate sustainability goals, and avoid potential sanctions in line with the expectations of investors, consumers, and regulatory authorities. The legal framework for compliance management in Turkey was shaped by the Turkish Commercial Code (TCC) No. 6102 of 2012 and the regulations of the Capital Markets Board (CMB) (TCC Articles 556–562; CMB, 2013). The TCC obliges the boards of directors of joint-stock and limited companies to act within the framework of their articles of association, observe diligent management standards, and refrain from conduct contrary to the company's interests. At the same time, the CMB defined detailed requirements for brokerage firms and public companies regarding corporate governance principles, risk management, and the establishment of compliance programs. In the banking sector, Banking Law No. 5411 and relevant BRSA communiqués mandate the establishment of internal control, ethical codes of conduct, and anti-money laundering measures, and that boards of directors oversee these processes.

In practice, to mitigate the risk of legal liability, managers should focus not only on regulatory compliance but also on creating an effective compliance culture. This culture should proceed through a PDCA-based cycle consisting of leadership and commitment, risk assessment, policies and procedures, training and communication, and monitoring and improvement. Boards of directors should integrate these five elements into the company's strategy and compliance process. An effective compliance program is driven by early warning systems, independent internal auditing, regular board reporting, and transparent annual reports. This minimizes legal and reputational risks and strengthens companies' ability to achieve their strategic objectives.

Effective compliance management and strong board oversight enable businesses to fully fulfill their legal obligations and secure their reputation and financial sustainability. Compliance is not merely a cost or constraint; it has become a strategic competitive advantage, a foundation for reinforcing stakeholder trust, and an essential component of long-term growth. This study aims to provide a comprehensive guide on the strategic steps organizations can follow on their compliance journey, potential pitfalls, and standards for building a strong compliance culture. Further studies will deepen data in the areas suggested above, adding new perspectives to the compliance and corporate governance literature.

I. GİRİŞ

Küreselleşen iş ortamı, artan rekabet ve hızla değişen ekonomi, işletmeleri yalnızca kâr elde etmeye odaklanmaktan öteye geçerek etik ve yasal yükümlülüklere de sıkı sıkıya bağlı olmaya zorlamaktadır. Bu bağlamda "compliance" (uyum) kavramı, organizasyonların faaliyetlerini hem uluslararası standartlara hem de ulusal mevzuata uygun biçimde yürütme zorunluluğunu getirmektedir. Uyum, sadece hukuka riayet etmekten ibaret değildir. Aynı zamanda kurum içi politika ve prosedürlerin benimsenmesi, risk yönetimi süreçlerinin oluşturulması, çalışanların eğitimi ve iç denetim mekanizmalarının tesis edilmesi gibi çok yönlü bir yönetim yaklaşımını da kapsamaktadır[1]. Günümüzde yatırımcı, tüketici ve düzenleyici kamu otoritelerinin beklentileri doğrultusunda şirketlerin itibarını koruması, kurumsal sürdürülebilirlik hedeflerine ulaşması ve muhtemel yaptırımlardan kaçınması için etkin bir uyum programına sahip olmaları kritik öneme sahiptir.

İşletmeler, faaliyet gösterdikleri coğrafya ve sektöre bağlı olarak sürekli değişen hukuk düzenlemeleriyle karşı karşıya kalmaktadır. Bu düzenlemeler, kimi zaman finansal uyuşmazlıkları önlemeye yönelik tedbirler içerirken, kimi zaman da veri koruma, rekabet hukuku veya kara para aklama risklerinin bertaraf edilmesini amaçlamaktadır. Uyum programlarının kapsamlı olarak tasarlanması, bu farklı risk alanlarının her birine yönelik politika ve prosedürlerin geliştirilmesini, sorumlu birimler ve komiteler aracılığıyla izlenmesini ve periyodik denetimlerle etkinliğinin ölçülmesini gerektirmektedir. Bu bağlamda, uyum yönetimi sistemleri sadece yasal düzenlemelere uyum için değil, aynı zamanda şirket içi değerler ve kurumsal kültürün güçlendirilmesi amacıyla da hayati bir işlev görmektedir.

Compliance kavramının tarihsel gelişimine bakıldığında, 1970'li yılların sonlarında ABD'de kabul edilen Foreign Corrupt Practices Act (FCPA) gibi düzenlemelerle rüşvet ve yolsuzlukla mücadele alanına yönelik ortaya çıktığı görülmektedir. Daha sonra, Sarbanes–Oxley Act ile, halka açık şirketlerin iç kontrol mekanizmaları ve finansal raporlama şeffaflığı zorunlu hale getirilmiştir. (Sarbanes–Oxley Act, 2002).

Avrupa'da ise, OECD'nin çok uluslu şirketler için yayımladığı rehberler ve 2014 yılında ISO 19600 standardı aracılığıyla uyum yönetim sistemlerine yönelik ilk kılavuz metin ortaya konulmuştur. 2021 yılında, bu rehber ISO 37301 standardı ile gereklilikleri tanımlayan belgelendirilebilir bir yapıya kavuşturulmuştur (ISO, 2021). Söz konusu uluslararası düzenlemeler, kuruluşların uyum fonksiyonlarını stratejik bir yönetim aracı olarak benimsemelerine zemin hazırlamış; uyum birimlerinin rolünü "kontrol eden" değil, "danışman ve yol gösterici" olarak yeniden tanımlamıştır[2].

Türkiye'de uyum yönetimine ilişkin yasal altyapı, 2012 tarihli 6102 sayılı Türk Ticaret Kanunu (TTK) ile Sermaye Piyasası Kurulu'nun (SPK) düzenlemeleri etrafında şekillenmiştir (TTK m. 556–562; SPK, 2013)[3]. TTK, anonim ve limited şirketlerin yönetim kurullarına, esas sözleşme hükümleri çerçevesinde hareket etme, özenli yönetici standardını gözetme ve şirket menfaatine aykırı davranışlardan kaçınma yükümlülüğünü getirmiştir. Aynı dönemde SPK, kurumsal yönetim ilkeleri ve risk yönetimi ile uyum programlarının oluşturulması konusunda aracı kurumlar ve halka açık şirketler için detaylı zorunluluklar tanımlamıştır[4]. Bankacılık sektöründe ise, 5411 sayılı Bankacılık Kanunu ve ilgili BDDK tebliğleri, iç kontrol, etik davranış kuralları ve kara para aklamayla mücadele önlemlerinin tesis edilmesini, yönetim kurullarının ise bu süreçleri gözetmesini zorunlu kılmıştır. Uyum sistemlerinin etkinliğini değerlendirmenin temel dayanaklarından biri, risk temelli yaklaşım ile politika ve prosedürlerin iş süreçlerine uyumudur. Her kuruluş, faaliyet alanına özgü riskleri belirlemek, bu risklere yönelik kontrol mekanizmaları tesis etmek ve periyodik testler aracılığıyla uygulama sonuçlarını yönetim kuruluna raporlamak durumundadır. Risk haritalarının düzenli güncellenmesi ve erken uyarı göstergelerinin (KRI) izlenmesi, şirketlerin potansiyel uyum ihlallerini tespit etmesine ve hızlı müdahale etmesine imkân tanımaktadır. Ayrıca, anonim ihbar hatları (whistleblowing) yoluyla çalışanların ve iş ortaklarının şüpheli durumu bildirmesine olanak sağlamak, şeffaflık ve hesap verebilirlik kültürünü güçlendirmektedir.

Yönetim kurulu üyelerinin hukuki sorumluluğu; sözleşmesel, tazmin ve cezai sorumluluk olmak üzere üç temel alanda ele alınabilir. Sözleşmesel sorumluluk, yönetim kurulu üyeleri ile şirket arasında kurulan ilişki kapsamında taraflarca kararlaştırılan yükümlülüklerin yerine getirilmemesini ifade etmektedir. TTK'da yer alan hükümler, yönetim kurulu üyelerinin esas sözleşmeye, iç politika ve komitelere aykırı hareket etmesi hâlinde şirket ve üçüncü kişilerle yapılan sözleşmelerden doğan yükümlülükleri ihlal etmiş sayılacaklarını öngörmektedir. Tazminî sorumluluk alanında ise, şirketin, pay sahiplerinin veya alacaklıların uğradığı zararın, kusurlu fiil ile illiyet bağı kurularak yönetim kurulu üyelerinden tazmin edilmesi gerekmektedir. Bu kapsamda, "görevini yerine getirirken gereken özeni göstermeme" hâli ihmali kusur sayılmakta ve özenli yönetici standardına aykırılık olarak değerlendirilmektedir. Cezaî sorumluluk ise, daha ağır yaptırımları içermektedir; rüşvet, yolsuzluk veya kara para aklama gibi suç teşkil eden eylemler nedeniyle yönetim kurulu üyeleri doğrudan hapis ve para cezalarıyla karşılaşabilmektedir (TCK m. 155, 157)[5].

---

[1] KESKİN, Duygu Anıl: "İşletmelerin Sürekliliğini Sağlamada Kritik Öneme Sahip Risk Yönetimi ve Risk Odaklı Denetim Yaklaşımı", Denetişim, 4(1), 2010, s.39.

[2] POLLACK, Andrew: "$4.9 Billion Jury Verdict In G.M. Fuel Tank Case", The New York Times, <https://www.nytimes.com/1999/07/10/us/4.9-billion-jury-verdict-in-gm-fuel-tank-case.html> (Erişim: 15.01.2025).

[3] KIRCA, İsmail/ ŞEHİRALİ ÇELİK, Feyzan Hayal/ MANAVGAT, Çağlar: Anonim Şirketler Hukuku Temel Kavram ve İlkeler, Kuruluş, Yönetim Kurulu, Cilt. 1, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları, Ankara 2013, s.6.

[4] KARASU, Rauf: "6102 Sayılı Türk Ticaret Kanunu ile Anonim Şirketlerde Kurumsal Yönetim ile İlgili Getirilen Yenilikler", İnönü Üniversitesi Hukuk Fakültesi Dergisi, 4(2), 2013, s. 42.

[5] KANGAL, Zeynel T.: Türk Ceza Hukuku Açısından Compliance, Türk-Alman Hukuk Sempozyumu Teori ve Uygulama Açısından

Uygulamada, yöneticilerin hukuki sorumluluk riskini azaltmak için yalnızca düzenlemelere uyuma değil, aynı zamanda etkin bir uyum kültürü oluşturmaya odaklanmaları gerekmektedir. Bu kültür; liderlik ve taahhüt, risk değerlendirmesi, politika ve prosedürler, eğitim ve iletişim ile izleme ve iyileştirme unsurlarından oluşan PDCA temelli bir döngüyle ilerlemek durumundadır. Yönetim kurulları, bu beş unsuru benimseyerek şirket stratejisi ile uyum sürecinin entegre etmelidir. Etkin bir uyum programı; erken uyarı sistemleri, bağımsız iç denetim, düzenli yönetim kurulu raporlaması ve şeffaf yıllık raporlarla yaşam bulmaktadır. Bu sayede, hukuki ve itibar riskleri asgariye inerken, şirketlerin stratejik hedeflerine ulaşma süreçleri de güçlenmektedir.

Literatüre bakıldığında, genellikle uyum programlarının teknik yapısı veya yönetim kurulu sorumluluğu alanlarından biri ayrı ayrı incelenirken, bu çalışmada her iki unsur bir arada ele alınmaktadır. Bunun temel nedeni, yönetim kurullarının stratejik karar organı olarak hem kurumsal yönetişim hem de uyum süreçlerine doğrudan etki etme yetkisi ve sorumluluğu taşımasıdır.

II. KAVRAMSAL ÇERÇEVE

A. Compliance Kavramı

Compliance, literatürde çoğunlukla "uyum yönetimi" veya "yasal düzenlemelere riayet" şeklinde Türkçeleştirilse de, kapsamı çok daha geniştir. Bir organizasyonun sadece yürürlükteki yasal düzenlemelere uymasını değil; aynı zamanda etik ilkeler, iç politika ve prosedürlerine, sektör kodlarına ve uluslararası normlara da bağlı kalmasını ifade etmektedir[6]. Bu çerçevede compliance, işletmenin tüm iş süreçlerine nüfuz eden ve karar alma mekanizmalarını etkileyecek şekilde yapılandırılan bir yönetim anlayışı olarak karşımıza çıkmaktadır. Özellikle faaliyet gösterilen coğrafya ve sektöre özgü düzenleyici otoritelerin beklentileri, şirketleri sadece yasalara uygun davranmaya değil; aynı zamanda toplumun genel kabul görmüş etik kurallarında da uyum sağlamaya zorlamaktadır.

Bir yandan faaliyet gösterilen ülkenin kanunlarına, yönetmeliklerine ve mahkeme kararlarına uyum sağlanması işletmenin temel yükümlülüğünü oluştururken; diğer yandan içsel düzenlemeler kapsamında tanımlanan etik ilke ve standartlar, işletmenin itibarını ve toplum gözündeki güvenilirliğini doğrudan etkilemektedir. Finans sektöründe, SPK Tebliğleri'ne veya bankacılık özelinde BDDK düzenlemelerine bütünüyle uyulması, sadece hukuki bir zorunluluk değildir. Aynı zamanda, sektördeki tüm paydaşların beklentilerine cevap vermek için zorunlu bir asgari standardı temsil etmektedir (SPK, 2013; BDDK, 2015)[7]. Bu bakımdan yasal uyum ve etik uyum birbirinin tamamlayıcısıdır. Yasal uyum şirketi cezai sorumluluktan korurken, etik uyum operasyonel ve itibar risklerini en aza indirger[8].

Kurum içi etik ilkeler, menfaat çatışmasının önlenmesi, rüşvet ve yolsuzluğun engellenmesi gibi konular, bir compliance programının en hassas alanlarını oluşturmaktadır. Bir davranış kuralı ihlali, doğrudan bir hukuki yaptırıma tabi olmayabilir; ancak işletmenin itibar kaybına, operasyonel aksamalara ve paydaş güveninin zedelenmesine yol açabilir. Etik ilkelerin belirlenmesi, yazılı hale getirilmesi ve çalışanlara benimsetilmesi; ayrıca ihlal durumunda uygulanacak disiplin ve cezai mekanizmaların öngörülmesi, modern uyum yönetim programlarının temel taşlarını oluşturmaktadır.

Compliance programının omurgasını oluşturan diğer unsurlar, şirket içindeki risk yönetimi, bilgi güvenliği, ihbar mekanizmaları (whistleblowing) ve tedarik zinciri denetimidir[9]. İş süreçlerinin her aşamasında muhtemel yasal, finansal ve itibar risklerinin belirlenmesi; bu risklere karşı uygun kontrol ve temkin mekanizmalarının kurulmasını sağlamaktadır. Risk haritası oluşturma çalışmaları, risklerin olasılık ve etki değerlerine göre önceliklendirilmesine imkân tanımakadır.

Özellikle dijitalleşme çağında şirketlerin sahip olduğu kişisel veri, ticari sır ve fikri mülkiyet niteliğindeki varlıkların korunması, hem KVKK hem de uluslararası veri koruma düzenlemeleriyle yakından ilgilidir.

Çalışanlar ve iş ortakları, tespit ettikleri uyum ihlallerini anonim veya tanımlı yollarla bildirebilmek durumundadır[10]. Güvenli bir bildirim sistemi, yalnızca ihlalin tespiti için değil, aynı zamanda etik kültürün kurum geneline yayılmasında önemli rol oynamaktadır.

Özellikle küresel tedarik zincirine sahip şirketlerde, taşeron veya tedarikçi firmaların etik ve yasal uyum standartlarına uygun hareket etmesi oldukça önemlidir. Tedarikçi sözleşmelerine uyum maddeleri eklemek ve düzenli denetimler yapmak, tedarik zincirindeki riski azaltmaktadır.

Uluslararası Standartlar Örgütü (ISO), 2014 yılında ISO 19600 standardını yayımlayarak uyum yönetim sistemleri için rehber niteliğinde bir çerçeve sunmuştur (ISO, 2014). ISO 19600, spesifik sertifikasyon gerektirmeyen, yol gösterici bir metin olarak şirketlerin kendi ihtiyaçlarına uygun uyum politikaları ve prosedürleri tasarlamalarına imkân tanımaktadır. Ancak belgelendirilebilir bir gereklilik

İşletmelerde Hukuk Kurallarına Uygun Hareket Etme (Compliance) Tartışmaları, eds. Erhan Temel ve Adem Sözüer, Adalet Yayınevi, Ankara 2013, s.75.

[6] PULAŞLI, Hasan: "Compliance Kavramı ve Yönetim Organının Compliance Sorumluluğu", Banka ve Ticaret Hukuku Dergisi, 35(2), 2019, s. 31.

[7] PASLI, Ali: ''Compliance' Kavramının Anonim Ortaklıklar Hukukundaki Anlamı ve Sorumluluk Sistemine Etkisi", İÜHFM, 71(2), 2013, s. 317.

[8] MERAKLI, Serkan: Şirket Faaliyetleri Kapsamında İşlenen Suçlarda Şirket Yetkililerinin Ceza Hukuku Sorumluluğunun Esasları, Seçkin Yayıncılık, Ankara 2022, s. 26.

[9] EMİNOĞLU, Cafer: Türk Ticaret Kanunu'nda Kurumsal Yönetim, 1. Bası, On İki Levha Yayıncılık, İstanbul 2014, s.56.

[10] ALP, Mustafa: Çalışanın İşvereni ve İş Arkadaşlarını İhbar Etmesi – Çalışanın Hukuka ve Etik Kurallara Aykırılıkları İfşa Hakkı ve İhbar Borcu, 1.Bası, Beta Yayıncılık, İstanbul 2013, s. 218.

standardı olmayan ISO 19600, 2021'de ISO 37301 ile ilga edilerek yerine belgelendirilebilir yapıda bir uyum yönetim sistemi standardı getirilmiştir (ISO, 2021). ISO 37301, Planla–Uygula–Kontrol Et–Önlem Al (PDCA) döngüsünü temel alan, yönetimin taahhüdünden başlayarak risk değerlendirmesi, politika/prosedür dokümantasyonu, eğitim, izleme ve sürekli iyileştirme süreçlerini ayrıntılı şekilde tanımlayan ilk uluslararası standart olmuştur.

Günümüzde compliance birimlerinin rolü "kontrol eden" değil, "danışman ve yol gösterici" olarak değişmiştir. Bu değişim, uyum uzmanlarının iş süreçlerine erken aşamalardan itibaren dahil edilmesi, yeni ürün veya hizmet geliştirme süreçlerinde yasal ve etik risklerin etkin bir şekilde yönetilmesi ve teknoloji destekli izleme mekanizmalarının kurulması gibi pratik uygulamalarda kendini göstermektedir.

B. Compliance Kavramının Temel Unsurları

ISO 37301, etkin bir uyum yönetim sisteminin beş temel unsurdan oluştuğunu ve bu unsurların bir bütün halinde işletilmesinin, kurum genelinde etkin risk yönetimi ve uyum sorumluluğunun paylaşılmasını mümkün kıldığını vurgulamaktadır (ISO, 2021). İlk unsur, üst yönetimin uyum kültürünü benimsemesi ve bu kültürün kurum içinde yayılması için gerekli kaynakları ayırmasıdır. Üst yönetim, sadece uyum programını onaylamakla kalmamalı; uyumun stratejik bir öncelik olduğunu tüm paydaşlara açıkça göstermek durumundadır. Bu, uyum politikalarının oluşturulması ve güncellenmesi için ayrılan bütçeden, uyum birimlerinin personel desteğine; teknoloji altyapısına yapılan yatırımlardan, performans değerlendirmelerde uyum kriterlerine yer verilmesine kadar geniş bir alanı kapsamaktadır. Üst yönetimin taahhüdü, uyum uygulamalarının etkinliğini doğrudan belirleyen bir etken olarak öne çıkmakta; zira bu taahhüt, kurumun en üst karar mekanizmasından gelen desteği sembolize etmekte ve tüm çalışanlara, uyumun azami öneme sahip bir konu olduğu mesajını iletmektedir[11].

İkinci unsur, risk değerlendirmesidir. Etkin bir uyum yönetim sistemi, hem yasal hem de itibari risklerin sistematik olarak tespit edilip önceliklendirilmesini gerektirmektedir. Yasal risk değerlendirmesi, işletmenin faaliyet gösterdiği coğrafyadaki mevzuat değişikliklerinin izlenmesi, ilgili düzenleyici kurumların yayınladığı tebliğ ve rehberlerin analizi ile başlamaktadır. İtibar riskleri ise müşteri memnuniyeti, medya gözetimi, çevresel sosyal yönetim kriterleri ve sürdürülebilirlik raporları gibi kaynaklardan elde edilen verilerin bütüncül yorumlanmasıyla değerlendirilmektedir. Risk değerlendirmesi sürecinde, bir risk haritası oluşturularak risklerin olasılık ve etki düzeyine göre sınıflandırılması sağlanmaktadır. Bu sınıflandırma, kaynakların hangi risklere odaklanması gerektiğini netleştirmekte ve uyum programının etkinliğini artırmaktadır. Ayrıca, risk değerlendirmesi sonuçlarının düzenli aralıklarla gözden geçirilmesi ve güncellenmesi; kurumsal faaliyetlerde ortaya çıkan yeni risklere karşı farkındalık kazandırır.

Üçüncü unsur, politika ve prosedürlerdir. Yazılı uyum politikaları, kurumun taahhüt ettiği değerleri, hedefleri ve kontrol mekanizmalarını açıkça ortaya koymaktadır. Bu politikalar; etik davranış ilkeleri, menfaat çatışması yönetimi, rüşvet ve yolsuzlukla mücadele, veri koruma, rekabet hukuku, kara para aklama önleme gibi uyum alanlarında net rehberlik sağlamaktadır. Prosedürler ise, bu genel ilkeleri, operasyonel iş akışlarına uyumlaştırarak somut adımlara dönüştürmektedir. Örneğin, tedarikçi seçim sürecine yerleştirilen bir prosedür, tedarikçi risk analizlerini ve denetim kriterlerini kapsarken; veri işleme süreçlerine dair prosedürler, kişisel veri sınıflandırması, saklama süreleri ve veri ihlali bildirim mekanizmalarını düzenlemektedir. Politika ve prosedür dokümantasyonunun erişilebilir olması, tüm çalışanların ve iş ortaklarının uyum beklentilerini net bir şekilde anlayabilmesi için hayati önemdedir.

Dördüncü unsur, eğitim ve iletişimdir. Yazılı politikalar ve prosedürler yalnızca bir başlangıçtır. Bu dokümanların uygulamaya geçebilmesi için çalışanların ve yönetim kademesinin düzenli olarak eğitilmesi gerekir. Eğitim programları, e-learning modülleri, yüz yüze atölye çalışmaları ve vaka analizleri gibi çeşitli yöntemler kullanılarak tasarlanmalıdır. Bu yöntemlerin her biri, farklı öğrenme stillerine hitap ederek uyum kültürünün kurum genelinde benimsenmesini kolaylaştırır. İletişim stratejisi ise, eğitimlerin yanı sıra güncel rehberlik materyallerinin, haber bültenlerinin ve kısa eğitim videolarının düzenli olarak paylaşılmasını kapsamaktadır.

Beşinci ve son unsur ise, izleme ve iyileştirmedir. Uyum yönetim sistemi, belirlenen politika ve prosedürlerin nasıl uygulandığını ölçmek için iç denetim, uyum incelemeleri ve geri bildirim mekanizmalarından yararlanmaktadır. Uyum incelemeleri sırasında elde edilen bulgular, uyum komitesi ve yönetim kuruluna raporlanır; raporlar, tespit edilen eksikliklerin giderilmesine yönelik düzeltici eylem planlarına dönüşür. Ayrıca, ihbar hatları (whistleblowing) aracılığıyla gelen geri bildirimler, gizlilik ve koruma garantisiyle değerlendirildiğinde, potansiyel uyum ihlallerinin erken aşamada yakalanmasını sağlamaktadır.

Bu beş unsurun bir bütün olarak uygulanması, organizasyonun tüm kademelerinde uyum sorumluluğunun paylaşılmasını ve etkin risk yönetimini mümkün kılmaktadır. Üst yönetimin öncülüğünde şekillenen uyum kültürü, risk odaklı yaklaşım, net politika ve prosedürler, kapsamlı eğitim ve iletişim stratejisi ile izleme-iyileştirme mekanizmaları, uyum yönetim sistemini sadece bir kontrol aracı olmaktan çıkarıp, stratejik bir değer yaratma sürecine dönüştürmektedir[12]. Böyle bir sistem, hem kurum içi süreçlerde ilgili paydaşların rol ve sorumluluklarını netleştirir hem de düzenleyici otoriteler, yatırımcılar ve kamu nezdindeki güveni pekiştirmektedir.

[11] ÜLGEN Hayri / MİRZE, S. Kadri: İşletmelerde Stratejik Yönetim, 7.Bası, Beta Yayıncılık, İstanbul 2013, s. 477.

[12] MAMAYSKY, Isaac: "Understanding Ethics and Compliance: A Practitioner's Guide to Effective Corporate Compliance Programs", Loyola University Chicago Journal of Regulatory Compliance (JRC), 6(1), 2021, s. 51.

C. Uluslararası Standartlar

Çalışmanın bu bölümünde, öncelikle ISO tarafından yayımlanan iki temel uyum yönetim standardı ele alınacak; ardından OECD Çok Uluslu Şirketler Rehberi, Birleşmiş Milletler Global Compact girişimi, ABD'nin Foreign Corrupt Practices Act'i ve İngiltere Bribery Act'i ile Avrupa Birliği'nin kara para aklamaya karşı uyum direktifleri ve Genel Veri Koruma Tüzüğü incelenecektir.

ISO 19600, 2014 yılında yayımlanan ve kuruluşların uyum yönetim sistemlerini oluştururken başvurabilecekleri kapsamlı bir rehber niteliği taşımaktadır. Standardın temel hedefi, kuruluşların mevcut iç kontrol, risk yönetimi ve denetim süreçlerini uyum perspektifiyle bütünleştirmelerine yardımcı olmaktır. ISO 19600, spesifik bir sertifikasyon mekanizması öngörmemekle birlikte, uyum programlarının kapsamını belirleme, kurumsal politika ve prosedürleri oluşturma ve bu politika-prosedürlerin etkinliğini değerlendirecek iç denetim sistemleri kurma konusunda yol göstermektedir. Standart, yüksek düzeydeki yönetimin taahhüdünden başlayarak, risk değerlendirmesi, dokümantasyon kontrolü, iletişim ve eğitim unsurları üzerinde durmaktadır. Bu rehber, kuruluşların uyum yaklaşımlarını kendi büyüklüklerine, sektör özelliklerine ve coğrafi kapsamlarına göre esnek şekilde uyarlamalarına imkân tanımaktadır.

ISO 37301 ise, 2021'de yayımlanan ve ISO 19600'ün rehber niteliğindeki yaklaşımını belgelendirilebilir bir çerçeveye dönüştüren ilk uyum yönetim sistemi standardıdır. ISO 37301, kuruluşların uyum programlarını dış denetim ve sertifikasyon sürecine tabi tutmalarına imkân sağlayarak uyum uygulamalarının uluslararası kabul görmüş bir ölçekte değerlendirilebilmesini mümkün kılmaktadır. Standart, Planla–Uygula–Kontrol Et–Önlem Al (PDCA) döngüsünü esas alır ve her aşamada ayrıntılı gereklilikler ortaya koymaktadır. ISO 37301 sadece süreç odaklı değil; kültürel değişimi ve stratejik entegrasyonu da destekleyen bütünsel bir yaklaşım sunmaktadır.

OECD Çok Uluslu Şirket Rehberi ise, 1976'dan bu yana güncellenerek yayımlanan ve üye devletlerle iş dünyasına etik, sosyal ve çevresel sorumluluk alanlarında yol gösteren bir referans metindir (OECD, 2011). Rehber; yolsuzlukla mücadele, insan haklarının korunması, istihdam ve çalışma standartları, çevresel sürdürülebilirlik, tüketici çıkarlarının gözetilmesi ve vergi sorumluluğu konularını kapsamaktadır. Ülkeler, rehberi ulusal irtibat noktaları aracılığıyla benimser ve şirketlerin rehbere aykırı davranışlarını şikâyet mekanizmalarıyla izlemektedir. OECD Rehberi'nin, özel bir uyum standardı olmamakla birlikte, çok uluslu şirketlerin hem ana merkezlerinde hem de şubelerinde tek tip bir etik ve uyum kültürü inşa etmelerine yardımcı olmaktadır. Rehberde öngörülen gönüllü ilkeler; şirket içi politika geliştirmelerinde, tedarik zinciri standartlarında ve paydaş iletişim stratejilerinde temel bir çerçeve sağlamaktadır.

Birleşmiş Milletler Global Compact girişimi, 2000 yılında başlatılan ve şirketlerin kurumsal sorumluluk alanında insan hakları, çalışma standartları, çevre ve yolsuzlukla mücadele başlıklarında on temel ilkeye uymalarını teşvik eden bir platformdur (UN Global Compact, 2000). Girişime katılan şirketler, yıllık İlerleme Raporları (Communication on Progress) sunarak taahhütlerinin nasıl uygulandığını ve elde ettikleri sonuçları açıklamak zorundadır. UN Global Compact'in önemi, uluslararası kabul görmüş ilkeler setini kurumsal stratejiye entegre ederek şirketlerin toplumsal sorumluluk ve sürdürülebilirlik hedeflerine ulaşmalarına katkı sağlamasında yatmaktadır.

ABD'nin Foreign Corrupt Practices Act'i (FCPA), 1977 yılında yürürlüğe giren ve yabancı kamu görevlilerine rüşvet vermeyi yasaklayan ilk kapsamlı anti-rüşvet yasasıdır (U.S. Department of Justice, 1977)[13]. FCPA; hem cezai yaptırımlar hem de ağır para cezaları öngörerek ABD menşeli şirketlerin ve ABD pazarında faaliyet gösteren yabancı kuruluşların uluslararası rüşvet uygulamalarını caydırmayı hedeflemektedir. Yasa; rüşvet veren kişilerin yanı sıra, rüşveti önleyici uygun kontrol mekanizmalarını tesis etmeyen şirket yöneticilerine de sorumluluk getirmektedir. FCPA'nın en önemli yeniliklerinden biri, şirketlere "adequate internal controls" (yeterli iç kontrol sistemleri) kurma yükümlülüğü getirmesi ve bu sistemlerin etkinliğinin denetlenebilmesidir. Dolayısıyla FCPA, modern uyum programlarının finansal kontrol, muhasebe kayıtları doğruluğu ve denetim mekanizmaları etrafında şekillenmesinde öncü bir rol oynamıştır[14].

İngiltere Bribery Act'i ise, 2010 yılında yürürlüğe girerek FCPA'dan farklı olarak hem kamu görevlilerine hem de özel sektörden kişilere yönelik rüşvet uygulamalarını kapsamına almıştır (UK Bribery Act, 2010)[15]. Act'in en çarpıcı hükmü "failure to prevent" (suça iştirak etmeye zemin hazırlama) maddesidir; buna göre, bir kuruluşun çalışanları veya aracılarının yaptığı rüşvet eylemleri, şirketin gerekli tedbirleri almaması hâlinde doğrudan şirket sorumluluğuna yol açmaktadır. Bu düzenleme, şirketlere risk değerlendirme yapma, tedarikçi ve kanal ortaklarını denetleme, eğitim programları oluşturma ve ihbar hatları tesis etme yükümlülükleri getirmektedir. UK Bribery Act'in yüksek yaptırım seviyeleri (suça iştirak eden şirketlere 10 milyon sterline kadar para cezası veya suçtan elde edilen gelirin dört katı) ve geniş kapsamı, küresel uyum stratejilerinde yüksek standartlara referans olmuştur[16].

Avrupa Birliği, kara para aklamaya karşı uyum yönetimini güçlendirmek amacıyla 2014'te 4. ve 5. Kara Para Aklama Direktifleri'ni yayımlamıştır (AB, 2014). 4. Direktif, finansal kurumlar ve yüksek riskli sektörlerde müşteri tanıma (KYC), müşteri profili oluşturma ve şüpheli işlem raporlama yükümlülükleri getirirken; 5. Direktif, elektronik para kuruluşları, sanal varlık hizmet sağlayıcıları ve emlak danışmanlarını

[13] MCGREAL, Paul E.: "Caremark in the Arc of Compliance History", Temple Law Review, 90(4), 2018, s.649.
[14] KURT, Ganite / UÇMA UYSAL, Tuğba: "COSO Kurumsal Risk Yönetimi Çerçevesi Güncelleme Projesinin Getirdiği Yenilikler", Muhasebe ve Denetime Bakış Dergisi, 18(54), 2018, s. 29.
[15] SOKOL, D. Daniel: "Teaching Compliance", University of Cincinnati Law Review, 84(2), 2016, s. 414.
[16] MORTON, Jeffrey C.: "The Development of a Compliance Culture", Journal of Investment Compliance, 6(4), 2005, s. 61-62.

da kapsayarak uyum çemberini genişletmiştir. 6. Direktif ile kara para aklama suçu ve terörün finansmanı suçu tanımları netleştirilmiş; para cezası ve hapis cezaları artırılmıştır. AB üyesi ülkeler, bu direktifleri ulusal mevzuatlarına 2020 sonuna kadar uyarlamak zorunda kalmış; uyum programlarına ilişkin denetim ve yaptırım mekanizmalarını sıkılaştırmıştır[17].

AB Veri Koruma Tüzüğü (GDPR) ise, 2016'da kabul edilmiş ve 2018'de yürürlüğe girmiştir. GDPR, kişisel verinin işlenmesi, depolanması ve paylaşılması süreçlerinde yasal uyumun yanı sıra veri minimizasyonu, amaç sınırlaması, şeffaflık, hesap verebilirlik ve veri sahibinin haklarını güvence altına alma ilkelerini zorunlu kılmaktadır. GDPR, 20 milyon euroya kadar veya küresel yıllık cironun %4'üne kadar ulaşan yaptırımlar öngörerek şirketleri teknik ve organizasyonel önlemler alma konusunda harekete geçirmiştir. Tüzük; veri koruma görevlisi atama, veri işleme envanteri tutma, risk değerlendirmesi yapma, ihlal durumunda 72 saat içinde bildirimde bulunma ve paydaşlara şeffaf bilgi sağlama yükümlülüklerini getirmiştir.

Uluslararası düzeyde kabul görmüş ISO standartlarından başlayarak OECD ve BM rehberlerine, FCPA ve UK Bribery Act gibi yasal düzenlemelerden Avrupa Birliği'nin AML direktifleri ve GDPR'a kadar uzanan kapsamlı bir çerçeve, modern uyum yönetiminin teknik, hukuki ve etik boyutlarını bütüncül biçimde tanımlamaktadır. Bu standartlar ve rehberler, kuruluşların sadece düzenlemelere riayet etmesini sağlamakla kalmaz; aynı zamanda etik ilkeler ve toplumsal sorumluluk çerçevesinde stratejik bir yönetim aracı olarak uyum işlevini konumlandırmaktadır.

III. HUKUKİ DAYANAK VE DÜZENLEMELER

A. Türk Mevzuatında Uyumluluk Yükümlülükleri

Türkiye'de uyum programlarının ve yönetim kurulu sorumluluklarının temeli; sermaye piyasası düzenlemeleri, Türk Ticaret Kanunu'nun ilgili hükümleri, bankacılık denetim mevzuatı, rekabet hukuku ile kişisel veri koruma kanunu gibi çok sayıda yasadan oluşmakta, bu farklı yasal düzenlemeler arasında sıkı bir uyum gerekmektedir[18]. Çalışmamızın ilerleyen bölümlerinde, başta Sermaye Piyasası Kurulu (SPK) düzenlemeleri olmak üzere, Türk Ticaret Kanunu (TTK), Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), Rekabet Kurumu ve Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında yönetim kurullarına yüklenen uyum yükümlülükleri ayrıntılı biçimde ele alınmıştır.

Sermaye Piyasası Kurulu, halka açık şirketlerin faaliyetlerinde şeffaflık ve hesap verebilirlik ilkelerini en üst düzeyde sağlamalarını zorunlu kılmak üzere çeşitli tebliğ ve ilke kararları yayımlamıştır. Özellikle Seri: IV, No: 56 Tebliği uyarınca aracı kurumlar ile bağımsız denetim kuruluşları, risk yönetimi ve iç kontrol sistemlerini oluşturmak ve bunları etkin biçimde işletmekle yükümlü kılınmıştır. Bu iç kontrol sistemleri; finansal raporlama süreçlerinin doğruluğunu güvence altına alacak muhasebe kayıt mekanizmeleri, uygun onay yetkileri, işlem limit kontrolleri ve süreklilik arz eden izleme prosedürlerini içermektedir.

2014 yılında SPK tarafından yürürlüğe konan Kurumsal Yönetim İlkeleri'nin dördüncü bölümü, yönetim kurullarının "etik değerler ve uyum kültürünü şirket genelinde yayma" sorumluluğunu ayrıntılı olarak tanımlamıştır. Buna göre, yönetim kurulu başkanı ve denetim komitesi üyeleri; uyum ihlallerinin raporlanması, soruşturulması ve gerektiğinde yaptırım süreçlerinin takibi konusunda doğrudan yetkilendirmektedir. Denetim komitesi, iç denetim birimi ile yakın koordinasyon içinde çalışarak, tespit edilen uygunsuzlukları düzenli raporlarla yönetim kuruluna sunmakta ve yönetim kurulunun hızla müdahale etmesini sağlamaktadır. Yine aynı kapsamda, şirketin internet sitesinde bir "Kurumsal Yönetim ve Uyum" bölümü açılması, yatırımcı ilişkileri raporlarında uyum başlıklı bir bölümün yayımlanması SPK ilkeleri tarafından teşvik edilmektedir.

SPK'nın uyum konusundaki bir diğer düzenlemesi, halka açık şirketlerin yıllık faaliyet raporlarında yönetim kurulu üyelerinin niteliklerine, bağımsızlık durumlarına, komite yapılarına ve uyum programının temel unsurlarına ilişkin bilgilendirme yapmasını zorunlu kılmasıdır. Bu hüküm; yatırımcıların, şirketin uyum kültürüne verdiği önemi doğrudan görebilmesini, yönetim kurulu üyelerinin profesyonel yeterlilik ve deneyimlerinin uyum programına katkısını değerlendirebilmesini mümkün kılmaktadır. Böylece, kurumsal yönetişim kalitesi ile finansal performans arasındaki ilişkiyi güçlendiren şeffaflık mekanizmaları hayata geçirilmiş olmaktadır.

6102 sayılı Türk Ticaret Kanunu, anonim ve limited şirketler bakımından yönetim kurulu üyelerinin hem şirket içi hem de üçüncü kişilere karşı sorumluluklarını ayrıntılı biçimde düzenlemektedir[19]. Limited şirketlerde, 375–381 inci maddeler; anonim şirketlerde ise, 395–408 inci maddeler, yönetim kurulu üyelerinin "dürüstlük kuralına" ve "şirket menfaatine aykırı davranmama" ilkelerine bağlı kalmasını öngörmektedir. Bu kapsamda, yönetim kurulu üyeleri; karar süreçlerinde şirket faaliyetlerinin sürdürülebilirliğini gözetmek, şirket varlıklarını şahsi menfaatleri doğrultusunda kullanmamak ve şirket aleyhine sonuç doğuracak işlemlerden kaçınmak durumundadır[20].

---

[17] MİLLER, Geoffrey Parsons: The Law of Governance, Risk Management, and Compliance, 2.edn. Wolters Kluwer, New York 2017, s. 288.

[18] YAŞAR, Tuğçe Nimet/ SONGUR, Damla: "Anonim Şirketlerde Rekabet Hukuku Uyum (Compliance) Programının Oluşturulması ve İşlevleri-7246 Sayılı Kanun ile yapılan Değişikliklerle Birlikte", Banka ve Ticaret Hukuku Dergisi, 36(4), 2020, s. 92.

[19] TEKİNALP, Ünal: Sermaye Ortaklıklarının Yeni Hukuku, 5. Bası, Vedat Kitapçılık, İstanbul 2020, s.45.

[20] BALYEMEZ, Ahmet Sinan: "Türkiye'de Özel Sektör ve Kamu İdareleri İç Kontrol Sistemlerinin Mevzuat Yükümlülükleri Açısından Karşılaştırılması", Gazi Üniversitesi Sosyal Bilimler Dergisi, 3(8), 2016, s.49.

TTK'nun 395. maddesi hükümlerine aykırı hareket eden bir yönetim kurulu üyesi, esas sözleşme veya kanunla getirilen onay prosedürlerini ihlal ettiğinde, bu ihlal nedeniyle şirketin veya üçüncü kişilerin uğradığı zararı bizzat tazmin etmekle yükümlü tutulmaktadır. Burada belirleyici kriter, "görevini yerine getirirken özenli yönetici standardı"dır. Makul bir yönetici davranışının ötesine geçen ihmal veya kasıt unsurunun varlığı ispatlandığı takdirde sorumluluk doğmaktadır.

TTK'nun 555–561 inci maddeleri ise tazminî sorumluluğu düzenlemektedir. Buna göre, yönetim kurulu üyelerinin kusurlu fiilleri sonucu şirket, pay sahipleri veya alacaklılar zarar görmüşse, bu zararın karşılanması için tazminat talep edilebilmektedir. Özellikle şirketin ödeme güçlüğüne düştüğü iflas veya konkordato süreçlerinde alacaklılar, yönetim kurulu üyelerinin kusurunu ispatlayarak doğrudan sorumluluk talep edebilir. Bu maddeler, yönetim kurulu üyelerinin stratejik karar süreçlerinde risk odaklı yaklaşım benimsemelerini ve karar öncesi hukuki-mali danışmanlık almalarını teşvik etmektedir.

Bankacılık sektörü, kara para aklama ve terörün finansmanını önleme başta olmak üzere uyum programlarının en sıkı uygulandığı alanlardan biridir[21]. 5411 sayılı Bankacılık Kanunu'nun 62 ila 64 üncü maddeleri, bankalara "etik davranış kuralları" ve "iç kontrol politikaları" oluşturma yükümlülüğü getirir. Bankalar, bu yükümlülüklerini yerine getirmek amacıyla bir uyum komitesi ve ayrı bir iç denetim birimi tesis etmek zorundadır[22].

BDDK ayrıca, bankaların kara para aklama ve terör finansmanıyla mücadele programlarını 6 aylık veya yıllık periyotlarla BDDK'ya sunmalarını zorunlu kılmaktadır. Raporlarda; müşteri tanıma (KYC) ve izleme prosedürleri, şüpheli işlem tespit ve bildirim mekanizmaları ile personel eğitimlerinin kapsamı ve etkinliği açıklanmaktadır. Uyumsuzluk tespit edilen bankalara, para cezası, faaliyet kısıtlaması veya yönetici değişikliği gibi idari yaptırımlar uygulanabilmektedir.

Rekabet Kurumu'nun 2017 tarihli "Rekabet Uyum Programı Rehberi" şirketlere, hâkim durumun kötüye kullanılmasını, kartel oluşturmayı ve diğer rekabet ihlallerini önlemek amacıyla uyum politikaları geliştirme çağrısında bulunmaktadır[23]. Bu rehbere göre, yönetim kurulları:

- Rekabet hukuku risk değerlendirmesi yapmalı,
- Rekabet kurulu kararlarını izlemeli,
- Personel ve tedarikçi eğitim programları düzenlemeli,
- İhbar mekanizmaları tesis ederek şüpheli rekabet ihlallerini soruşturmalıdır.

Rehber, uyum programlarının kurulmasından ve yürütülmesinden üst düzeyde sorumlu tutulacak bir "Rekabet Uyum Sorumlusu" atamasını önermektedir. İhlal durumunda, şirketler ve sorumlu yönetim kurulu üyeleri; idari para cezaları, zararın tazmini ve itibar kaybı riskiyle karşılaşmaktadır.

Buna ek olarak, Sermaye Piyasası Kanunu, Bankacılık Kanunu ve Rekabet Kanunu'nun yanı sıra Enerji Piyasası Düzenleme Kurumu, Telekomünikasyon Kurumu, Sigortacılık Düzenleme ve Denetleme Kurumu gibi sektörel düzenleyici kurumlar da uyum yükümlülükleri getirmektedir. Örneğin, EPDK düzenlemeleri enerji şirketlerine fiyatlandırma süreçlerinde usulsüzlüğü önleyecek iç kontrol mekanizmaları, BTK düzenlemeleri telekom operatörlerine kullanıcı verilerinin korunması ve siber güvenlik altyapısının güçlendirilmesi, SDDK düzenlemeleri ise sigortacılara dolandırıcılık vakalarını önlemek için risk analiz sistemleri kurma zorunluluğu yüklemektedir.

6698 sayılı Kişisel Verilerin Korunması Kanunu ile Türkiye, Avrupa Birliği'nin Genel Veri Koruma Tüzüğü ile paralel bir veri koruma rejimi oluşturmuştur. KVKK'nın 5 ila 11 inci maddeleri, kişisel verilerin işlenmesinde aydınlatma, rıza, amaç ve özen ilkelerini düzenlerken; 12 ila 17 inci maddeler veri sahibinin haklarına ilişkin hükümler içerir. Şirketler "veri sorumlusu" sıfatıyla:

- Veri işleme envanterlerini tutmak,
- Veri işleme faaliyetlerini kurumsal politika haline getirmek,
- Veri güvenliği organizasyonları kurmak,
- Veri ihlallerini 72 saat içinde Kurula bildirmek,
- Veri koruma görevlisi atamak (gerektiğinde),

  yükümlülüklerini yerine getirmek zorundadır.

Yönetim kurulunun bu süreçteki rolü; veri koruma politikalarının onaylanması, gerekli kaynakların tahsis edilmesi, izleme mekanizmalarının tesis edilmesi ve veri ihlali vakalarında hızlı aksiyon alınmasına öncülük etmek şeklindedir. KVKK'ya aykırı davranışlar, yüksek miktarda idari para cezaları ve rıza ihlallerine dayalı tazminat davaları riski doğurmaktadır. Bunun yanı sıra, veri ihlallerinin açıklanması, tüketici güveninin zedelenmesine ve markaya zarar gelmesine neden olabilir; yönetim kurulu, itibar riskini asgariye indirmek için şeffaf ve hızlı kriz yönetimi süreçlerini planlamalıdır.

Yönetim kurulları, bu çok katmanlı mevzuat ağı içinde stratejik karar organı sıfatıyla hem hukuki sorumluluklarını yerine getirmeli hem de kurumun sürdürülebilirliği, itibar yönetimi ve paydaş güvenini destekleyecek şekilde etkin bir uyum kültürü oluşturmalıdır[24].

---

[21] GÜLERCİ, Altan Fahri: Sorumluluk Hukuku Bakımından Bankacılıkta Risk Kavramı, Türkiye Bankalar Birliği Yayınları, İstanbul 2015, s.224.

[22] USUL, Hayrettin / MİZRAHİ, Rozi: Risk Odaklı Denetim, Detay Yayıncılık, Ankara 2016, s.11-15.

[23] ALTUN, Mücteba: "Kartellerin Ortaya Çıkarılmasında Kullanılabilecek Araçlar Bağlamında Rekabet Kurumu Uygulamasına Bir Öneri: İhbarcı Koruma ve Ödül Programları", Rekabet Dergisi, 19(1), 2018, s. 70.

[24] PULAŞLI, S. 1575; EMİNOĞLU, s. 314; BAHTİYAR, Mehmet: Ortaklıklar Hukuku, 17. Bası, Beta Yayıncılık, İstanbul 2024, s. 189-191.

B. Avrupa Birliği Düzenlemeleri

Avrupa Birliği, üye ülkelerde finansal suçlarla mücadeleden veri korumaya, etik yönetim uygulamalarına ve ihbar mekanizmalarına kadar uzanan geniş bir uyum çerçevesi oluşturmuştur. Kara para aklamayla mücadele alanında, Birliğin dördüncü, beşinci ve altıncı Kara Para Aklama Direktifleri (4AMLD, 5AMLD ve 6AMLD) kademeli olarak yürürlüğe girmiştir. Mayıs 2015'te yayınlanan dördüncü direktif, "müşteri tanıma" (Know Your Customer) yükümlülüklerini ayrıntılandırarak finansal kurumların yeni müşteri kabulü sırasında kimlik tespiti yapmasını; yüksek riskli işlemlerde ek inceleme gerçekleştirmesini; işlem geçmişini ve varlık kaynağını sorgulamasını; şüpheli işlemlerin ulusal mali istihbarat birimine raporlanmasını şart koşmuştur. Nihai faydalanıcı tanımını getirerek, finansal işlemleri gerçekleştiren kişi veya kuruluşun gerçekte kim tarafından kontrol edildiğinin ortaya konmasını zorunlu kılan bu düzenleme, kara para aklama yöntemlerinin şeffaflık ve izlenebilirlik ilkelerine dayalı olarak önlenmesini hedeflemiştir.

2018 yılında kabul edilip Ocak 2020'de tamamı yürürlüğe giren beşinci direktif, elektronik para kuruluşları ile sanal varlık hizmet sağlayıcılarını ve emlak aracılık hizmetlerini de kapsamına alarak, kara para aklama riskinin aşamalı olarak yeni sektörlerde de kontrol altına alınmasını sağlamıştır. Bu direktif kapsamında, kripto varlık platformları lisanslama zorunluluğuna tabi tutulmuş; kripto cüzdan sağlayıcılarının müşterilerine dair kimlik ve işlem verilerini saklaması; yüksek değerli gayrimenkul alımlarının ise şüpheli işlem bildirim mekanizmalarına dahil edilmesi öngörülmüştür. Yüksek nakit ödeme tutarlarına sınırlama getirilmesi, para aklama faaliyetlerinin nakdi yöntemlerle kolaylaştırılmasının önüne geçme amacını taşırken, finansal kurumların risk tabanlı iç denetim süreçlerini güçlendirmesi ve periyodik olarak güncellemesi beklenmiştir.

Altıncı Kara Para Aklama Direktifi ise Aralık 2020'den itibaren uygulama alanına alınarak, kara para aklama suçunun tanımını genişletmiş; vergi kaçakçılığı, örgütlü suç gelirlerinin aklanması ve terörün finansmanı gibi alanları da kapsayacak şekilde uyum yükümlülüklerini derinleştirmiştir. Bu direktif uyarınca, üye ülkeler arasında mali istihbarat paylaşımı, kolluk kuvvetleri ve vergi otoriteleri arasında koordinasyon ve bilgi akışı mekanizmalarının tesis edilmesi zorunlu hale getirilmiştir. Ayrıca, kara para aklama işlemlerine ilişkin cezaî yaptırımların asgari hapis ve para cezaları seviyeleri doğrudan bu direktifle belirlenmiş; suçtan elde edilen malvarlığına el konulması ve zapt edilmesi süreçleri standartlaştırılmıştır. Böylelikle hem suç gelirlerinin aklanması riskinin hem de terör finansmanının önlenmesi hedeflenmiştir.

Kara para aklama direktiflerinin ardından, AB 2016 yılında Genel Veri Koruma Tüzüğü'nü (GDPR) kabul ederek kişisel verinin işlenmesi, depolanması ve aktarılması süreçlerinde benzeri görülmemiş bir koruma düzeyi belirlemiştir. GDPR, veri işleyen tüm kuruluşların kapsamlı bir veri işleme envanteri tutmasını; işleme amaçlarını, veri kategorilerini ve ilgili kişilerin haklarını açıkça dokümante etmesini şart koşmaktadır. Veri sahiplerine, kişisel verilerinin nasıl kullanıldığı konusunda anlaşılır ve erişilebilir bilgi sunulması; onayın özgür iradeyle, belirli bir amaç için alınması ve gerektiğinde geri çekilebilmesi; hassas veri olarak sınıflanan sağlık, etnik köken veya dini inanç gibi veriler söz konusu olduğunda ise ek koruma önlemleri uygulanması öngörülmektedir. GDPR ayrıca, olası bir veri ihlalinin tespit edilmesinden itibaren 72 saat içinde ilgili veri koruma otoritesine bildirilmesini ve etkilenen veri sahiplerinin kapsamlı şekilde bilgilendirilmesini zorunlu kılmaktadır.Tüzük kapsamında belirlenen en önemli yükümlülüklerden biri de, belirli ölçek ve sektörde faaliyet gösteren kuruluşlara veri koruma görevlisi (DPO) atama zorunluluğu getirmesidir. DPO'nun bağımsız çalışması ve doğrudan yönetim kuruluna rapor vermesi GDPR'ın temel şeffaflık ve hesap verebilirlik ilkelerini pekiştirmektedir. Uyumsuzluk durumunda, kuruluşlar küresel yıllık cirolarının dörtte birine veya 20 milyon euroya kadar varan idari para cezalarıyla karşılaşabilir; bu yaptırımlar GDPR'ın etkinliğini ve caydırıcılığını ortaya koymaktadır.

Kara para aklama ve veri koruma düzenlemelerinin tamamlayıcı niteliğindeki bir diğer AB girişimi, Whistleblower Direktifi'dir[25]. 2019/1937 sayılı bu düzenleme, çalışanların ve diğer paydaşların yolsuzluk, suiistimal ve uyum ihlallerini güvenli, gizli ve yetkin mercilere bildirmelerini sağlayacak dahili ve harici bildirim kanallarının kurulmasını zorunlu kılmaktadır. Direktife göre, bu kanallar iletilen bildirimlerin gizliliğini korumak, bildirim sahiplerini misilleme ve mağduriyetten korumak ve bildirimleri bağımsız bir değerlendirme mekanizmasıyla hızlıca ele almak üzere tasarlanmalıdır. Bildirim sahiplerine, ihlal konusu olaya ilişkin geri bildirim sağlanması ve bildirim süreçleriyle ilgili koruyucu tedbirlerin uygulanması yükümlülükler arasındadır. Üye devletler, bu direktifi ulusal mevzuatlarına 2021 sonuna kadar aktarmak zorundadır; bu süre zarfında, kuruluşların bildirim mekanizmalarını oluşturması, uyum politikalarına Whistleblower hükümlerini dahil etmesi ve ilgili personeli konu hakkında eğitmesi gerekmektedir.

AB düzenlemeleri yalnızca direktiflerle sınırlı kalmayıp, OECD ve Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) gibi uluslararası kuruluşların yayımladığı rehberlerle de desteklenmektedir. OECD'nin 2019 tarihli Yolsuzlukla Mücadele Rehberi, şirketlerin tedarikçi ve ajan yönetimi süreçlerine dair kapsamlı tavsiyeler sunar; çıkar çatışmalarının önlenmesi, üçüncü taraf denetimleri, hediyeler ve ağırlama politikalarının belirlenmesi gibi uygulama alanlarını ayrıntılandırmaktadır. UNODC'nin 2018 tarihli "Business Integrity Guidance" dokümanı ise, şirketlerin etik riskleri proaktif şekilde tanımlamasına, kültürel uyum stratejileri geliştirmesine ve uyum programlarının sürdürülebilirliğini garanti altına alacak yapıların oluşturulmasına yönelik pratik araçlar önermektedir.

[25] ALP, Mustafa: "Avrupa Birliği'nin 2019/1937 Sayılı Birlik Hukukuna Aykırılıklarını Bildirenlerin Korunması (Whistleblowing) Yönergesi Işığında İşçinin Hukuka Aykırılıkları İfşa Etmesi", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 23(1), 2021, s.4.

Türkiye'de faaliyet gösteren uluslararası şirketler, bu AB düzenlemelerini ulusal mevzuatlarına uyum sağlamakla yükümlüdür. Kara Para Aklama Direktifleri çerçevesinde hazırlanan ulusal kanun ve tebliğlerde, finansal kurumların ve yüksek riskli sektörlerin uyum programlarına dair detaylı süreç ve kontrol mekanizmaları tanımlanmıştır. GDPR'ın yansımaları ise 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili ikincil mevzuatta yer almakta; veri sorumlularına GDPR ile paralel yükümlülükler getirmektedir. Whistleblower Direktifi ise halen ulusal mevzuata aktarılma sürecindedir ve şirketlerin iç düzenlemelerini güncellemelerini gerektirmektedir.

Bu kapsamlı düzenleyici çerçeve, Türkiye'de faaliyet gösteren tüm şirketlerin, özellikle üst düzey yönetim ve yönetim kurullarının, hem stratejik hem de sürekli denetleyici rol üstlenmesini zorunlu kılmaktadır. Yönetim kurulları, uyum programlarını onaylamak, kaynak tahsisini garanti etmek, etkinlik ölçüm göstergelerini tanımlamak, risk raporlarını düzenli olarak değerlendirmek ve gerektiğinde düzeltici eylem planları geliştirmekle yükümlüdür. Böylece, uluslararası alanda geçerli uyum standartlarına uyum sağlanırken; şirketlerin hukuki sorumluluk riskleri minimize edilmekte, kurumsal itibar korunmakta ve sürdürülebilir büyüme hedeflerine destek vermektedir.

C. Yönetim Kurulunun Hukuki Sorumluluğu

Yönetim kurulu üyelerinin sözleşmesel sorumluluğu, Türk Ticaret Kanunu'nun 396 ve devamı maddelerinde ayrıntılı şekilde düzenlenmiştir. Bu hükümlere göre, yönetim kurulu üyeleri, şirketle kurdukları ilişkilerde –ister doğrudan, ister dolaylı olsun– esas sözleşmede belirlenen usullere ve yetki sınırlarına riayet etmek zorundadır. Şirket adına taahhütlerde bulunan bir üye, esas sözleşmede tanınmayan yetkileri kullanarak üçüncü kişilere zarar verecek şekilde işlem yaparsa, bu "ultra vires" yani yetki aşımı olarak nitelendirilir ve hem iç hukuka hem de üçüncü kişilere karşı ileri sürülemez[26]. Örneğin, esas sözleşmede yalnızca yatırım kararı alma yetkisi öngörülen bir kurul üyesinin şirket varlıklarını devretmeye yönelik bir sözleşmeye imza atması, geçersiz sayılır ve bu nedenle şirket üçüncü kişilerden hiçbir talepte bulunamaz[27]. Aynı şekilde, yetki devri ve imza yetkilendirmesi uygulamalarında da mutabakatın yazılı olarak tescil edilmemesi veya yetki sınırlarının net şekilde belirlenmemesi halinde, yetki devredilen kişi tarafından imzalanan sözleşmeler geçersiz sayılabilir; bu durumda yönetim kurulu üyeleri, hukuken sorumlu tutulur. Örneğin, yönetim kurulu üyesinin esas sözleşmenin izin vermediği bir borçlanma işlemine imza atması sonucunda ortaya çıkan zarara karşı sözleşmesel sorumluluğunu teyit etmiş, zararın tazmini hükmünü vermiştir.

Buna paralel olarak tazminî sorumluluk, TTK'nın 555–561 inci maddeleri arasında düzenlenen haksız fiil sorumluluğu çerçevesinde ele alınmaktadır. Bu hükümlerde, yönetim kurulu üyelerinin şirketin menfaatine aykırı veya özen yükümlülüğünü ihlal eden davranışları sonucu meydana gelen zararın, sorumludan tazmin edilmesi zorunluluğu öngörülmüştür[28]. Özenli yönetici standardı olarak adlandırılan bu kriter (TTK m. 556), makul bir yöneticiden beklenen dikkat ve titizliği ölçüt alır; finansal tablolarda olağan dışı dalgalanmalar veya uyumsuzluk işaretleri gören bir üyenin derhal inceleme yapmaması, ihmal veya kasıt oluşturur ve tazminî sorumluluk doğurur[29]. Tazmin hükmü için zararın somut biçimde gerçekleşmiş olması ve zararla fail arasındaki illiyet bağının ispatı şarttır. Örneğin, bir bankanın kredi limitini aşması veya teminatlandırma prosedürlerini esnetmesi sonucu doğan faiz yükümlülükleri, üçüncü kişiye tazminat olarak ödenen meblağlar bu kapsamda değerlendirilebilir. Tazminî sorumluluk yalnızca şirkete karşı değil, aynı zamanda pay sahiplerine ve alacaklılara karşı da doğabilir. Kanuna göre, şirket menfaati ihlal edildiğinde doğrudan şirkete karşı sorumluluk gündeme gelirken (TTK m. 561), genel kurul kararıyla hakları zedelenen pay sahipleri kişisel tazminat talep edebilir (TTK m. 557). Ayrıca iflas veya konkordato durumunda alacaklılar, şirketin borç erteleme yükümlülüklerini ihlal etmesi halinde yönetim kurulu üyelerini muhatap alabilir (TTK m. 560). Örneğin, bir inşaat şirketinin yönetim kurulu, ihale şartnamesine aykırı teknik bir düzenleme yaparak şirketi ağır cezai yaptırımlara maruz bırakırsa bundan sorumlu olacaktır.

Cezaî sorumluluk ise, Türk Ceza Kanunu (TCK), Kabahatler Kanunu ve diğer özel düzenlemelerde yer alan suç tiplerinin kapsamına girmeyen hallerde dahi, şirket yöneticilerinin suç teşkil eden fiilleri nedeniyle adli yaptırımlarla muhatap olmalarını öngörmektedir[30]. TCK m. 252–256'da rüşvet ve yolsuzluk suçları düzenlenmiştir; bu maddelere göre hem kamu görevlisine rüşvet verme hem rüşvet alma eylemleri cezalandırılmaktadır. Anonim şirket yönetim kurulu üyeleri, kamu ihalelerine ilişkin usulsüzlük veya yolsuzluk yapmaları halinde bu yaptırımlarla karşılaşır[31]. Ayrıca TCK m. 282–283'te suçtan kaynaklanan malvarlığı değerlerinin aklanması suçu; yönetim kurulu üyelerinin suç gelirlerini meşrulaştırma faaliyetlerinde bulunması halinde hapis ve para cezalarını öngörmektedir. TCK m. 155 de güveni kötüye kullanma suçu başlığı altında, şirket varlığını kişisel çıkarları için kullanma eylemlerini kapsamaktadır. Örneğin, şirket hesabından usulsüz para transferi yapan bir üye, bu hüküm kapsamında cezalandırılır. Cezaî

[26] PULAŞLI, Hasan: Şirketler Hukuku Genel Esaslar, 4. Baskı, Adalet Yayınevi, Ankara 2016, s. 444.
[27] ÜLGEN/MİRZE, s. 33-34; DOĞAN, Beşir Fatih: "Yönetim Kurulunun Devredilemez Yetkileri ve Yönetim Yetkisinin Devri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 18(2), 2012, s. 612-614.
[28] DEMİREL, Duygu: "Anonim Şirketlerde Yönetim Yetkisinin Devri", Hacettepe Hukuk Fakültesi Dergisi, 7(2), 2017, s. 240-242.
[29] ATASOY, Ömer Adil/ ERGÜN, Berkay: "Anonim Şirketlerde Yönetim Kurulu Üyelerinin Görevleri Kapsamında Kurulması Zorunlu Komitelerin Faaliyetlerinden Doğan Sorumlulukları", İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi, 4(2), 2018, s. 40.
[30] ERBAŞ, Rahime: ''Compliance' Fenomeni Ekseninde Şirket İç Soruşturmalar ve Türk Ceza Hukukundaki Olası Sonuçları", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2(1), 2023, s.1249.
[31] ÖZATLAN, Yurdal: Anonim Şirketlerde Yönetim Kurulunun Üst Gözetim Görevi ve Yetkisi, (Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2022, s. 32-33.

sorumluluğun yanı sıra, KVKK, SPK ve BDDK gibi düzenleyici kurumlar da uyum ihlallerine yönelik idari para cezaları verebilir.

Tüm bu sorumluluk alanları, yönetim kurulu üyelerinin stratejik risk yönetimine dair sorumluluklarını da kapsamaktadır. Üyeler geçmişe yönelik sorumluluk yüklenmenin ötesine geçerek, potansiyel hukuki risklerin tespiti, raporlanması ve giderilmesi süreçlerini proaktif şekilde yönetmelidir[32]. Bu çerçevede risk haritalarının onaylanması ve kritik erken uyarı göstergelerinin (Key Risk Indicators – KRI) takip edilmesi, yönetim kurulu için zorunlu bir görev olarak ortaya çıkmaktadır. Aksi halde, tazminî sorumluluk davalarında risk haritalarını oluşturamayan ya da güncelleyemeyen kurul üyeleri, eksik gözetim nedeniyle sorumluluk altına girmektedir. Ayrıca, bağımsız iç denetim birimi veya uyum komitesinin kurulmasıyla düzenli raporlama mekanizmalarının tesis edilmesi, ihlallerin zamanında tespiti ve müdahale edilmesi açısından hayati öneme sahiptir. Bu yapılar, hem hukuki sorumluluğu azaltmaya yardımcı olur hem de kurum genelinde güçlü bir uyum kültürünün inşa edilmesini sağlar. Yönetim kurullarının, iç denetim raporları ve uyum inceleme bulgularını değerlendirerek düzenli eylem planları oluşturması, şirketin sürdürülebilirliğini ve itibarını korumasında temel belirleyici olacaktır[33].

IV. COMPLIANCE PROGRAMLARI VE DENETİM

A. Compliance Programının Temel Unsurları

ISO 37301'e göre etkin bir uyum yönetim sistemi, Planla–Uygula–Kontrol Et–Önlem Al (PDCA) döngüsü çerçevesinde şekillenen ve birbirini tamamlayan beş temel unsurdan oluşmaktadır. Bu yaklaşım, yalnızca prosedürleri yerine getiren bir kontrol mekanizması olmanın ötesine geçerek, kurumun tüm düzeylerinde uyum kültürünü inşa etmeyi ve sürekli olarak geliştirmeyi hedeflemektedir. Sürecin başlangıcını oluşturan üst yönetimin ve yönetim kurulu üyelerinin açık ve yazılı taahhüdü, uyum programının temel dayanağını oluşturmaktadır. Uyum programının stratejik bir girişim olarak kabul edilmesi, yönetim kurulu başkanı veya CEO'nun imzasını taşıyan uyum politikalarının yayımlanmasını, bu politikaların kurumsal strateji belgeleriyle uyumlu hale getirilmesini ve kaynak tahsisinin (bütçe, insan kaynağı, teknoloji) öncelikli işler arasında yer almasını zorunlu kılmaktadır. Bu taahhüt, sadece uyum biriminin yetkilerini ve sorumluluklarını belirlemekle kalmamakta; aynı zamanda tüm çalışanlara, tedarikçilere ve paydaşlara "uyumun en üst düzey karar alıcıların desteğini aldığı" mesajını vermektedir. Üst düzey yönetimin bu şekilde programa aktif katılımı, uyum kültürünün kurum geneline benimsetilmesinin en etkili yolu olarak kabul edilmektedir.

Yönetim kurulu tarafından verilen bu taahhüt, uyum programının sonraki aşamalarına temel hazırlamaktadır. İlk adımda, kuruluşun faaliyet gösterdiği sektör, coğrafya ve iş süreçlerinin yarattığı yasal, finansal ve itibari risklerin eksiksiz şekilde tanımlanması gerekir. Risk değerlendirmesi, yalnızca hukuki mevzuat takibiyle sınırlı kalmamalı; paydaş görüşmeleri, süreç tabanlı teftişler, saha ziyaretleri ve üçüncü taraf denetimleri gibi çoklu yöntemlerle desteklenmelidir. Örneğin, yüksek itibari risk barındıran bir pazar girişimi ya da karmaşık uluslararası tedarik zinciri ilişkileri, daha sıkı kontrol ve özel prosedürler gerektirirken, düşük düzeyde risk oluşturan rutin işlemler standart iş akışlarıyla yönetilebilir. Risk değerlendirmesi süreci, ilk kurulumun ardından yılda en az bir kez güncellenmeli; önemli yasal değişiklikler veya kurumsal dönüşümler gerçekleştiğinde ise revize edilerek sürekli dinamik bir araç olarak kullanılmalıdır[34].

Risk haritası tamamlandığında, risklerin kontrol altına alınmasını sağlayacak yazılı uyum politikaları ve bunlara ilişkin prosedürler geliştirilir. Uyum politikaları, kurumun üst düzey taahhüdünü yansıtan temel prensipleri ve değerleri belgelendirirken; prosedürler bu ilkeleri operasyonel iş adımlarına dönüştürmektedir. Hazırlanan politikalar; etik davranış ilkeleri, menfaat çatışmasının önlenmesi, rüşvet ve yolsuzlukla mücadele, veri koruma, rekabet hukuku ve kara para aklamanın önlenmesi gibi kritik alanları kapsamalıdır. Her politika belgesinde, belgenin amaç ve kapsamı, sorumluluk dağılımı, süreç adımları ve ihlal durumunda uygulanacak yaptırımlar açıkça tanımlanmalıdır. Prosedürler ise politika metinlerini somut kontrol noktalarına çevirerek iş süreçlerine entegre eder; örneğin, tedarikçi onay süreçlerinde risk derecesine göre dokümantasyon gereksinimleri, onay hiyerarşisi ve denetim kriterleri belirlenir. Politika ve prosedür dokümantasyonunun erişilebilir olması, tüm çalışan ve paydaşların beklentileri net şekilde anlamasına imkân verir, böylece uygulama aşamasında tutarlılık ve hesap verebilirlik sağlanır .

Politika ve prosedürlerin açıklanması, uyum eğitimi ve iletişim faaliyetleriyle desteklenmediği sürece yeterli etkiyi yaratamaz[35]. Bu nedenle, tüm çalışanlara ve özellikle risk düzeyi yüksek pozisyonlardaki personele yönelik yıllık uyum eğitim programları düzenlenmelidir. Eğitimler; e-learning modülleri, yüz yüze atölye çalışmaları, vaka analizleri ve simülasyon senaryolarını içerecek şekilde çeşitlendirilerek, farklı öğrenme stillerine hitap etmelidir. Ayrıca, iletişim planı çerçevesinde düzenli bültenler, intranet duyuruları, kısa eğitim videoları ve interaktif seminerler ile uyum konuları güncel tutulmalıdır. Çalışanların uyum ihlallerini gizli ve güvenli bir şekilde bildirebileceği anonim ihbar hatları (whistleblowing) kurulması da,

[32] ORAN, Ozan: Anonim Şirketlerde Yönetim Kurulu İç Yönergesi, (Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2019, s. 73-77.
[33] HACIMAHMUTOĞLU, Sibel: "Anonim Ortaklığın Yönetim Kurulu Üyelerinin Özen Yükümlülüğü: Fonksiyonel Bir Yaklaşım", Banka ve Ticaret Hukuku Dergisi, 31(3), 2015, s. 28-29.
[34] KARSLIOĞLU, Hasan: "Anonim Şirketlerde İç Yönerge ve İç Yönergenin Yönetim Kurulunun Sorumluluğuna Etkisi", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, 8(1), 2022, s. 41-42.
[35] EFİL, İsmail: İşletmelerde Yönetim ve Organizasyon, 13. Baskı, Dora Yayıncılık, Bursa 2015, s. 12; ÖRÜCÜ, Edip: Modern İşletmecilik, 10. Baskı, Dora Yayıncılık, Bursa 2015, s. 87.

ihlallerin erken aşamada tespit edilip müdahale edilmesini sağlar. Böylece, ihlaller kurum içinde açıklıkla ele alınır, sorumluluk mekanizmaları işlerlik kazanır ve kurum genelinde güvene dayalı bir uyum kültürü oluşur .

Uygulamada politikaların ne ölçüde işlediğini anlamak ve sistemdeki aksaklıkları tespit etmek amacıyla izleme, denetim ve sürekli iyileştirme mekanizmaları devreye alınmalıdır. İç denetim fonksiyonu veya ayrı bir uyum birimi, önceden belirlenen sıklıkta politika ve prosedürlerin uygulanmasını test eder. Denetim raporları, uyum komitesine ve doğrudan yönetim kuruluna sunularak stratejik karar alacak üst yönetimin bilgisine getirilir. Raporlarda tespit edilen uygunsuzluklar; düzeltici eylem planlarına dönüştürülür, sorumlu birimlere aksiyon takvimleri verilir ve düzeltici faaliyetlerin tamamlanma durumu takip edilir. Ayrıca, ihbar hatları üzerinden gelen bildirimler gizlilik ve koruma garantisiyle değerlendirilerek, potansiyel ihlallerin erken safhada yakalanması sağlanır. Böyle bir sürekli iyileştirme döngüsü, uyum yönetim sisteminin hem dinamik hem de etkili bir yapıda kalmasını temin etmektedir.

B. Yönetim Kurulunun Denetim ve Gözetim Rolleri

Yönetim kurulu, şirket stratejisini oluştururken yalnızca finansal ve operasyonel hedeflere odaklanmakla kalmayıp, aynı zamanda uyum programının etkinliğini de doğrudan gözetme sorumluluğu üstlenmektedir[36]. Türk Ticaret Kanunu'nun 558–561. maddelerinde düzenlenen hukuki sorumluluk, yönetim kurulu üyelerine uyum programının başarısını sağlamak bakımından etkin bir rol vermekte; zira uyum programındaki eksiklikler hem sözleşmesel hem de tazminî sorumluluk riskini artırmaktadır. Bu nedenle yönetim kurulu, uyum sürecini yalnızca onaylayıp bir kenara bırakmak yerine, programın planlanmasından, uygulamasına, performans değerlendirmesinden sürekli iyileştirme mekanizmalarına kadar tüm aşamalarda aktif gözetim fonksiyonu görmelidir.

Bu yaklaşım, öncelikle uyum programının kurumsal hiyerarşi içindeki konumlandırılmasıyla başlamaktadır. Yönetim kurulu, uyum biriminin ve iç denetim fonksiyonunun bağımsızlığını sağlamak, gerektiğinde kaynak tahsisini artırmak ve kritik karar süreçlerinde uyum biriminin görüşünü almakla yükümlüdür[37]. Denetim ve uyum komiteleri, SPK Kurumsal Yönetim İlkeleri çerçevesinde oluşturulan mekanizmalardır; bu komitelerin temel görevi, uyum politikasının güncelliğini ve geçerliliğini koruyacak şekilde tasarımı gözden geçirmek, olası ihlalleri araştırmak ve bulguları yönetim kuruluna raporlamaktır[38]. Denetim komitesi ile iç denetim birimi arasındaki koordinasyon, karar süreçlerinin şeffaflığını artırır ve şirket içindeki kontrol noktalarının etkin işlemesini güvence altına alır. İç denetim birimi, bağımsızlığını koruyarak doğrudan yönetim kuruluna rapor verir ve bu raporlarda tespit edilen uygunsuzlukların giderilmesi için somut aksiyon planları önerir. Böylelikle hem regülasyonlarla uyum sağlanır hem de kurum kültüründe "hesap verebilirlik" anlayışı güçlenir.

Uygulamada, yönetim kurulu üyelerinin uyum programına ilişkin sorumluluklarını etkili biçimde yerine getirmesi; performans göstergelerinin ve erken uyarı sistemlerinin titizlikle belirlenmesine bağlıdır. Uyumluluk göstergeleri, niceliksel ve niteliksel verileri bir araya getirerek programın canlı bir izleme mekanizmasıyla desteklenmesini sağlar. Bildirim kanallarından gelen ihbar sayısı, denetim bulgu raporlarının adedi, eğitim katılım oranları, politika ihlalinde geçen ortalama müdahale süresi gibi nicelik sel göstergeler; kaçınılmaz risklerin üstelemelerini azaltmak ve programın verimliliğini anlamak için önemli dir. Öte yandan, niteliksel göstergeler olarak ihlal türlerinin ciddiyeti, politika güncellemelerine yönelik geribildirimlerin kalitesi, çalışan memnuniyeti ve yönetim kurulunun uyum raporlarına ilişkin değerlendirme notları izlenmelidir. Bu göstergeler hem komite hem de tüm yönetim kurulu toplantılarında sunularak stratejik kararların uyum perspektifiyle uyumlu olmasını temin etmektedir.

Yönetim kurulunun raporlama ve şeffaflık yükümlülüğü de bu çerçevenin ayrılmaz bir parçasıdır. Yıllık faaliyet raporunun bir bölümünde uyum programının ana bulguları, gelişim alanları, denetim sonuçları, ihlal vakalarına ilişkin özetler ve düzeltici eylem planları paylaşılmalıdır. SPK'ya yapılan düzenleyici bildirimlerin sayısı, KVKK ivazsız veri işleme ihlallerinin raporları ve iç denetim raporlarının özetleri, şirketin dış paydaşları nezdinde güven tesis etmektedir. Yatırımcılar ve finansal analistler, uyum raporlarındaki şeffaflığı bir kurumsal itibar unsuru olarak değerlendirir; bu sayede sermaye maliyeti düşerken, şirketin kamuoyu ve düzenleyici kurumlar karşısındaki konumu güçlenir.

Ancak, yalnızca gösterge belirlemek ve rapor sunmak yeterli değildir. Yönetim kurulu, hem cezai hem de mali sorumluluk risklerini minimize edecek şekilde uyum programının güncelliğini sürekli sağlamalıdır. Etkili denetim anlayışı; uyum politikalarının mevcut yasal mevzuat ve en iyi uygulamalarla uyumlu olmasını, kritik olgunluk seviyelerindek boşlukların tespit edilmesini ve yeni düzenlemelerin hızla entegrasyonunu kapsamaktadır. Bu husus, yalnızca iç denetim planlarının revizyonlarıyla sınırlı kalmamalı; dijital gözetim araçları, büyük veri analitiği ve yapay zeka destekli uyum platformları vasıtasıyla uyum ihlallerinin gerçek zamanlı tespiti ve analizi gerçekleştirilmelidir. Böylece yönetim kurulu, potansiyel cezai yaptırımlar ve idari para cezaları riskine karşı şirketi korurken, aynı zamanda yasal uyumun yanı sıra etik ve sürdürülebilir yönetim ilkelerini işletme kültürüne entegre edilmiş bir değer yaratma sürecine dönüştürebilir.

[36] YANLI, Veliye: "Anonim Şirketlerde İmza Yetkileri Sadece Yönetim Kurulu Tarafından mı Atanabilir?", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71(2), 2013, s. 439.

[37] KOÇ, Himmet: "Anonim Şirketlerde İç Yönerge ve İç Yönergenin Benzer Hukuki Kurumlarla Olan İlişkisi", Medeniyet ve Toplum Dergisi, 1(2), 2017, s. 170-171.

[38] TUĞ, Mehmet Arif: "Kurumsal Yönetim Kavramının Genel Çerçevesi ve Türk Hukukundaki Yansımaları", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, 5(1), 2019, s.221.

Aslında yönetim kurullarının bu stratejik gözetim fonksiyonu, uyumun yalnızca bir maliyet unsuru veya risk yönetimi mekanizması olarak görülmesinin önüne geçer. Uyum programı etkin yönetildiğinde, şirketlerin tedarikçi ilişkilerinden müşteri memnuniyetine, çalışan bağlılığından marka itibarına kadar geniş bir yelpazede rekabet avantajı sağlar. Örneğin, tedarik zincirinde uyum programı gereği gerçekleştirilen denetimler, olası insan hakları ihlallerinin, çevresel standart sapmalarının veya etik dışı üretim yöntemlerinin önceden tespit edilmesini mümkün kılar. Yönetim kurulu, bu denetim sonuçlarını stratejik kararlara yansıtmak suretiyle hem kurumsal itibarını hem de sürdürülebilir tedarik zinciri riskini yönetir. Benzer şekilde, müşteri verilerinin korunmasına ilişkin GDPR veya KVKK yaptırımlarının finansal sonuçları ve itibar riskleri, yönetim kurulunun veri koruma stratejilerini önceliklendirmesini ve gerekli kaynak tahsislerini yapmasını kaçınılmaz kılar.

Buna ek olarak, yönetim kurulu üyelerinin uyum programına ilişkin sorumluluklarını yerine getirmesinde ivmeyi sağlayan bir diğer faktör de kurumsal öğrenme döngüsüdür. Denetim ve geribildirim süreci, yalnızca hata düzeltmeyi değil; aynı zamanda sistemdeki kuvvetli yönlerin, iyileştirme fırsatlarının ve yenilikçi uygulama örneklerinin belirlenmesini hedeflemelidir. Yönetim kurulu, denetim raporlarında sunulan "başarı hikâyeleri" ve "en iyi uygulama modelleri"ni tanıtarak organizasyon genelinde motive edici bir etki yaratır. Böylece uyum birimi ile iş birimleri arasındaki bariyerler azalır, sürekli eğitim ve iletişim faaliyetleri güç kazanır.

Her ne kadar yönetim kurulu üyeleri yasal sorumluluklarını (TTK m. 558–561) yerine getirmek zorunda olsa da, uyum programının etkin gözetimi aynı zamanda kuruma değer katan bir stratejik işlevdir[39]. Etkili denetim, politika revizyonu, erken uyarı sistemleri ve şeffaf raporlama mekanizmaları, şirketin finansal sağlığını korumasına, yatırımcı güvenini pekiştirmesine ve kurumsal itibarını güçlendirmesine katkı sağlamaktadır. Yönetim kurullarının bu sorumluluklarını layıkıyla yerine getirmeleri, sadece yasal yaptırımların önüne geçmekle kalmaz; aynı zamanda şirketin sürdürülebilir büyüme yolculuğunu destekleyen bir uyum kültürünün inşasını teminat altına almaktır. Böylelikle uyum, kurum içinde bir maliyet kalemi değil, stratejik bir rekabet avantajı ve değer yaratma mekanizması olarak konumlandırılır.

V. SONUÇ

Bu çalışmada, "compliance kavramı" ve "yönetim kurulu organlarının hukuki sorumluluğu" kavramları birarada ele alınmıştır. Öncelikle compliance kavramının yalnızca hukuka riayet mekanizması olmadığı, aynı zamanda etik kültürün, iç politika ve prosedürlerin, risk yönetimi süreçlerinin, sürekli eğitimin ve iç denetimin birbiriyle etkileşimli beş temel unsur şeklinde ele alınması gereken çok boyutlu bir yönetim yaklaşımı olduğu vurgulanmıştır. Bu unsurları tek tek uygulamaya koymak, organizasyonel uyum hedeflerine ulaşmak için yeterli görünse de, aralarındaki karşılıklı bağımlılık ve sürekli iyileştirme döngüsünün işletilmesi olmadan, uyum programları ne yazık ki biçimsel kalmaya mahkûm olur. Dolayısıyla uyumun bir yönetim aracı olarak işleyebilmesi için üst düzey yönetimin taahhüdü, kapsamlı risk değerlendirmeleri, politikaların iş süreçlerine entegre edilmesi, tüm çalışan düzeyinde eğitim ve iletişim faaliyetleri ile izleme-denetim-iyileştirme metotlarının eşgüdümlü bir şekilde yürütülmesi zorunludur.

Türkiye'de uyum programlarının hukuki altyapısı, başta SPK'nın kurumsal yönetim ilkeleri ve tebliğleri, TTK'nın yönetim kurulu sorumluluklarına dair maddeleri, BDDK'nın bankacılık sektörüne yönelik iç kontrol düzenlemeleri, Rekabet Kurumu'nun uyum rehberi ve KVKK'nın veri koruma yükümlülükleri gibi düzenlemeler kapsamında şekillenmektedir. Bu çok katmanlı mevzuat, şirketlerin hem derinleşmiş hem de örtüşen uyum yükümlülükleriyle karşı karşıya bulunduğunu ortaya koymaktadır. Bu kapsamda yönetim kurulu üyelerinin; sözleşmesel, tazminî ve cezaî sorumluluk alanlarında hem geçmişe yönelik sorumluluk üstlendikleri hem de etkin bir yaklaşımla karar öncesi risk analizine yatırım yapmak durumunda oldukları anlaşılmaktadır. Aksi halde, yetki sınırlarını aşan işlemlerden doğan sözleşmesel sorumluluk, kusurlu karar süreçlerinden kaynaklanan tazminî sorumluluk ve hukuki ihlaller nedeniyle doğan cezaî yaptırımlar şirket ve üçüncü kişiler nezdinde ağır mali yükler ve itibar kayıpları yaratacaktır.

Uluslararası düzeyde ise ISO 19600 ve ISO 37301 standartları, OECD Çok Uluslu Şirket Rehberi, Birleşmiş Milletler Global Compact Girişimi, ABD'nin FCPA ve İngiltere Bribery Act mevzuatları, AB Kara Para Aklama Direktifleri, GDPR ve Whistleblower Direktifi gibi düzenlemeler, uyum yönetimini yalnızca bir iç kontrol fonksiyonu olmaktan çıkarıp stratejik bir yönetim aracına dönüştürmüştür. Bu çerçevede uluslararası normlar, şirketlerin en üst düzey liderliğini uyum kültürünü benimsemeye teşvik etmekte; risk değerlendirmesinden politika-prosedür dokümantasyona, eğitim-iletişim faaliyetlerinden izleme-denetim-sürekli iyileştirme döngüsüne kadar kapsamlı bir yapı sunmaktadır. Özellikle ISO 37301'in PDCA yaklaşımı, uyum yönetim sisteminin dinamik kalmasını sağlayacak şekilde politika revizyonlarını, performans ölçümlerini ve kaynak tahsisini döngüsel biçimde ele almayı zorunlu kılar.

Özetle, etkin bir compliance yönetimi ve güçlü bir yönetim kurulu gözetimi, işletmelerin hem yasal yükümlülüklerini eksiksiz yerine getirmesine hem de itibar ile finansal sürdürülebilirliklerini güvence altına almalarına imkân tanır. Uyum, yalnızca bir maliyet ya da kısıtlama unsuru değil; stratejik bir rekabet avantajı, paydaş güvenini pekiştiren bir yapı ve uzun vadeli büyüme için olmazsa olmaz bir bileşen haline gelmiştir.

KAYNAKÇA

[39] SIRAKAYA, Elif Yalçın: "Anonim Şirketlerde Yönetim Yetkisinin Devri Bağlamında Yönetim Kurulunun Üst Gözetim Yükümlülüğü", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 24(2), 2020, s. 200-201.

ALP, Mustafa: "Avrupa Birliği'nin 2019/1937 Sayılı Birlik Hukukuna Aykırılıklarını Bildirenlerin Korunması (Whistleblowing) Yönergesi Işığında İşçinin Hukuka Aykırılıkları İfşa Etmesi", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 23(1), 2021, s.1-37.

ALP, Mustafa: Çalışanın İşvereni ve İş Arkadaşlarını İhbar Etmesi –Çalışanın Hukuka ve Etik Kurallara Aykırılıkları İfşa Hakkı ve İhbar Borcu, 1. Baskı, Beta Yayıncılık, İstanbul 2013.

ALTUN, Mücteba: "Kartellerin Ortaya Çıkarılmasında Kullanılabilecek Araçlar Bağlamında Rekabet Kurumu Uygulamasına Bir Öneri: İhbarcı Koruma ve Ödül Programları", Rekabet Dergisi, 19(1), 2018, s. 66-125.

ATASOY, Ömer Adil/ ERGÜN, Berkay: "Anonim Şirketlerde Yönetim Kurulu Üyelerinin Görevleri Kapsamında Kurulması Zorunlu Komitelerin Faaliyetlerinden Doğan Sorumlulukları", İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi, 4(2), 2018, s. 33-52.

BALYEMEZ, Ahmet Sinan: "Türkiye'de Özel Sektör ve Kamu İdareleri İç Kontrol Sistemlerinin Mevzuat Yükümlülükleri Açısından Karşılaştırılması", Gazi Üniversitesi Sosyal Bilimler Dergisi, 3(8), 2016, s. 1-70 .

DEMİREL, Duygu: "Anonim Şirketlerde Yönetim Yetkisinin Devri", Hacettepe Hukuk Fakültesi Dergisi, 7(2), 2017, s. 211-250.

EFİL, İsmail: İşletmelerde Yönetim ve Organizasyon, 13. Baskı, Dora Yayıncılık, Bursa 2015.

ÖRÜCÜ, Edip: Modern İşletmecilik, 10. Baskı, Dora Yayıncılık, Bursa 2015.

EMİNOĞLU, Cafer: Türk Ticaret Kanunu'nda Kurumsal Yönetim, 1. Baskı, On İki Levha Yayıncılık, İstanbul 2014.

ERBAŞ, Rahime: ''Compliance' Fenomeni Ekseninde Şirket İç Soruşturmalar ve Türk Ceza Hukukundaki Olası Sonuçları", Galatasaray Üniversitesi Hukuk Fakültesi Dergisi, 2(1), 2023, s.1241-1286.

GÜLERCİ, Altan Fahri: Sorumluluk Hukuku Bakımından Bankacılıkta Risk Kavramı, Türkiye Bankalar Birliği Yayınları, İstanbul 2015.

HACIMAHMUTOĞLU, Sibel: "Anonim Ortaklığın Yönetim Kurulu Üyelerinin Özen Yükümlülüğü: Fonksiyonel Bir Yaklaşım", Banka ve Ticaret Hukuku Dergisi, 31(3), 2015, s. 23-56.

KANGAL, Zeynel T.: Türk Ceza Hukuku Açısından Compliance, Türk-Alman Hukuk Sempozyumu Teori ve Uygulama Açısından İşletmelerde Hukuk Kurallarına Uygun Hareket Etme (Compliance) Tartışmaları, eds. Erhan Temel ve Adem Sözüer, Adalet Yayınevi, Ankara 2013.

KARASU, Rauf: "6102 Sayılı Türk Ticaret Kanunu ile Anonim Şirketlerde Kurumsal Yönetim ile İlgili Getirilen Yenilikler", İnönü Üniversitesi Hukuk Fakültesi Dergisi, 4(2), 2013, s. 33-60.

KARSLIOĞLU, Hasan: "Anonim Şirketlerde İç Yönerge ve İç Yönergenin Yönetim Kurulunun Sorumluluğuna Etkisi", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, 8(1), 2022, s. 37-53.

KESKİN, Duygu Anıl: "İşletmelerin Sürekliliğini Sağlamada Kritik Öneme Sahip Risk Yönetimi ve Risk Odaklı Denetim Yaklaşımı", Denetişim Dergisi, 4(1), 2010, s. 38-46.

KIRCA, İsmail/ ŞEHİRALİ ÇELİK, Feyzan Hayal/ MANAVGAT, Çağlar: Anonim Şirketler Hukuku Temel Kavram ve İlkeler, Kuruluş, Yönetim Kurulu, Cilt 1, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları, Ankara 2013.

KOÇ, Himmet: "Anonim Şirketlerde İç Yönerge ve İç Yönergenin Benzer Hukuki Kurumlarla Olan İlişkisi", Medeniyet ve Toplum Dergisi, 1(2), 2017, s. 163-186.

KURT, Ganite / UÇMA UYSAL, Tuğba: "COSO Kurumsal Risk Yönetimi Çerçevesi Güncelleme Projesinin Getirdiği Yenilikler", Muhasebe ve Denetime Bakış Dergisi, 18(54), 2018, s. 19-34.

MAMAYSKY, Isaac: "Understanding Ethics and Compliance: A Practitioner's Guide to Effective Corporate Compliance Programs", Loyola University Chicago Journal of Regulatory Compliance (JRC), 6(1), 2021, s. 6-58 .

MCGREAL, Paul E.: "Caremark in the Arc of Compliance History", Temple Law Review, 90(4), 2018, s.41-59.

MERAKLI, Serkan: Şirket Faaliyetleri Kapsamında İşlenen Suçlarda Şirket Yetkililerinin Ceza Hukuku Sorumluluğunun Esasları, Seçkin Yayıncılık, Ankara 2022.

MİLLER, Geoffrey Parsons: The Law of Governance, Risk Management, and Compliance, 2.edn. Wolters Kluwer, New York 2017.

MORTON, Jeffrey C.: "The Development of a Compliance Culture", Journal of Investment Compliance, 6(4), 2005, s.45-71.

ORAN, Ozan: Anonim Şirketlerde Yönetim Kurulu İç Yönergesi, (Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2019.

ÖZATLAN, Yurdal: Anonim Şirketlerde Yönetim Kurulunun Üst Gözetim Görevi ve Yetkisi, (Doktora Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2022.

PASLI, Ali: ''Compliance' Kavramının Anonim Ortaklıklar Hukukundaki Anlamı ve Sorumluluk Sistemine Etkisi", İÜHFM, 71(2), 2013, s. 317-334.

POLLACK, Andrew: "$4.9 Billion Jury Verdict In G.M. Fuel Tank Case", The New York Times, 10/07/1999.<https://www.nytimes.com/1999/07/10/us/4.9-billion-jury-verdict-in-gm-fuel-tank-case.html> (Erişim: 15.01.2025).

PULAŞLI, Hasan: Şirketler Hukuku Genel Esaslar, 4.Baskı, Adalet Yayınevi, Ankara 2016.

PULAŞLI, Hasan: "Compliance Kavramı ve Yönetim Organının Compliance Sorumluluğu", Banka ve Ticaret Hukuku Dergisi, 35(2), 2019, s.27-59.

SIRAKAYA, Elif Yalçın: "Anonim Şirketlerde Yönetim Yetkisinin Devri Bağlamında Yönetim Kurulunun Üst Gözetim Yükümlülüğü", Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi, 24(2), 2020, s.195-220.

SOKOL, D. Daniel: "Teaching Compliance", University of Cincinnati Law Review, 84(2), 2016, s.405-432.

TEKİNALP, Ünal: Sermaye Ortaklıklarının Yeni Hukuku, 5. Baskı, Vedat Kitapçılık, İstanbul 2020.

TUĞ, Mehmet Arif: "Kurumsal Yönetim Kavramının Genel Çerçevesi ve Türk Hukukundaki Yansımaları", Anadolu Üniversitesi Hukuk Fakültesi Dergisi, 5(1). 2019, s.203-227.

USUL, Hayrettin / MİZRAHİ, Rozi: Risk Odaklı Denetim, Detay Yayıncılık, Ankara 2016.

ÜLGEN Hayri / MİRZE, S. Kadri: İşletmelerde Stratejik Yönetim, 7. Baskı, Beta Yayınevi, İstanbul 2013.

DOĞAN, Beşir Fatih: "Yönetim Kurulunun Devredilemez Yetkileri ve Yönetim Yetkisinin Devri", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 18(2), 2012, s.609-640.

YANLI, Veliye: "Anonim Şirketlerde İmza Yetkileri Sadece Yönetim Kurulu Tarafından mı Atanabilir?", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71(2), 2013, s.439-448.

YAŞAR, Tuğçe Nimet/ SONGUR, Damla: "Anonim Şirketlerde Rekabet Hukuku Uyum (Compliance) Programının Oluşturulması ve İşlevleri-7246 Sayılı Kanun ile yapılan Değişikliklerle Birlikte", Banka ve Ticaret Hukuku Dergisi,

36(4), 2020, s. 87-129.

Yazar Beyanı | Author's Declaration

Mali Destek | Financial Support: Tayfun Ercan ve Ayşe Nur Tiryaki, bu çalışmanın araştırılması, yazarlığı veya yayınlanması için herhangi bir finansal destek almamıştır. | Tayfun Ercan and Ayşe Nur Tiryaki who is the author has not received any financial support for the research, authorship, or publication of this study.

Yazarların Katkıları | Authors's Contributions: Bu makale yazarlar tarafından birlikte hazırlanmıştır. Ayşe Nur Tiryaki tarafından hazırlan tez projesi kapsamında hazırlanmıştır. | This article was prepared by the authors. This article was produced within the scope of Ayşe Nur Tiryaki's thesis project.

Çıkar Çatışması/Ortak Çıkar Beyanı | The Declaration of Conflict of Interest/Common Interest: Yazarlar tarafından herhangi bir çıkar çatışması veya ortak çıkar beyan edilmemiştir. | No conflict of interest or common interest has been declared by the authors.

Etik Kurul Onayı Beyanı | The Declaration of Ethics Committee Approval: Çalışmanın herhangi bir etik kurul onayı veya özel bir izne ihtiyacı yoktur. | The study doesn't need any ethics committee approval or any special permission.

Araştırma ve Yayın Etiği Bildirgesi | The Declaration of Research and Publication Ethics: Yazarlar, makalenin tüm süreçlerinde İnÜHFD'nin bilimsel, etik ve alıntı kurallarına uyduğunu ve verilerde herhangi bir tahrifat yapmadığını, karşılaşılacak tüm etik ihlallerde İnÜHFD'nin ve editör kurulunun hiçbir sorumluluğunun olmadığını ve bu çalışmanın İnÜHFD'den başka hiçbir akademik yayın ortamında değerlendirilmediğini beyan etmektedir. | The authors declare that they complie with the scientific, ethical, and quotation rules of InULR in all processes of the paper and that they do not make any falsification of the data collected. In addition, they declare that Inonu University Law Review and its editorial board have no responsibility for any ethical violations that may be encountered, and that this study has not been evaluated or published in any academic publication environment other than Inonu University Law Review.