KÜRESEL BAKIŞ AÇILARI VE ANLAYIŞLAR

İç denetim ve uyum: Daha güçlü yönetişim için açıklık ve işbirliği

The Institute of Internal Auditors

Önceki Yayınlar

Küresel Bakış Açıları ve Anlayışlar broşürünün önceki sayılarına erişim için şu adresi ziyaret edebilirsiniz: www.theiia.org/GPI.

Okuyucu Geribildirimi

Soru ve yorumlarınızı şu adrese yollayabilirsiniz: globalperspectives@theiia.org.

İçindekiler Tablosu

Teşekkürler

IIA, Mark Carawan, Caroline Maurice, Vandana Siney, Karen Brady, Benito Ybarra, Mike Joyce, Stacey Schabel, Mani Sulur, Jee Kymm, Dana Lawrence, Geoff Rusnak, Paul Ricci, Senthil Kumar, Marta Budavari, Kathryn Reimann, Emily Wright, Akash Singh, Nora Ilmoni, Christine Ong, Calum Owen, Trygve Sorlie, Francis Nicholson, Jill Austin, ve IIA – Avustralya dâhil olmak üzere bu belgeye katkıda bulunan üyelere ve paydaşlara teşekkürlerini sunar.

IIA Hakkında

İç Denetçiler Enstitüsü (IIA) iç denetim mesleğinin en tanınmış savunucusu, eğitmeni ve standart, rehber ve sertifika sağlayıcısıdır. 1941 yılında kurulan IIA, bugün, 170'den fazla ülke ve bölgeden 200.000'i aşkın üyeye hizmet vermektedir. Birliğin global genel merkezi Lake Mary, Fla., ABD adresinde bulunmaktadır. Daha fazla bilgi için, lütfen www.globaliia.org sitesini ziyaret ediniz.

Sorumluluğun Reddi Beyanı

Küresel Bakış Açıları ve Anlayışlar' içerisinde yer alan görüşler, çalışmaya katkı sağlayan kişilerin ya da bu kişilerin çalışanlarının mutlak görüşleri değildir.

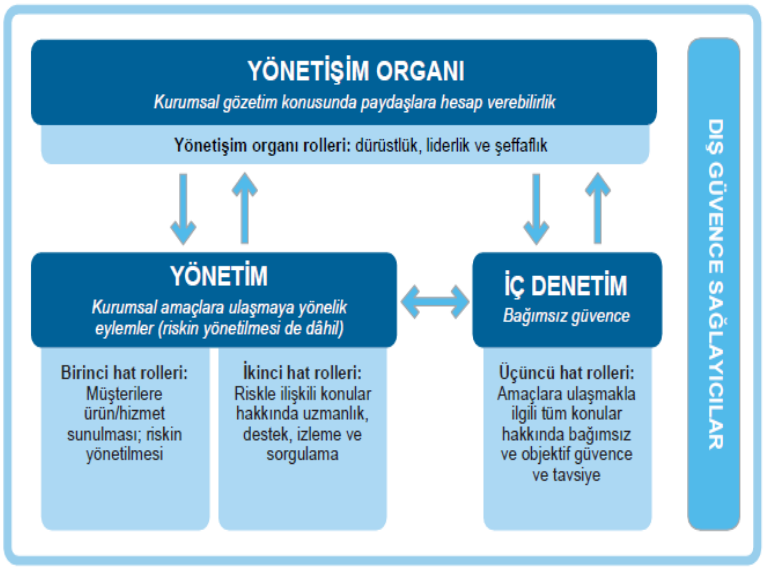
Telif Hakkı Uyarısı

Giriş

İç denetim ve uyum arasındaki ilişki bazen net olmayabiliyor ve bu da önemli sorular doğuruyor: İç denetimin uyum açısından sorumluluğu olabilir mi? Bir uyum departmanı, bir kurum genelindeki tüm uyumdan sorumlu mudur? Bir iç denetim yönetici olarak uyumdan sorumlu olmak uygun mudur?

Bu yayın, söz konusu karmaşıklıklara açıklık getirmeye ve kafa karışıklığını, boşlukları ve gereksiz tekrarları önlemeye yardımcı olmak üzere tasarlanmıştır. Sarih bir anlayış gereklidir, işbirliği ciddi bir biçimde teşvik edilir ve iç denetimin bağımsızlığı[1] temel öneme sahiptir.

Bu, uyumun nasıl denetlenmesi gerektiğine yönelik bir yayın *değildir*. Kurullar, yönetim, uyum uzmanları ve iç denetim yöneticileri için bir araç olarak kullanılmak üzere hazırlanmış olup iç denetim ve uyum arasındaki ilişkiyi açıklamanın bir yolu olarak *Üçlü Hat Modeli*nden faydalanmaktadır. Bu çalışma, *Üçlü Hat Modelinin* Altı Prensibi ve bunların uyum konusuna nasıl uygulanabileceğine dair derinlemesine bir bakış sunmaktadır.



Okuyucular bu çalışmayı, bir yönetişim yapısı içinde — ülke, sektör, karmaşıklık, olgunluk ya da büyüklükten bağımsız olarak — *Üçlü Hat Modeli* ile ilişkili olarak çeşitli açılardan etkin uyumu ve uyum riski yönetimini net bir şekilde tespit etmek, anlamak, değerlendirmek ve uygulamak için kullanmalıdır.[2] Risk ve uyum sorumluları ve iç denetçilerin uyum konularıyla ilgili sahada karşılaştıkları sorunlara yönelik pratik çizimler, uyum faaliyetlerinin *Üçlü Hat Modeli* ile uyuşup uyuşmadığını değerlendirirken modelin Altı Prensibinin pratik uygulaması konusunda yardımcı olacaktır. (Bkz. sayfa 8-16)

[1] Sürdürülebilir yönetişimin bir parçası olarak uyumun tamamlayıcı mahiyeti, *B20 Italy Integrity & Compliance Policy Paper 2021* (B20 İtalya Bütünlük ve Uyum Politika Belgesi 2021) dokümanında B20 İtalya tarafından G20 bakanlarına önerilmiş olan bir temel odak ve politika eylemidir. Özellikle sayfa 11'de yer alan Politika Eylemi başlığı altında Üçlü Hat Modelinde tanımlandığı gibi iç denetimin rolünden bahsedilmektedir.

[2] Bazı ülke ve sektörlerde uyum ve uyum riski yönetimiyle ilişkili roller ve sorumluluklar detaylı şekilde tanımlanmış olup bunlar kapsamlı yasama, düzenleme, içtihat hukuku ve akademik araştırma konusudur. Daha detaylı çalışmalar mevcuttur ve bu pratik dokümanın okuyucularının söz konusu detaylı çalışmaları incelemelerini öneririz. Örneğin bkz. Amerika Hukuk Enstitüsünün hazırladığı *Principles of the Law, Compliance, Risk Management, and Enforcement* No. 1 (Hukuk, Uyum, Risk Yönetimi ve Yürütmenin Prensipleri No. 1) ve *Principles of the Law, Compliance and Enforcement* No. 2 (Hukuk, Uyum, Risk Yönetimi ve Yürütmenin Prensipleri No. 2) çalışmaları.

Hesap Verebilirlik, Eylemler ve Güvence

Üçlü Hat Modeli, yönetişim organının hesap verebilirliğinin, yönetimin eylemlerinin ve iç denetimin sağlayacağı bağımsız güvencenin etkin yönetişimin temelini nasıl oluşturduğunu açıklamaktadır. Ayrıca Altı Prensibin bir kurumda ilgili rol ve sorumluluklara ilişkin bir değerlendirme yaparken nasıl yardımcı olduğunu göstermektedir. Modelin temel unsurlarının ve Altı Prensibin uygulanışı amaçlar, kaynaklar ve şartlara bağlı olarak her bir kurum için farklı olacaktır. Model, kurumlara hedeflerine ulaşmalarına en çok yardımcı olacak yapıları belirleme, süreçleri tasarlama ve sorumlulukları atama konusunda destek olur. Bu, yönetimin sorumluluğu olmakla birlikte[3] ortak bir çabayla ulaşılan uyum riski yönetimini de içermektedir.

Bir kurumun uyuma yönelik olarak dikkate alması gereken gereklilikler ve beklentiler kanunlar, kurallar ve yönetmelikler gibi kaynağı dışarıdan olan ve politikalar, standartlar, prosedürler ve iş ya da davranış kuralları gibi kaynağı içeriden olan unsurları içermektedir. Bunlar resmen ve açıkça tanımlanmış olabilecekleri gibi, toplumsal, etik yahut kültürel beklentiler gibi daha örtük de olabilir. Bu kapsamlı, dinamik telakki yelpazesine bu çalışmada "gereklilikler ve beklentiler" olarak atıfta bulunulmaktadır.

Paydaşlar bir kurumun amacına ulaşmasını ve yasal ve etik açıdan değerini en üst düzeye çıkarmasını beklerler. Kurumlar bu doğrultuda sağlık ve güvenlik, çalışma, veri koruma ve gizlilik, tüzel kişilik ve ticari kanun ve kurallar, sektöre ilişkin düzenlemeler, kalite standartları, rüşvet ve yolsuzlukla mücadele, yatırımcı ve tüketicinin korunması, mali raporlama ve vergilendirme ve bireysel davranış kuralları gibi temel alanlarda uyumu yakından izlemeye yönelik yatırım yapar. Liste daha da uzatılabilir. Uyum, etkin yönetişime genel bir yaklaşımın parçası olarak *Üçlü Hat Modelinde* tanımlandığı gibi hesap verebilirlik, eylemler ve güvence bağlamında anlaşılıp uygulamaya geçirilebilir.

Uyum Nedir?

Kurumlar, iş yapmanın bir ön koşulu olan geçerli kanunlar ve diğer harici gerekliliklere sadık kalmak (ya da uymak) zorundadır. Bu uyum gereklilikleri çalışan ilişkilerinden vergilerin ödenmesine kadar her şeyi kapsamaktadır. Belirli sektörlerde bir dizi kural koyucu organ, denetleyici ve düzenleyicinin yanı sıra tanımlanmış gereklilikler bulunur ancak diğer sektörlerde dışarıdan dayatılan yasal ve düzenleyici sınırlar ve kısıtlamaların sayısı daha azdır. Bununla birlikte kamu sektöründe ya da özel sektörde harici uyum gerekliliklerine tâbi olmayan bir kurum bulmak zordur.

Kurumlar aynı zamanda politika ve prosedür biçiminde kurum içi beklentileri tasarlar, geliştirir ve uygular; etik davranış ve iş yapışa yönelik standartlar belirler. Düzenlenmiş belirli sektörlerde harici gereklilikler, bir kurumun dâhili politikalar, standartlar ve davranış kuralları oluşturmasını ve bunlara sadık kalmasını zorunlu kılar. Bu kadar katmanlı bir gereklilikler ağı söz konusu olduğunda da bir kurum içinde "uyum" kavramı birçok boyuta sahip olmaktadır. Bu doğrultuda uyumu, kapsamlı ve birbiriyle ilişkili ancak farklı

[3] Bu belgenin amacı doğrultusunda *yönetim* kavramı, yönetişim organı ya da iç denetimin sorumluluğu olmayan rolleri belirtmek için geniş anlamda kullanılmaktadır.

yönlerini ve kurumlarda nasıl tartışıldığını göz önünde bulundurarak ele almak faydalı olacaktır: bir çıktı olarak; bir risk kategorisi olarak[4]; bir rol, departman, işlev vs. olarak[5] ve bir faaliyetler dizisi olarak.

Bunların her biri aşağıda tartışılmaktadır.

Bir çıktı olarak uyum

Kurumlar kanunlara, kurallara, politikalara, yönetmeliklere vs. uymak ya da "uyumlu olmak" için çeşitli faaliyetlere dâhil olur. Belirli uyum gerekliliklerini ve beklentilerini karşılamak kurumların faaliyet gösterebilmesi ve stratejik hedeflerinin peşinden gidebilmesi için sıklıkla bir ön şart olarak karşımıza çıkar.

Bir risk kategorisi olarak uyum

Uluslararası Mesleki Uygulama Çerçevesi riski *amaçlara ulaşılması üzerinde etkisi olacak bir olayın meydana gelme ihtimali* olarak tanımlamaktadır. Söz konusu etkiler olumlu olabileceği gibi olumsuz da olabilir. Dolayısıyla riski değerlendirirken uyum gerekliliklerini ve beklentilerini, uyumsuzluk olasılığı ve bunun hedefler üzerindeki potansiyel etkisiyle birlikte ele almak gerekir.

Kurumlar için hem uyum hem de uyumsuzluğa ilişkin riskler bulunur. Bunların etkileri, maddi ya da manevi olabilecek ödül ya da cezalar şeklinde olabilir. Örneğin, Uluslararası Standardizasyon Örgütünün (ISO) standartlarına uyumun, operasyonel etkinlik ve benzeri kazanımların yanı sıra uyulması zorunlu olmayan bir kurala gönüllü olarak uyumdan kaynaklı kuruma yönelik olumlu bir ilgi sağlaması tasarlanmıştır. Bunlara uymama bahsi geçen kazanımları ortadan kaldırır ve ayrıca doğrudan zarara neden olabileceği gibi para cezası kesilmesi, lisansların iptali, yaptırımlar, operasyonların sonlandırılması, hukuki ya da cezai kovuşturma ve fon ya da desteğin kaybı gibi cezalara da yol açabilir. Ayrıca uyumsuzluk potansiyel paydaş memnuniyetsizliği, halka açık eleştiri ya da başka tür zararlar şeklinde itibar riskine yol açabilir.

Uyum riski tespiti, ölçümü ve değerlendirmesi ve uyum riski iştahı ve toleransların belirlenmesi politikalar, prosedürler, sınırlar ve kontroller dâhil olmak üzere uygun yanıtların saptanmasına yardımcı olur.[6]

Bir rol ya da departman olarak uyum

Uyum ayrıca belirli gereklilikleri ve beklentileri karşılamak ya da uyumla ilişkili konularda gözetim, uzmanlık, kontrol ve sınama, izleme, test veya güvence imkânı sağlamak amacıyla oluşturulmuş bir rol ya da departmana atıfta bulunmak için de sıklıkla kullanılmaktadır. Bunlar *Üçlü Hat Modelinde* tanımlandığı gibi, yönetimin genel yetki alanı ve sorumlulukları içinde kalan ve rolün spesifik özelliklerine bağlı olarak birinci hattaki rollerin sahiplerine ve üst düzey yöneticilere uzman desteği ve risk yönetimi imkânı sunma olasılığını beraberinde getiren çeşitli birinci veya ikinci hat rollerinin özellikleridir.

---

[4] Bir risk sınıflandırması, bir kurumdaki geniş uyum riski kategorisi altında kanunlar, kurallar, yönetmelikler, politikalar ya da davranışlar açısından hem spesifik riskleri hem de bağlantılı riskleri ele alan bir alt kategoriler basamaklandırmasını ortaya koyar.

[5] Roller, davranış riski sorumlusu, veri koruma riski sorumlusu vs. gibi spesifik riskleri kapsayacak şekilde tanımlanabilir.

[6] Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (COSO) risk yönetimi için çerçeveler sunar ve ERM risk çerçevesinin uyum risklerinin yönetimine uygulanmasına yönelik yeni ilkeler dâhil olmak üzere ilgili konularda fikir önderliği yapar.

Yasal ve düzenleyici gerekliliklere ve ilgili kurumun faaliyet sektörüne, büyüklüğüne ve karmaşıklığına bağlı olarak bir kıdemli uyum rolü, spesifik sorumlulukları doğrultusunda hiyerarşik açıdan kurum içindeki farklı rollerden birine bağlı olarak çalışabilir. Söz konusu roller üst yönetim kadrosunu (örneğin, icra kurulu başkanı, risk direktörü, operasyon direktörü, baş hukuk müşaviri veya diğerleri) ve bunların ilgili yönetim zincirlerini içerebilir ve/veya kıdemli uyum rolü doğrudan yönetişim organı ya da atanmış alt komiteye bağlı olarak çalışabilir. Bir uyum rolü ya da departmanı, yine yukarıda belirtilen unsurlara ve iç denetim işlevinin bağımsızlığını temin edecek bir mekanizmaya bağlı olarak bazı durumlarda, iç denetim yöneticisine (İDY) ya da hem uyum departmanını hem de iç denetim departmanını yöneten bir kişiye bağlı olarak çalışabilir. Her bir rolün sorumluluklarının gerekliliklere ve beklentilere uyup uymadığını değerlendirmek için *Üçlü Hat Modelinde* tanımlanan Altı Prensip uygulanmalıdır. Modelde açıklandığı gibi, şayet sorumluluklar ile gereklilikler ve beklentiler arasındaki ilişki çıkar çatışması ya da objektiflik veya bağımsızlığa zarar olasılığını beraberinde getiriyorsa hafifletici aksiyon alınmalıdır. Ayrıca olası ya da olmuş çıkar çatışması durumlarının veya objektifliğe yönelik zararların ele alınabilmesi ve uygunsa, düzenleyici otoriteye bildirim dâhil olmak üzere, muhtemel aksiyonların alınabilmesi için yönetişim organına bildirilmesi gerekir.

Bir faaliyetler dizisi olarak uyum

Uyum; uyumu temin etmek, desteklemek, izlemek, gözetlemek, kontrol etmek, test etmek, sınamak veya doğrulamak için tasarlanan süreç ve kontrollere atfen kullanılabilir. Bu tedbirleri uygulayan kişiler, kurumun ve kurumun üyelerinin gerekliliklere ve beklentilere uyduğunu temin etmeye yardımcı olur.

Bir kurumda uyuma, kurum için veya kurumla çalışan herkesin rollerine ve kıdemlerine uygun eylemleri ve davranışları yoluyla ulaşılır.

Spesifik gereklilikleri ve beklentileri belirli bir düzeyde ve kabul edilebilir bir kesinlik derecesiyle karşılamak üzere tasarlanan rutin süreçler, prosedürler ve kontrollere yönelik sorumluluk kurum içinde çeşitli kişilerde toplanabileceği gibi kurum dışı kişilere de verilebilir. *Üçlü Hat Modeli*, gereklilikler ve beklentilere uyumu değerlendirmede temel bir unsurun uyum faaliyetleriyle ilişkili karar alma yetkilerini belirlemek olduğunu ortaya koymaktadır. (Ek bölümünde detaylı bir şekilde sunulmuş olan uyumu oluşturan rol ve faaliyetlere bakınız.)

Üçlü Hat Modeli

Uyum

Yönetişim organı, bu organın ve ayrıca yönetim ve iç denetimin eylemleri ve davranışları aracılığıyla temin edilebilen yönetişimin nihai sorumlusudur.[7]

Her bir kurum, ilgili harici gerekliliklere tâbi olarak kendi şartları doğrultusunda uyumun farklı yanlarına yönelik sorumluluklar atarken kurumda atanan bu spesifik rol ve sorumlulukların *Üçlü Hat Modelinin* Altı Prensibiyle ne kadar iyi bir uyum içinde olduğunu analiz etmelidir. Yapılan değerlendirme bazı sorumlulukların yönetişim organı rollerine, bazılarının uyum ve risk yönetimi dâhil olmak üzere yönetim rollerine, bazılarının ise iç denetim rollerine uygun olduğunu gösterebilir.

Birinci hat rolleri, gereklilik ve beklentilere uyarak müşterilere ürün ve hizmet sunmayı ve ayrıca bunun yapılabilmesi için gereken desteği vermeyi içerir. İkinci hat rolleri, uzman gözetimi ve tavsiyesi sunar, risk değerlendirmesi yapar (özellikle toplu ya da portföy bazında) ve risk yönetimi faaliyetleri (izleme, gözetleme ve test etme dâhil) gerçekleştirir ve bunları yaparken birinci hattı makul bir şekilde sınar. Üçüncü hat iç denetim rolü, ikinci hattın makul bir biçimde birinci hattı ne kadar iyi sınadığına ilişkin güvence de dâhil olmak üzere bağımsız güvence sunar. Bu üç hattın faaliyetlerinin yersiz çakışmalar, tekrarlar ve boşluklar ve ayrıca herhangi bir çatışma ya da uyumsuzluk olmaksızın gerektiği gibi uyum içinde olduğunu temin etmek için bu hatların uygun koordinasyon, iletişim ve işbirliği yoluyla etkin çalışmaları gerekir.

Modeli ortaya koymak için kullanılan grafikte bir uyum rolü ya da departmanı yahut başka herhangi spesifik ikinci hat rolü, departmanı ya da sorumlulukları belirtilmemektedir. Tanımlanmış bir organizasyon yapısına karşılık merkezi yönetişim rolleri arasındaki ilişkileri tarif etmektedir.

Uyum rolleri ve faaliyetleri için sorumlulukların belirlenmesi

Hesap verebilirlik, eylemler ve güvence; yönetişimin temel unsurlarıdır. Risk yönetimi, uyum, etik, sürdürülebilirlik, güvenlik, veri gizliliği, hukuk müşavirliği, mali kontrol ve benzeri konularda uzman departmanlar oluşturulması ve bu departmanların özellikleri birçok faktöre bağlıdır. Organizasyonel karmaşıklık, büyüklük, sektör, kaynaklar, düzenleme, yasalar ve kültür, yönetişim organının risk toleransı/iştahı ve ayrıca ilgili uzman departmandaki rollerin hedefleri ve sorumlulukları bu faktörler arasındadır.

[7] Yönetişim organı yapıları ülkeye, düzenleyici gerekliliklere ve münferit organizasyon tasarımına bağlı olarak farklılaşır. Burada yönetişim organlarından bahsederken çeşitli ülke ve endüstrilerde hem kamu sektörü hem de özel sektörde bulunan çeşitli yönetişim organı yapılarını kastediyoruz. Yönetişim organının şu sorumlulukları olabilir: kurumun yönünü tayin etmek; vizyon, misyon, değerler ve risk iştahını tanımlamak; risk ve risk yönetimi açısından planlanan, gerçekleşen ve beklenen çıktılar hakkında yönetimden raporlar almak.

Belirli sektörlerde spesifik düzenleyici kurallara tâbi olan kurumlarda ayrıca tanımlanmış bir uyum departmanı bulunmayabilir. Birçoğunda böyle bir departman yoktur; bunun yanı sıra kurumların, unvanlarında ya da iş tanımlarında uyum ifadesi bulunan çalışanları da olmayabilir.

Bununla birlikte, ayrıca tanımlanmış bir uyum rolü ya da departmanı bulunmasa dahi, bir kurum geçerli gerekliliklere ve beklentilere uyumu temin edebilmek amacıyla kendi özelliklerine orantılı bir biçimde rol ve sorumluluk dağılımı yaptığı ve ilgili kurum çalışanları tanımlanmış rollerine sadık kaldığı taktirde söz konusu kurum etkin yönetişimi sağlayabilir ve gereklilik ve beklentilere uyabilir.

Genel olarak karşılaşılan durumda kurumlar büyüdükçe, karmaşıklaştıkça, kaynakları arttıkça veya yoğun olarak düzenlemeye tâbi oldukça uyumun farklı yanlarına yönelik bireysel roller ve departmanlara ayrı, özel sorumluluk ve kaynak ayırmaya karar verebilir yahut yapılan düzenlemelerle buna mecbur kalabilir.

Ayrıca bir çalışan birden fazla rol üstlenebilir. Bu durumda söz konusu rollerin uyumluluğunun uygun bir değerlendirmeyle incelenmesi gerektiği gibi her bir rolün sorumlulukları ve bu rollerin ifasına yönelik gözetim ve güvenceye ilişkin net bir tanım bulunmalıdır. Bazı durumlarda yönetişim organı ve düzenleyicinin onayı gerekebilir.

Birden fazla rol söz konusu olduğunda daha yüksek uyumsuzluk riski, çıkar çatışması ve ayrıca hesap verebilirlik ve sorumluluk konularında daha az netlikle karşılaşılabilir. Gerektiğinde, yönetişim organına ve düzenleyici otoriteye bildirim yapılmasının yanı sıra, risk iştahı sınırları içinde kalabilmek için hafifletici aksiyon alınması gerekebilir.

Uyuma ulaşmaya yönelik ortak çaba

Ayrıca tanımlanmış bir uyum rolü ya da departmanı bulunduğu durumlarda dahi tüm uyum faaliyetlerinin bir kurumun yapısı içinde tek bir noktada odaklanmayacağını bilmek önemlidir. İcra direktörleri ve diğer direktörlerin yanı sıra her seviyeden çalışanın uyuma yönelik toplu çabaya katkıda bulunması gerekir. Sorumluluk ve hesap verebilirlik; uyumu temin etmek, uyum risklerini hafifletmek ve gereklilik ve beklentilere uyumu izlemek amacıyla bir kurumdaki hiyerarşik yapının, tanımlanmış rollerin ve hat yönetimi yapısının geneline yayılır.

Harici ve dâhili gereklilik ve beklentilere uyum sıklıkla tanımlanmış bir uyum departmanı dışında uzman departmanlar ya da bireylerce ele alınır. Bu departman veya kişilerin rolleri ve sorumlulukları, sektöre yönelik düzenlemelerce, belirli bir tekil veya bir dizi gereklilik ve beklenti şeklinde belirlenmiş olabilir. Örnek olarak şunlar verilebilir: insan kaynakları (İK) departmanı tarafından ele alınan İK kanun ve düzenlemelerine uyum; finans departmanı tarafından ele alınan mali raporlama ve vergi gereklilikleri.

Yukarıda önerildiği üzere, uyumun çeşitli yanlarının gözetlenmesi, izlenmesi ve test edilmesine ilaveten uyumun temin edilmesi konusundaki sorumluluklar farklı roller ve departmanlar arasında bölüştürülebilir. Netice itibariyle münferit bir rolün uyumla ilişkili özelliklerini ve rolün sorumluluklarını belirlerken Altı Prensibin uygulanmasının önemi ortadadır.

Etkin yönetişim, hem resmi hem de gayrı resmi iletişim, koordinasyon ve işbirliğinden fayda sağlar ve şeffaflığı destekleyip teşvik eder. Bununla birlikte şayet yönetişim ve kontrol yapılarında gayrı resmi etkileşimler uyum sorunlarının gerektiği gibi tespiti, eskalasyonu ve hafifletilmesini engellerse resmi yönetişim ve kontrol yapılarının etkinliği zayıflayabilir ve hesap verebilirlik ve sorumluluk sınırları bulanıklaşabilir.

Bir yönetişim modelinin etkinliğini ölçerken uyumu temin etmek için tasarlanıp geliştirilmiş resmi yönetişim yapısını değerlendirmenin yanı sıra, gayrı resmi yönetişim yapısının resmi yapıyı zayıflatıp zayıflatmadığını ya da buna zarar verip vermediğini, şayet zayıflatıyorsa bunun hangi noktalarda ve ne zaman gerçekleştiğini tespit etmek için kurumu gayrı resmi iletişim, karar alımı ve eylem hatları açısından da derinlemesine incelemek gerekir. Üçlü Hat Modeli iletişim, koordinasyon ve işbirliğini kolaylaştırmak ve desteklemek için güçlü resmi ve gayrı resmi etkileşimleri teşvik eder. Ancak gayrı resmi bir yönetişim yapısı uyumu engelleyebilir, kontrollerin etrafından dolanabilir ve neticede faydasız ve etkisiz uyum riski yönetimine ve sorumluluk ve hesap verebilirlik açısından bulanık bir tabloya yol açabilir. Rolleri, sorumlulukları ve eylemleri tespit etmek için *Üçlü Hat Modelini* uygulamak, kurumların etkin bir yönetişim çerçevesi tasarlamasına imkân sunar; buna uyum konusunda başarısızlıklara neden olabilecek gayrı resmi yönetişim, karar alımı ve eylem risklerini hafifletmeye yönelik tedbirler geliştirilmesi de dâhildir.

Etkin bir uyum programı resmi, belgelendirilmiş bir yönetişim ve kontrol yapısını benimsemeye ve buna sadık kalmaya teşvik etmekle kalmayacak, ayrıca böyle bir program bir uyum ve kontrol kültürünün geliştirilmesi ve sürdürülmesinde temel unsur olacak ve *Üçlü Hat Modelinin* etkinliğini arttıracaktır.

Altı Prensibi Uygulamak

Spesifik uyum gereklilikleri ve beklentileri dâhil olmak üzere bir kurumun şartlarını dikkate alan Üçlü Hat Modeli roller ve sorumlulukların değerlendirilmesi ve uyumlaştırılması için prensiplere dayanan bir yaklaşımı teşvik etmektedir. Modelin Altı Prensibi —bir çıktı olarak, bir risk kategorisi olarak, bir rol ya da departman olarak, bir faaliyetler dizisi olarak— uyumu ve bunun başarılı bir yönetişim çerçevesine katkısını daha iyi anlamak için kullanılabilir. (Altı Prensibe ilişkin detaylı bilgi için bkz. *Üçlü Hat Modeli*)

Prensip 1: Yönetişim gerekliliklerini belirlemek

Prensip 1 minimum yönetişim gereklilikleri olarak şunları ortaya koyuyor:

- Hesap verebilirlik (başarı için yönetişim organı tarafından paydaşlara).
- Eylemler ve kaynakların kullanımı (amaçlara ulaşmak için yönetim tarafından – risk ve uyumu yönetmeyi içerir).
- Güvence ve tavsiye (etkin gözetim ve şeffaflığı temin etmek ve güven ve sürekli gelişimi teşvik etmek için tüm hususlara ilişkin olarak bir bağımsız iç denetim işlevi tarafından).

Son kertede yönetişim organı, kurumun kabul gören standartlar ve toplumsal normlara uygun davranmasını temin etmekten sorumludur. Yönetim, yönetişim organı tarafından açıklanan risk iştahı doğrultusunda uyum ve uyumsuzluk ile ilişkili hususlarda risk yönetiminden sorumludur. Bu, spesifik olarak uyumun farklı yanlarına odaklanan bireysel roller ve ekipler belirlemeyi ve riskleri sahiplenen birinci hat ile makul sınama sunan ve birinci hattın risk iştahına uygun hareket etmesini teşvik eden ikinci hat arasında karar alma yetkilerini açıkça tanımlamayı içerebilir. İç denetim, uyuma yönelik kontrollerin yeterliliği ve etkinliği konusunda yönetime ve yönetişim organına güvence sağlar ve sürekli gelişim ve inovasyon için tavsiyelerde bulunur.

Sahadan Pratik Örnekler

> **Sağlık hizmeti oldukça düzenlenmiş bir sektördür ve dolayısıyla neredeyse her bir hizmeti sağlarken bazı kurallara, düzenlemelere ya da standartlara uyum söz konusudur. Hemşireler, doktorlar ve diğer klinisyenler sunulan her hizmetin uygun şekilde yetkilendirildiğini ve belgelendirildiğini temin etmek zorundadır. Uyum sorumlulukları bulunanlar (münferit roller ya da bir departman), belirli bir prosedürün belgelendirilmesi ve yetkilendirilmesine yönelik gereklilikler konusunda klinik departmanları bilgilendirebilir ancak nihayetinde süreçleri ve kontrolleri uygulama ve söz konusu gerekliliklere uyumu temin etme sorumluluğu birinci hat bakım verenlerdedir.**
>
> – Uyum ve İç Denetim Müdürü, Amerika Birleşik Devletleri

> **Çalıştığım sektörden verebileceğim bir örnek, kurum ve düzenleyici gereklilikler açısından en önemli uyum risklerinin bir listesini oluşturmak ve ilgili düzenleyici gerekliliklere uyumu gözeterek ve söz konusu risklerle orantılı bir şekilde faaliyetleri, kontrolleri, izlemeyi ve sorumlulukları uyumlaştırmaktır. Örneğin bir kurumda düzenleyici gereklilikler doğrultusunda**

bir kara para aklamayla mücadele uyum sorumlusu, gizlilik sorumlusu, rüşvetle ve yolsuzlukla mücadele sorumlusu vs. olabilir ve bu temel risk alanlarında uyumu temin etmeyi ve yönetimi sağlamayı desteklemek üzere ürün, açıklama, çalışma, şikâyet vs. konularında sorumluluklar ve belirlenmiş kaynaklar bulunabilir. Düzenli raporlama yönetişim organına yapılır ve faaliyetlerin tümü bağımsız iç denetime tâbidir.

– Baş Uyum Yöneticisi, Birleşik Krallık

Günümüzde kurumların karşı karşıya olduğu zorluklara iyi bir örnek de "çevresel, sosyal ve yönetişimsel" ya da "ESG" standartlarını benimseme ve kucaklama güdüsüdür. Yönetişim organı, yönetimi, kurumun yönetişim organı tarafından belirlenen strateji, standartlar ve toplumsal normlara uygun davranmasından sorumlu tutmakla yükümlüdür. ESG kurumun her bir köşesini, her bir çalışanı, tedarikçiyi ve müşteriyi kapsar, dolayısıyla yönetişim organı, yönetimin kuruma yönelik ESG risklerinin, harici kanun ve yönetmeliklerin, dâhili politika ve prosedürlerin, ilgili performans ölçümlerinin ve ayrıca söz konusu dâhili gereklilik ve beklentilere uyulduğunu ortaya koyacak güvenilir, doğru ve kıyaslanabilir verilerin açıkça ifade edildiğini garanti etmesi gerekir. Ayrıca hem yönetim hem de yönetişim organı ESG uyum hedeflerine ulaşıldığına dair güvence isteyecek ya da buna ihtiyaç duyacaktır. İlgili rolleri ve departmanları ve bunların ESG'yi benimsemesi ve uyumu temin etmek için gerekli olan faaliyetlerini tespit edebilmek için kurum çapında sorumluluk ve hesap verebilirliğe ilişkin detaylı bir harita çıkarılmalıdır.

– Baş Uyum Yöneticisi, Amerika Birleşik Devletleri

Prensip 2: Yeterli yönetişim gözetimi sağlamak

Prensip 2 şu açılardan yönetişim organının rollerini tanımlamaktadır:

- Yönetişim.
- Yönetimi gözetmek.
- Etkin bir iç denetim işlevi oluşturmak ve bunu gözetmek.

Yönetişim organı nihai olarak yönetişimden sorumludur ve uygun yapı ve süreçlerin tesisini sağlar. Bu, uyumun yanı sıra iç denetim rolünün gözetimine yönelik düzenlemeleri de içerir.

Yönetişim organı, riske maruziyet düzeyi ve stratejik hedefleri etkileme potansiyeliyle ilişkili olarak gereklilik ve beklentilere uyum konusunda sahip olduğu ve ihtiyaç duyduğu güvenin derecesini belirlemelidir. Yönetişim organı, uyum riski iştahı veya toleransını saptarken yönetimin uyum riski iştahı ve bununla bağlantılı toleranslara uygun olarak uyum çıktılarına ulaşmaya yönelik faaliyetleri ifasını ve atanmış rollerin ve departmanların ilgili sorumluluklarını yerine getirişini gözetleyecektir.

Yönetişim organı, iç denetimin uyum konusunda bağımsız ve etkin güvence ve tavsiye vermesine imkân sağlayacak biçimde konumlandırıldığını ve bu doğrultuda uygun kaynaklara sahip olduğunu temin etmelidir. Otoritesinin ve bağımsız konumunun emniyete alınması için İDY'nin yönetişim organına, bir bağımsız denetim komitesine ya da yönetişim organının eşdeğerde atanmış bir komitesine karşı sorumlu olmalıdır.

Sahadan Pratik Örnekler

Etkin bir yönetişim organı bir kurumda değişimi gerçekleştirebilir ve söz sahibidir. Bazen eskalasyonlar ve bildirimler iş akışı içinde olağan bir prosedür olarak yerine getirilmektedir fakat etkin gözetim sağlamak ve eski verilere dayalı ve geriye dönük değil 'şimdiye' odaklı bir istikamet çizebilmek ancak günceli yakalayabilen bir yönetişim organı ve kaliteli bilgilerle mümkündür. İç denetim, yönetişim organının yönetilen riskleri öngörebilmesi, bunlara yönelik gözetim sunabilmesi ve istikamet belirleyebilmesi için söz konusu risklere ilişkin net bir görüşünün olup olmadığını teyit etmelidir. Yönetimi uyum ve kontrol etkinliği açısından sınama ve yönetişim organına risk iştahı kapsamında uyum riski yönetiminin etkinliğiyle ilgili içgörü ve anlayış sağlama noktasında uyum önemli bir ikinci hat rolü oynamaktadır.

– Uyum Sorumlusu, Singapur

Hem sağlık sektöründe hem de diğer birçok sektörde uyum departmanlarının, uyum programının belirli unsurlarına yönelik günlük sorumlulukları bulunur; bunlara eğitim, danışma hattı izleme, etik kuralları yayınlama, geçmiş sorgulamalarını gerçekleştirme vesaire dâhildir. Bu faaliyetlerden bazıları uyuma ulaşmakla ilgiliyken bazıları politikalar belirlemek, izleme yapmak ya da uyum etkinliği hakkında üst yönetime ve yönetişim organına raporlama yapmakla ilgili olabilir. Uyum departmanı hiyerarşik olarak İDY'ye bağlıysa ve ona raporlama yapıyorsa iç denetim departmanı uyum programının etkinliğine yönelik bağımsız güvence sunamaz. Ancak bu gibi durumlarda yönetişim organına güvence sunmak üzere bir bağımsız üçüncü taraf sürece dâhil edilebilir.

– Uyum ve İç Denetim Müdürü, Amerika Birleşik Devletleri

Yönetişim organı uyum risklerinin iç denetimin denetim planında kapsamlıca değerlendirildiğini/dikkate alındığını temin etmeli, iç denetimin düzenlemeye ilişkin temel riskleri ve düzenleyici odak alanlarını içeren çok yıllık plan kapsamını anlamalı ve uyumla ilişkili raporların/faaliyetlerin sonuçlarını gözden geçirmelidir.

– İç Denetim Yöneticisi, Birleşik Krallık

Yönetişim organı hem yönetim hem de iç denetim için uyum riski yönetimi açısından tavrı belirler. Yönetişim organının uyum gözetiminde etkin olabilmesi için hem yönetim hem de iç denetim tarafından sunulan, uyumun durumuna yönelik uygun nicel ve nitel verilerin etraflıca, periyodik ve sık incelemesinin yapılması gerekir. Yönetişim organı ihlâllere, uyumsuzluklara ve iyileştirmeye odaklı yalnızca geriye dönük ve olaya dayalı yaklaşım yerine ileriye dönük uyum riski yönetimini sağlamak için çeşitli uyum riski yönetimi faaliyetlerini rutin gündem maddeleri olarak belirlemelidir.

– Baş Uyum Yöneticisi, Birleşik Krallık

Prensip 3: Birinci ve ikinci hattaki yönetim rollerini tanımlamak

Prensip 3 yönetim rollerini (kaynaklara, amaçlara, düzenlemelere vs. bağlı olarak birleştirilip ayrılabilecek birinci ve ikinci hat rolleri) tarif eder.

Birinci ve ikinci hat rolleri yönetimi oluşturur. Bunlar birinci hattın müşterilere ürün ve hizmet sunma sorumluluklarını ve ikinci hattın uzman gözetim sunma, riski değerlendirme (özellikle toplu ya da portföy bazında) ve risk yönetimi faaliyetleri gerçekleştirme ve bunları yaparken birinci hattı makul bir şekilde sınama sorumluluklarını yansıtır.

Bir uyum departmanı gibi ayrı departmanlar oluşturulabilir yahut doğrudan ya da yönetişim organının bir komitesi aracılığıyla yönetişim organına karşı raporlama sorumluluğu olan bir departman müdürü veya daha küçük ve az karmaşık kurumlarda bir kişi tayin edilebilir. Söz konusu departman müdürü ya da kişi hiyerarşik olarak CEO'ya veya yönetim içindeki belirlenmiş bir kişiye de bağlı olabilir. Departman müdürü ya da kişinin yönetişim organına karşı bu raporlama sorumluluğu ya da hesap verme yükümlülüğü söz konusu departman müdürü veya kişi için daha fazla bağımsızlık sağlayabilir. Bununla birlikte unutulmamalıdır ki bağımsızlığın temel bir unsuru, karar alma sorumlulukları olmamasıdır. Tipik olarak bir uyum rolündeki kişi müşteri kabulünden politika istisnaları belirlemeye, yeni ürün onayına vb. konularda bir derece yönetim düzeyinde karar alma sorumluluğu üstlenmektedir. Dolayısıyla yönetişim organına ya da yönetişim organının bir komitesine karşı raporlama sorumluluğu böyle bir departman, departman müdürü ya da kişi için aslında gerçek bağımsızlık sunmaz. İç denetim ve İDY, raporlama sorumluluklarında yönetimden bağımsızlıklarının yanı sıra hiçbir yönetim düzeyinde operasyonel karar alma sorumluluğuna sahip değildir ki bu da bir derece daha bağımsızlık sağlamaktadır.

Bu doğrultuda hatlarda rollerin özellikleri şöyle sayılabilir:

- Birinci hat rolleri: ürün ve hizmetleri sunarken kanunlara, düzenlemelere, davranış kurallarına, kurumsal politikalara vs. uyumu temin etmek. Uyum yönetimin sorumluluğu olarak devam eder.
- İkinci hat rolleri: münferit uyum rolleri ve departmanları çerçeveler oluşturur, gözetim yapar, tavsiye, izleme ve gözetleme sağlar, test ve sınama yönetimini üstlenir ve genellikle yönetim düzeyinde operasyonel karar alımı ve risk üstlenme güçlerini (örneğin müşteri kabulü, yeni ürün ya da hizmet onayı, işlem onayı, limit aşımı onayı, politika istisnaları vb. konuları kapsayabilir) bünyesinde barındırabilir.
- Üçüncü hat rolleri: iç denetim; uyum, yönetimin uyumu temin etmeye yönelik çabalarının etkinliği ve uyum rolü ya da departmanının uyum riski yönetimine yönelik gözetim ve kontrolünü izleme ve sağlamaya ilişkin çalışmaları konusunda bağımsız güvence sağlar. İç denetimin yönetim düzeyinde hiçbir karar alma sorumluluğu yoktur ve bağımsız olarak yönetişim organına raporlama yapar.

Bir kurum, *Üçlü Hat Modelini* kullanarak gereklilik ve beklentilere uyuma ulaşabilir ve ayrıca etkin ve sürdürülebilir yönetişime katkıda bulunup kanunsuzluk ve yolsuzlukla mücadele edebilir. Şeffaflığa dayandırılan uyum, bir kurumda uygun bir standart ortaya koyar. Ayrıca şeffaflığı teşvik eden etkin bir uyum programı hissedarlar, devlet organları, düzenleyici otoriteler ve düzenleyici faaliyetlerin paylaşımı için platformlar, tedarikçiler ve tedarik zinciri dâhil olmak üzere harici paydaşlara kuruma yönelik güven aşılar.

Sahadan Pratik Örnekler

Birinci ve ikinci hat rolleri, kurumun uyum risklerinin nasıl hafifletileceğini belirlemek, yönetmek ve izlemek için etkin bir biçimde birlikte çalışmalıdır. Bir şeyleri izlemesi, test etmesi

ve bulması için iç denetime bel bağlanmamalıdır. Bunu yapanlar ve sorumluluğu üstlenenler birinci ve ikinci hat rolleri olmalıdır.

– Baş İdareci, Amerika Birleşik Devletleri

Bir uyum rolü, süreçlerin ve kontrollerin net bir biçimde uyumlaştırıldığını temin ederek kuruma destek olmalıdır. İkinci hat olarak bir uyum rolünün kuruma tavsiyede bulunduğu birçok durum söz konusudur. Ana performans göstergeleri ve ana risk göstergeleri, kurumun, etkin kontrole yönelik riskleri tespit edip yönetmesini destekleyecektir.

– Baş Uyum Yöneticisi, Meksika

Birçok endüstri, sayısız karmaşık düzenlemeye tâbidir. Uyum departmanı, herhangi bir departmandaki düzenleyici gereklilikler veya son yapılan düzenleyici değişiklikler hakkında uzmanlığını ve tavsiyesini sunar. Örneğin, sağlık sektöründe, uyumu sağlamak için gerekli kontrollerin tasarlanması ve uygulanmasından çeşitli klinik departmanların yönetimi sorumludur. Uzmanlığı dolayısıyla uyum departmanı, bu gerekliliklere uyumu değerlendirmek için ideal bir konumdadır.

– Baş Uyum Yöneticisi, Amerika Birleşik Devletleri

Daha büyük firmalarda iyi yönetilen ancak önemli bir zorluk da uyum gerekliliklerini ve beklentilerini kimlerin üstleneceği, bunların ne tür yükümlülükler getirdiği ve uyum rolleri ya da uyum departmanlarındakilerin bu süreçleri nasıl yürüttüğüdür. Bu, sağlam yönetişim yoluyla etkin eskalasyon rotalarının tesis edildiği anlaşılır ve açık hesap verebilirlik ve rol ve sorumluluk hatlarına sahip çok net bir risk yönetimi ve kontrol çerçevesi gerektirir. Bu olmadan, uyumluluk gözetimi bulanık kalacak ve yürütülmesi zor olacaktır.

– Baş Uyum Yöneticisi, Birleşik Krallık

Uyum herkesin sorumluluğudur. Sağlık gibi yüksek düzeyde düzenlemeye tâbi sektörlerde, bu sorumluluk her bir bakım vereni ilgilendirir ve herhangi bir prosedür için yetkilendirme ve belgelendirme gerekliliklerine uyumu içerebilir. Uyum departmanı belirli işlemler veya prosedürler için politikalar, süreçler ve kontroller geliştirirse veya ilgili bir prosedür kapsamında rutin bir sorumluluğa sahipse, nesnel bir güvence sunamaz. Bununla birlikte bir işlem veya prosedürle ilgili düzenleyici gereklilikler hakkında tavsiye ve danışmanlık vermek, uyum departmanının objektifliğini etkilemeyecektir.

– Uyum ve İç Denetim Müdürü, Amerika Birleşik Devletleri

Prensip 4: Üçüncü hattın rolünü tanımlamak

Prensip 4 bağımsız güvence ve tavsiye sağlayıcı olarak iç denetimin rolünü tarif eder.

Üçlü Hat Modeli, yönetişimin temel bir bileşeni olarak kontroller dâhil olmak üzere risk yanıtlarının yeterliliği ve etkinliğine ilişkin güvenceye olan kritik ihtiyacı kuvvetlendiriyor. Bu bağlamda uyum ve uyum riski yönetimine ulaşmak, bunları izlemek ve bunlara ilişkin gözetim sağlamaya yönelik risk yanıtları ve kontrollerine atıfta bulunulmaktadır. Bu da, kurumun yönetimden bağımsız tek güvence sağlayıcısı olarak

iç denetim tarafından yetkinlikle yürütülen sistematik ve disiplinli süreçler, uzmanlık ve iç görü ve anlayış sayesinde mümkün olur.

Uyum rolleri ile iç denetim rolleri arasında etkin koordinasyon ve işbirliği, her birinin birbirinden farklı rollerini yerine getirmedeki etkinliğine zarar vermeden bir kurumun yararına olabilir.

Bir kurumda çeşitli roller ve hesap verebilirlik unsurları bulunmasının bir sonucu olarak, bir bütün halinde ele alındığında bir kurum hakkında kapsamlı, karma bir bakış açısı sağlayabilecek başka güvence kaynakları olabilir. Ancak bu tür bir güvencenin kalitesini ve objektifliğini ölçmek için spesifik rolleri ve bunların birbiriyle uyumlaşmasını *Üçlü Hat Modeline* göre analiz etmek ve değerlendirmek önemlidir.

İç denetim hem yönetişim organına karşı hesap verebilirliğini hem de yönetim sorumluluklarından bağımsızlığını korur. Bu, güvence rollerini ve iç denetimin yönetişim yapısı içindeki farklı konumunu anlama noktasında kritik öneme sahiptir. İç denetim faaliyetinin bağımsızlığı ve iç denetçilerin nesnelliği tehdit altındaysa, İDY, düzeltici eylemler alınması için bunu yönetişim organına bildirmelidir.

İç denetçiler uyum rolleri ve departmanlarının etkinliğini değerlendirirken *Üçlü Hat Modelini* etkin biçimde uygulayabilmek ve bir uyum ve kontrol kültürünü teşvik etmek için iletişim, koordinasyon ve işbirliğine açık olmalıdır.

Sahadan Pratik Örnekler

> **Sorunları hafifletmek için gerçekleştirilen faaliyetlerin etkinliği, uyum riskinin yönetimini değerlendirirken ele alınması gereken temel bir konudur. Spesifik uyum riski unsurlarına yönelik sağlam bir risk değerlendirmesi ve faaliyetlerin bu risklerle orantılı olarak uyumlaştırılması önemlidir. Aksi halde kurumu uyumsuzluk risklerinden koruma konusunda fayda sunmayan birçok faaliyet gerçekleştiriliyor olabilir.**
>
> – İç Denetim Yöneticisi, Güney Afrika

> **İç denetçileri özellikle zorlayan bir durum da kanun ve düzenlemelerin ihlâli, politikaların, standartların ve davranış kurallarının çiğnenmesi gibi uyumsuzluk durumlarına yönelik bariz tespitlerin iç denetim işlerine dâhil edilmesi ve bunların raporlanmasıdır. Bu tür bir güvence sunulabilmesi için arzu edilen uyum çıktısına ulaşıldığını etkin biçimde değerlendirebilmeyi ve raporlayabilmeyi mümkün kılacak yeterince kalifiye kaynaklara erişim gereklidir.**
>
> – İç Denetim Yöneticisi, Birleşik Krallık

Prensip 5: Üçüncü hattın bağımsızlığını korumak

Prensip 5 iç denetim bağımsızlığının önemini tarif eder.

Üçüncü hat olarak iç denetimin bağımsızlığını açıklamaya yardımcı olacak bazı özellikleri bulunmaktadır. Bunlar yönetişim organına ya da bir yönetişim organı komitesine karşı bağımsız bir hiyerarşik raporlama sorumluluğunu ve yönetim düzeyinde karar alımından bağımsızlığı içerir.

Sıklıkla yönetişim organına ya da bir yönetişim organı komitesine karşı bir işlevsel raporlama sorumlulukları bulunmakla birlikte, (uyum riski yönetimi işlevleri dâhil olmak üzere) risk yönetimi işlevlerinin ilgili rolleri kapsamında aynı zamanda tipik olarak yönetim düzeyinde karar alma sorumlulukları

da bulunur; bu bağlamda özellikle, uyum riski de dâhil olmak üzere, risk alımı, yönetimi, azaltımı, kontrolü ve raporlamasına ilişkin sorumluluklar söz konusudur.

İkinci hat, birinci hatta yönelik etkin ve makul sınama sağlama sorumluluğunu koruyabilir. Buna karşın iç denetimin yönetim düzeyinde karar alımından bağımsız olması, yukarıda Prensip 3'te de detaylandırıldığı gibi üçüncü hattın rolü ve ikinci ve birinci hatların rolleri arasında önemli bir ayrıştırıcı husustur.

Sahadan Pratik Örnekler

> **İç denetim açısından herhangi bir çatışma olmaması için iç denetçilerin kurumdaki kontrolleri tasarlamamış yahut uygulamamış ya da yönetim düzeyinde karar alımına katılmamış olması gerekir; iç denetimin odağı, temel risklerin amaçlandığı gibi tespit ve kontrol edilip edilmediğini belirlemek amacıyla gözlem, test ve değerlendirme yapmaktır. Hiçbir önyargıları yahut beklentileri olmamalıdır.**
>
> – İç Denetim Yöneticisi, Avustralya

> **İç denetimin ana paydaşı yönetişim organıdır ve iç denetimin organizasyonel bağımsızlığı sonuçları ve önerileri sansürsüz şekilde raporlamasına imkân sağlar. Kontrol mekanizmaları ve bunları hayata geçiren kişilerin olumlu resmedilmesini temin etmeye yönelik bir beklenti ya da ihtiyaç yoktur. İç denetim, doğruyu ve gerçeği raporlama konusunda hesap verir konumdadır.**
>
> –Denetim ve Uyum Müdürü, Amerika Birleşik Devletleri

> **Uyumun ikinci hat rolleri politikaları belirler, işletmelere kontrol tasarımına ilişkin tavsiyede bulunur, ticari risk iştahlarını gözden geçirir ve bu konuda tavsiye verir ve ayrıca güvence sunar. Uyum departmanları ya da uyum için görevlendirilen kişiler birinci hat adına operasyonel işlevleri yerine getirmeye yönelik sorumluluklara sahip olabilir. Bu tür durumlarda uyum departmanları ya da uyum için görevlendirilen kişiler birinci hattan tamamen bağımsız değildir. Birinci ve ikinci hattın sahip olduğu yönetim düzeyinde karar alma sorumluluğu bulunmadığından tam manasıyla bağımsız olan tek faaliyet iç denetimdir.**
>
> – Kurumsal Risk ve İç Denetim Müdürü, Amerika Birleşik Devletleri

Prensip 6: İşbirliği yoluyla değer yaratmak ve bunu korumak

Prensip 6 sayılan tüm bu roller arasında koordinasyon ve işbirliğini temin etmenin önemini tarif eder.

Etkin yönetişim, yalnızca sorumlulukların uygun şekilde paylaştırılmasını değil aynı zamanda faaliyetlerin koordinasyon, işbirliği ve iletişim yoluyla güçlü bir biçimde uyumlaştırılmasını gerektirmektedir. Yönetişim organları; hedeflere ulaşabilmesi, riski yönetebilmesi ve değer yaratabilmesi için yönetime istikamet çizebilmek ve gözetim sorumluluğunu yerine getirebilmek için yönetim, iç denetim ve diğerlerinden gelen raporlara riayet etmektedir. Birinci, ikinci ve üçüncü hat rolleriyle birlikte yönetişim organı rolleri, birbirleriyle ve paydaşların öncelikli çıkarlarıyla uyumlaştırıldığında değer yaratılmasına ve değerin korunmasına hep birlikte katkıda bulunurlar. Bu doğrultuda uyum sorumluluklarının, karar alma yetkilerinin, raporlama yükümlülüklerinin, risk iştahının, ortak sınıflandırmaların, iyi tanımlanmış değerlendirme birimlerinin, gereklilikler ve beklentilere yönelik performans ve risk raporlamalarının ve test ve güvence programlarının kurum çapında açıkça duyurulması koordinasyon ve işbirliğini iyileştirmeye hizmet eder.

Sahadan Pratik Örnekler

Koordinasyon ve işbirliğine örnek olarak veri gizliliği verilebilir. Uyum ya da bazı kurumlarda hukuk departmanıyla işbirliği içinde uyum, düzenleyici gereklilikleri tespit eder, bunları kuruma duyurur ve uygun süreç ve kontrollerin hayata geçirilmesini temin eder. İş ekipleri (operasyon, BT, bilgi güvenliği vs.), gerektiği gibi bilginin izlenmesi, eskalasyonu ve raporlanması da dâhil olmak üzere ilgili faaliyetleri gerçekleştirir. Bilgi güvenliği ekibi ve uyum ekipleri, iş ekiplerinin prosedürleri uyguladığını ve uygun şekilde izleme ve raporlama yaptığını temin etmek için temel risk alanlarını izlerler. İç denetim söz konusu alanları denetlerken uyum riski dâhil ilgili riskleri ve iş ekiplerinin üstlendiği ilişkili süreçleri ve kontrolleri yönetmek için çizilmiş çerçeveyi değerlendirir.

– Baş Uyum Yöneticisi, Birleşik Krallık

ESG (çevresel, sosyal ve yönetişimsel standartlar), gerekliliklere ve beklentilere uyumu temin etmek için kurum çapında koordinasyon ve işbirliğine iyi bir örnektir. Birinci, ikinci ve üçüncü hat rolleri, hedeflenen ESG çıktılarını elde edebilmek için kendi ilgili rolleri kapsamında birlikte ve aynı zamanda yönetişim organının gözetimi altında çalışmalıdır. Çeşitli uyum sorumlulukları bulunanlar, kurumun ESG hedeflerine ulaşmak için kurumdaki diğer kişilerle birlikte çalışacaktır:

- **Yönetişim organı stratejiyi ve risk iştahını belirler ve kurumda kültür ve davranış açısından tavrı ortaya koyar.**
- **Yönetim, ESG gereklilikleri ve beklentilerini kurumun yönetişimine ve operasyonlarına entegre eder.**
  - **ESG ile ilişkili stratejik ve operasyonel planlama, amaç belirleme, veri toplama, karar alma ve raporlama için uygun yapılar, sistemler ve süreçlerin içeriği, tasarımı ve uygulamasına yönelik tavsiyelerde bulunur, çerçeve ve gereklilikleri belirtir.**
  - **ESG'ye yönelik harici gereklilik ve standartların yanı sıra kurum içi politika ve hedeflere uyumu temin etmeye ilişkin riskleri değerlendirir.**
  - **ESG çıktılarına ulaşmayı etkileyecek unsurları ölçmek, izlemek ve raporlamak için benimsenmesi gereken standartları, çerçeveleri, prensipleri veya modelleri geliştirir.**
  - **Sürdürülebilirlik ve ESG raporlamasında faydalanılacak verilerin ve bunları toplamak için kullanılan yöntemlerin doğruluğunu ve tutarlılığını değerlendirir.**
  - **Ölçüm ve değerlendirme süreçlerini belirler; önemlilik tanımını ve ilgili göstergelerin (KPI'lar) listelemesini yapar; raporlama yöntemleri, kılavuzları ve araçlarını (hem kurum içi hem kurum dışı) tanıtır.**
- **İç denetim, yukarıda sayılan faaliyetler ve yönetimin ESG hedeflerine ulaşması konusunda yönetişim organına bağımsız güvence sunar; ayrıca gereklilik ve beklentilere uygunluk konusunda raporlama yaparak yönetime de güvence sunar.**

– Baş Uyum Yöneticisi, Birleşik Krallık

Uyum Hakkında Temel Bilgiler

Dikkate değer on önemli çıkarım:

1. Uyum için ayrılmış kaynak, departman, yönetici vs. olmayabilir. Her kurum kaynaklarını bu şekilde bölemeyebilir yahut bunu yapmasına gerek de olmayabilir. Sıklıkla, kurumlar daha kompleks hale geldikçe, yoğun bir şekilde ya da spesifik olarak düzenlemelere tâbi oldukça, büyüdükçe, daha fazla incelemeye maruz kaldıkça, hızla değişen ortamlarda (düzenleme, ticaret vs. açısından) faaliyet göstermeye başladıkça ve benzer unsurları ele almaya başladıkça bir iş bölümü ve organizasyonel tasarımın resmi bir bileşeni olarak uyumun farklı yanlarına bireylerin, ekiplerin, sistemlerin ve/veya başka kaynakların atanması gerektiğine karar verir. Bu tür kaynaklar bazı kurumlarda harici olabilir; örneğin belirli uyum izleme görevi ya da konu uzmanlığı için dış kaynak kullanımı.

2. Uyumla alakalı rolleri değerlendirmek için *Üçlü Hat Modelinin* Altı Prensibini uygularken ilgili rolün sorumlu olduğu çıktıları göz önünde bulundurmak faydalı olacaktır:

- Ürün ve hizmetleri sunarken kanunlara, düzenlemelere, sözleşmelere, politikalara, prosedürlere, davranış kurallarına yahut diğer gerekliliklere uyumu temin etmek.
- Uzman gözetim sunmak, riski değerlendirmek (özellikle toplu ya da portföy bazında) ve risk yönetimi faaliyetleri gerçekleştirmek ve kurum çapında cari davranış kuralları ya da standartlar, gereklilikler ve beklentilere uygun olarak uyumu teşvik ve temin etmesi için birinci hattı makul bir şekilde sınamak.
- Uyum programının yeterliliği ve etkinliğine yönelik bir değerlendirme sunmak.
- Uyum programı ve bunun bileşenlerinin etkinliğine yönelik olarak kurum çapında uzman sınama sağlamak.

3. Bir kurumda tek bir uyum rolü ya da departmanı bu kurum için uyumla alakalı tüm hususları kapsayamayabilir[8]. Bu tür durumlarda kurumun uyum rolünün/rollerinin veya departmanının/departmanlarının kapsamını açıkça belgelendirmesi gerekir; ayrıca diğer gereklilik ve beklentiler konusundaki sorumlulukların hangi rollere verildiği de açık olmalıdır. Bu, - birden çok sorumluluk ve rolün bir kişiye verildiği ve bazı sorumluluklar için dış kaynak kullanımı yapılabilecek - küçük kurumlar için olduğu kadar - çeşitli uyum faaliyetleriyle görevlendirilen birden fazla rol veya departman bulunabilen - büyük kurumlar için de önemlidir.

4. Bir uyum rolü ya da bir uyum departmanının müdürü pratikte ve yasal ve düzenleyici gerekliliklere tâbi olmak kaydıyla bir kurumda birden fazla farklı rolden birine raporlama yapabilir. Bu roller arasında şunlar sayılabilir: üst yönetim kadrosu (örneğin icra kurulu başkanı, risk direktörü, operasyon direktörü, baş hukuk müşaviri veya diğerleri) ve/veya yönetişim organı ya da bunun bir komitesi. Bazı durumlarda uyum, yönetimin bir parçası olmakla birlikte, İDY'ye raporlama yapabilir. Bu raporlama ilişkisinin uygunluğu

[8] Örnek vermek gerekirse etik, sürdürülebilirlik, mali raporlama, veri gizliliği, insan kaynakları ve yasal yükümlülükler birimleri uyumu temin etmek veya uyumun spesifik bileşenleri için ilave gözetim ve risk yönetimi sağlamak üzere kendilerine özgü kurum içi ve/veya kurum dışı kaynaklara sahip olabilir. Örneğin çevresel, sosyal ve yönetişimsel (ESG) kriterlerin evrimiyle birlikte birçok kurumda ESG'nin kapsamlı yanlarına uyumu sağlamaya odaklanan bir dizi yeni rol, sorumluluk, faaliyet ve departman ortaya çıkıyor.

kısmen sorumlulukların *Üçlü Hat Modeline* ve ilgili yasal ve düzenleyici gerekliliklere uygunluğunu değerlendirmek suretiyle belirlenebilir.

5. Bir uyum rolü ya da bir uyum departman müdürünün bir ya da birden fazla kurul komitesi veya bir ya da birden fazla kurul komitesinin başkanı ile raporlama ilişkisi olabilir yahut raporlama konusunda bunlara karşı hesap vermesi gerekebilir. Fakat bu durum yönetimden bağımsızlık anlamına gelmez ve iç denetim tarafından sağlanan bağımsız güvenceye olan ihtiyacı ortadan kaldırmaz.

6. Münferit uyum rolleri ve uyum departmanlarının sorumlulukları şu sayılanları içerebilir ancak bunlarla sınırlı değildir: uyum riski yönetimi, izleme, test etme, analiz, değerlendirme, tavsiye, güvence, politika belirleme, sistem ve kontrol geliştirme ve uygulama, yönetim kararları, gözetim ve eğitim.

7. Uyum rolleri ve departmanları ayrıca ürün ve hizmetlerin sunulmasıyla yakından ya da doğrudan ilişkili sorumluluklara sahip olabilir. Bunun için rol kapsamındaki sorumlulukların, yetkinin ve hesap verebilirliğin açıkça belgelendirilmesi gerekir (örneğin, ürün veya hizmet sunumunda aykırılık durumlarını bir işlemi engelleyerek ya da bir yönetim kararını reddederek önleme yetkisi).

8. Birinci ve ikinci hat rolleri ayrılmalıdır. Birinci hattakiler aldıkları riski üstlenirken ikinci hattakilerin birinci hattın üstlendiği riskleri yönetmesine yardımcı olacak çerçeve ve standartları belirlemesi ve gözetlemesi ve bir yandan da birinci hattın karar ve faaliyetlerine yönelik makul sınama sağlaması gerekir. Pratikte, ülke ya da sektör gerekliliklerine ve kurumun büyüklüğü, karmaşıklığı ve diğer faktörlere bağlı olarak harmanlanmış roller söz konusu olabilir. Bu durumda ilgili rollerin uyumluluğunun bir değerlendirmesi yapılmalı ve ilgili riskler hafifletilmelidir. Bu, bir rol kapsamındaki uyumsuz bir faaliyetler dizisinden kaynaklanan riskleri etkin biçimde hafifletmek için rollerin harmanında ayarlamalar yapmayı gerektirebilir. Riski yönetme sorumluluğu birinci hat rollerinin bir parçasıdır ve yönetimin kapsamı dâhilindedir.

9. Yönetim, kurumların uyum yükümlülüklerine ayrılan kaynaklarını nasıl yapılandırdıklarına bakılmaksızın, kurumun yönetişim organı tarafından belirlenen risk iştahı parametreleri kapsamında gereklilik ve beklentileri karşıladığını temin etme sorumluluğunu haizdir.

10. İkinci hat uyum rolünün temel bir sorumluluğu da kurumun uyum programının ve kurumun uyum gerekliliklerini ve beklentilerini temin etmesi için gereken çabaların etkinliğini değerlendirmektir.

EK: Uyum Rolleri ve Faaliyetlerine Yönelik Sorumlulukların Uyumlaştırılması

Uyum faaliyetleri bir kurumun yönetişim, risk yönetimi ve iç kontrol faaliyetlerinin temel bir bileşenidir. Uyumu temin etmek, desteklemek, kontrol etmek ve teyit etmek için gereken eylemlere yönelik sorumluluk ve bu sorumlulukların yerine getirilmesi kurumun çeşitli bölümlerine paylaştırılabilir. Uyum faaliyetlerinden sorumlu olanlar uyumu oluşturan beklenen çıktıları tanımlamalı ve ayrıca söz konusu çıktılara ulaşıldığını gösterecek uygun ölçüm yöntemlerini belirlemelidir.

Uyumu oluşturan faaliyetler şunları içerebilir ancak bunlarla sınırlı değildir:

- Kurum hedefleriyle paralel ilgili harici kanunlar, kurallar, düzenlemeler ve kurum içi politikalar, standartlar, prosedürler ve iş ve davranış kurallarını tespit etmek.
- Kurum hedefleriyle paralel ilgili harici kanunlar, kurallar, düzenlemeler ve kurum içi politikalar, standartlar, prosedürler ve iş ve davranış kurallarına uyum ve uyumsuzluk durumu için uygun risk ölçüm yöntemlerini belirlemek.
- Kurum hedefleriyle paralel ilgili harici kanunlar, kurallar, düzenlemeler ve kurum içi politikalar, standartlar, prosedürler ve iş ve davranış kurallarına uyum için, mevcut ve gelecekteki riskleri de kapsayacak şekilde risk değerlendirmesi gerçekleştirmek.
- Kurum hedefleriyle paralel ilgili harici kanunlar, kurallar, düzenlemeler ve kurum içi politikalar, standartlar, prosedürler ve iş ve davranış kurallarına uyumu temin edecek süreçler ve kontroller tasarlamak, geliştirmek ve hayata geçirmek.
- Kurum hedefleriyle paralel ilgili harici kanunlar, kurallar, düzenlemeler ve kurum içi politikalar, standartlar, prosedürler ve iş ve davranış kurallarına uyumu temin edecek süreçler ve kontrolleri gerçekleştirmek, sürdürmek ve yönetmek.
- Kurum hedefleriyle paralel ilgili harici kanunlar, kurallar, düzenlemeler ve kurum içi politikalar, standartlar, prosedürler ve iş ve davranış kurallarına uyumu değerlendirmek, test etmek ve izlemek.
- Yönetime uyum riski bağlamında makul sınama sağlamak.
- Uyum riskini yönetmek ve hafifletmek.
- Uyum veya uyumsuzluk olaylarını belirlemek.
- Uyumsuzluk olaylarını bildirmek ve üst makamları bilgilendirmek.
- Uyum veya uyumsuzluk durumlarını harici ve dâhili gerekliliklere uygun olarak raporlamak.
- Uyum için elverişli bir kültürü teşvik etmek.
- İletişim, eğitim ve tanıtım yoluyla farkındalığı arttırmak.

- Uyumun farklı yanlarına yönelik istişarelerde bulunmak ve tavsiye vermek.
- Bir etik bildirim ya da gizli ihbar (whistleblowing) programı oluşturmak ve bunu korumak.
- Uyum eğitimi geliştirmek ve vermek ve farkındalık sağlamak.
- Düzenleyici yetkililer ve kurum arasında düzenleme konularına ilişkin aracılık sorumluluklarını yerine getirmek.
- Kurumun ve ilgili faaliyetlerinin sadık kalması gereken veya sadık kalmayı tercih edeceği ilgili standartları, kuralları veya kılavuzları tespit etmek ve ayrıca kıyaslama (benchmark) bilgilerinin toplanması ve raporlamasını kolaylaştırmak için mesleki kurumlar ve sektör kuruluşlarıyla ilişkiler geliştirmek ve sürdürmek.
- Altyapı kullanıcıları ve diğer taraflar için gereklilik veya beklentileri belirleyebileceği gibi bunlara uyumu şart koşabilecek sektör altyapı kurumlarıyla bir köprü sunan ilişkiler kurmak ve sürdürmek. (Ç.N. altyapı kurumları; sivil toplum sektörü için kapasite geliştirme, teknik destek, danışmanlık, atölye, eğitim, konferans, savunuculuk ve araştırma gibi faaliyetler yürüten ve sıklıkla kendileri de kâr amacı gütmeyen kurumlardır.)

Her bir rolün sorumlulukları ve beklenen çıktılarının net olması önem arz eder. *Üçlü Hat Modelinde* detaylı açıklandığı üzere, işlem onayı, müşteri kabulü veya diğer iş riski karar alma rolleri ve faaliyetlerinden bazıları üçüncü hat sorumlulukları kapsamındaki diğer rollerle uyumsuzdur. İç denetimden bu tür rolleri üstlenmesi istendiği taktirde yönetişim organı ya da denetim komitesinin rızasının alınması, bu durumdan etkilenen alanlarda bağımsız güvence sağlamak için bir üçüncü tarafın kullanılması ve, uygunsa, düzenleyici otoriteden onay alınması dâhil olmak üzere bazı temel önlemlere ihtiyaç vardır.

Benzer şekilde, müşterilere ürün ve hizmet sağlarken uyumu temin etme çıktısını elde etme konusunda tamamen iyi niyetli olunsa dahi bir kurum rolleri belirleme noktasında uyanık olmalıdır; ilgili rollerin sorumlulukları hem ürün veya hizmeti sağlarken uyumu temin etmek hem de gözetim ve daha geniş kapsamlı uyum riski yönetimi sunmak üzere tasarlanmalıdır. Temel prensipler olan görevler ayrılığı ve bağımsızlık her daim geçerlidir; ayrıca rollerde uyumsuz faaliyetler tespit edildiğinde ortaya çıkan risklerin hafifletilmesi beklenir.

Aynı şekilde gözetim rollerindeki kişilerde ürün veya hizmet sunumunun temelini teşkil eden risk yönetimi ve kontrol faaliyetlerindeki açıkları ya da eksiklikleri tespit ederken zaman zaman işlerinin kapsamını gözetimi aşarak uygulamayı içerecek şekilde genişletme isteği görülebilir. Bunun tersi de geçerli olabilir; birinci hattakiler, gözetim sağlayan ya da risk yönetimi sorumluluklarına sahip olan rollere aşırı güven duyabilir. Bu durum nesnel gözetimin faydalarını ortadan kaldırabilir. Bu tür durumlarda ilgili açığı ya da eksikliği ve yönetimin bulduğu çözümü belirlemek, eskale etmek ve izlemek gözetim rolünün görevidir. Bu unsurların yerleşik yönetişim rolleri ve sorumluluklarına uygun olarak uyumlaştırılması ve belgelendirilmesi gerekir.