



Yönetim Kurullarının KRY Gözetimi Hakkında Bilmesi Gerekenler

Günümüzün belirsiz iş ortamında, yönetim kurulu üyelerinden risk gözetimi görevlerinin kapsamını genişletmeleri beklenmektedir. Her türden paydaşın, sürekli değişen risk ortamının gözetimi konusunda yönetim kurullarından proaktif rol üstlenmeleri yönünde beklentisi giderek artmaktadır.

Kurumun karşı karşıya kaldıkları riskler arasında jeopolitik çalkantılar, siber güvenlikle ilgili endişeler, yeni çıkan teknolojilerin etkisi, tedarik zinciri sorunları, işgücü açıkları ve şiddetli hava olayları gibi konular yer almaktadır. Harvard Hukuk Fakültesi, Kurumsal Yönetişim Forumunun “Risk Yönetimi ve Yönetim Kurulu (Risk Management and the Board of Directors)” başlıklı makalesine göre, “Kurumsal riski yönetmek, sadece bir şirketin yönetim ekibinin ticari ve operasyonel sorumluluğu değildir — yönetim kurulunun gözetim sorumluluğunun tam ortasında duran bir yönetişimle ilgili ve stratejik konudur.”

Bu makale, mahkemelerin ve düzenleyici kurumların krizler doğduğunda yönetim kurulunun gözetimine ve duruma verdiği yanıtlara odaklandığını eklemektedir. Yönetim kurulu üyelerinin günlük risk yönetim sürecine dâhil olmamaları gerekmektedir; buna rağmen makaleye göre “yönetim kurullarının gözetim rolünün, kurul komitelerinin uygun bir şekilde kullanılması da dâhil olmak üzere anahtar kurumsal risk faktörlerini izleme sürecine aktif katılımı içermesi gerekmektedir.”

Bu sayı, kurumsal risk yönetimi (KRY) gözetimi ve iç denetimin yönetim kurullarına değerli güvence ve tavsiyeler sunma rolü konusunda yönetim kurullarının dikkate alması gereken konuları ele almaktadır.

KRY Olgunluğunun Belirlenmesi

Kurumun KRY olgunluk düzeyine ilişkin gerçekçi bir değerlendirme yönetim kurullarına mevcut durum ve ne tür değişikliklere ihtiyaç duyulabileceği konusunda daha kapsamlı bir anlayış sağlayabilir.. PwC'nin [Yönetim Kurulu Üyesinin KRY Temelleri Kılavuzu \(Director's Guide to ERM Fundamentals\)](#) yayınına göre, yukarıdan bir bakışla, bir kurumun KRY olgunluk aşamaları genel hatlarıyla aşağıda sayılanları içermektedir:

- **Başlangıç aşaması.** Birtakım gayri resmi uygulamalar vardır ancak hiçbir resmi politika veya süreç yoktur. Kurum sorunlara reaksiyon vermektedir.
- **Gelişme aşaması.** Tasarım veya operasyonun bazı yönlerinde etkili olan sistemler ve süreçler vardır. Yaklaşımlar ticari operasyonlarla bir yere kadar uyumludur.
- **Gelişmiş aşama.** Kabul görmüş standartları karşılamak için yerleşik olan ve işleyen resmi çerçeveler ve sistemler vardır.
- **Entegre edilmiş aşama.** Kurum, güncel ve yeni ortaya çıkan risklere karşı eşgüdümlü bir stratejik ve verimli yanıt sağlayan entegre, iş birliğine dayalı ve geliştirilmiş sistemlere ve süreçlere sahiptir.
- **Optimize edilmiş aşama.** Sistemler, süreçler ve kültür stratejik önceliklere iyi düzeyde entegre ve hizalanmış durumdadır. Teknoloji yönetimi, risk yönetimini ve izleme/raporlama faaliyetlerini geliştirmek için kullanılmaktadır.

Kılavuza göre "KRY programı olgunlaştıkça yönetim kurulu, yönetimi nelerin işe yaradığı ve yaramadığı konusunda sorgulayarak sürekli iyileşmeyi teşvik edebilir."

Daha Yakından İnceleme

COSO'nun *Kurumsal Risk Yönetimi – Strateji ve Performansla Bütünleşik Çerçeve (Enterprise Risk Management–Integrating With Strategy and Performance)* yayınındaki [Yönetici Özeti](#), yönetim kurullarının aşağıdakiler de dâhil olmak üzere yönetime KRY hakkında sorabilecekleri sorular önermektedir:

- Tüm yönetim — sadece risk yöneticisi değil — strateji veya ticari kararları belirlemede riskin nasıl ele alındığını ifade edebiliyor mu?
- Yönetim kurumun risk iştahını ve spesifik bir kararı nasıl etkileyebileceğini açıkça ifade edebiliyor mu? COSO, yanıtın kurumun risk alma konusundaki gerçek zihniyetine ilişkin içgörülerini ortaya çıkarabileceğini not etmektedir.
- Üst yönetim sadece risk süreçlerini değil, aynı zamanda kurumun kültürünün risk almasını nasıl sağladığını veya engellediğini tartışabiliyor mu?
- Yönetim risk kültürünü izlemek için hangi bakış açısını kullanır ve bu bakış açısı nasıl değişmiştir? Kurum bünyesinde ve dışında değişimin kaçınılmaz olduğu göz önünde bulundurulduğunda, yönetim kurulu yönetimin risklere uygun ve zamanında yanıt vereceğinden nasıl emin olabilir?

COSO'nun *"Compendium of Examples"* (Örnekler Derlemesi) yayını yönetim hakkında spesifik gözlemler içermektedir. Bu örneklerden biri KRY'nin daha iyi sonuçlar elde edilmesi için karar alma sürecini nasıl iyileştirebileceğini, fırsatları nasıl artırabileceğini ve olumsuz sürprizleri nasıl en aza indirebileceğini ele almaktadır.

Bu örnekte, bir şirket var olan ve arzu edilen KRY yetkinliklerini daha iyi anlamak için adımlar atmıştır. Örneğin, genel müdür ve iç denetçi iş performansı hedefleriyle ilgili kaydedilen ilerlemeyi takip etmek ve riskleri anlamının bu hedeflere ulaşmayı nasıl etkilediğini tespit etmek için operasyon bölümleriyle performans inceleme toplantılarına katılmaktadır. Bu çaba sayesinde genel müdür performansı daha iyi anlayabilir ve iç denetçi daha iyi bir denetim planı geliştirebilir.

En İyi Uygulamalar Rehberi

KRY yaklaşımlarını geliştirmek isteyen kurumlar *COSO'nun Kurumsal Risk Yönetimi – Bütünleşik Çerçeve (COSO's Enterprise Risk Management–Integrated Framework)*, ISO 31000 Risk Yönetimi Standardı ve ABD Ulusal Standartlar ve Teknoloji Enstitüsü Risk Yönetimi Çerçevesi dâhil olmak üzere birden fazla farklı KRY çerçevesinden birini seçebilir. Optro'nun *"Kurumsal Risk Yönetiminin Temelleri (Enterprise Risk Management Fundamentals)"* yayınına göre, bu çerçevelerde tipik olarak beş temel bileşen ortaktır:

- Şirket kültürü, yönetim ve değerler.
- Stratejik planlama, amaçlar ve hedef belirleme.
- Risk yönetimi döngüsü.
- İzleme ve sürekli iyileştirme.
- Şeffaflık, iletişim ve raporlama.

IIA'nın [Üçlü Hat Modeli](#), yönetim kurulunun risk yönetimi gözetimi için en iyi uygulama modellerinden biridir ve anahtar rollerin güçlü yönetimi desteklemek için birlikte nasıl çalıştığını göstermektedir. Bu Model ile hizalı durumda olan [Kurumsal Süreç ve İş Süreci Riskleri Aracı \(Enterprise and Business Process Risks Tool\)](#), riskleri kurumsal ve süreç seviyelerinde tanımlamak, değerlendirmek, yönetmek ve izlemek için pratik ve özelleştirilebilir bir yaklaşım sağlayarak kurumların yapılandırılmış bir KRY programı uygulamasına ve yönetmesine yardımcı olmaktadır.

İç Denetimle İş Birliği

İç denetim, KRY'yi iyileştirme çabasında yönetim kurumları için değerli bir ortak olabilir. Gerçekten de IIA, KRY ile ilgili iç denetim rollerinin gelişmekte olduğunu ve giderek artan sayıda İç Denetim Yöneticisinin (İDY) KRY sorumluluğu bulunduğunu bildirmektedir. IIA Kuzey Amerika İç Denetimin Nabızı (IIA North American Pulse of Internal Audit) çalışmasına göre, İç Denetim Yöneticisi olarak üstlendikleri role ilave olarak KRY programlarından da sorumlu olduklarını bildiren İDY'lerin yüzdesi 2025 yılında %34'e yükselmiştir.

Etkili bir risk yönetimi fonksiyonunu destekleyen temel unsurlardan biri üç hat boyunca iş birliğidir. IIA'nın Üçlü Hat Modeline göre:

- **Birinci hat:** Riskleri yöneten yönetim ve operasyon liderleri.
- **İkinci hat:** Riskleri izleyen ve gözetken risk yönetimi ve uyum fonksiyonları.
- **Üçüncü hat:** Kurumun hedeflerine ulaşmasında bağımsız güvence ve danışmanlık sunan iç denetim.

IIA Hakkında

İç Denetçiler Enstitüsü (IIA), 265.000'den fazla küresel üyeye hizmet veren ve 200.000'den fazla Sertifikalı İç Denetçi (CIA) sertifikası veren kâr amacı gütmeyen uluslararası bir meslek birliğidir. 1941 yılında kurulan IIA, dünya çapında iç denetim mesleğinin standartlar, sertifikalar, eğitim, araştırma ve teknik rehberlik alanlarındaki lideri olarak tanınmaktadır. Daha fazla bilgi için theiia.org adresini ziyaret edin.

IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 ABD

Ücretsiz Abonelik

Ücretsiz abonelik kaydınızı yapmak için theiia.org/Tone adresini ziyaret edin.

Okuyucu Geribildirimi

Sorularınızı/Yorumlarınızı gönderin:
Tone@theiia.org.

Yönetim Kurullarından Beklentiler

Yönetim kurulu için riskle ilişkili temel sorumluluklar aşağıdakileri içermektedir:

- Kurumun risk iştahını ve toleransını belirlemek.
- KRY çerçevesini onaylamak ve izlemek.
- Strateji ve risk maruziyetini hizalı hale getirmek.
- Risk kültürünü ve iç kontrollerin gözetimini sağlamak.
- Yeni ortaya çıkan riskleri ve kritik alanları izlemek.
- Roller ve sorumlulukların net ve açık olmasını sağlamak.

– Diligent, “Risk Yönetiminde Yönetim Kurulu Gözetimini Anlamak: Bugün ve Gelecek”
(Diligent, “Understanding Board Oversight of Risk Management Now and for the Future”)

Baker Tilly, İç Denetim Vakfı ve Wolters Kluwer TeamMate tarafından hazırlanan [Ödün Vermeden İş Birliği: Uygulayıcıların İç Denetim, Risk Yönetimi ve Yönetişim Uygulamaları Hakkındaki Bakış Açıları](#) (Collaboration Without Compromise: Practitioner Perspectives on Internal Audit, Risk Management, and Governance Practices) başlıklı bir rapora göre bu Model “iç denetimin yönetimden bağımsız olmasının, planlama ve çalışmalarını yürütme sürecinde engellerden ve önyargıdan bağımsız olmasını sağlamasına rağmen, bağımsızlığın tam izolasyon anlamına gelmediğini açıkça ortaya koymaktadır.” İç denetimin KRY de dâhil olmak üzere birçok alanda kapsamı genişleyen sorumlulukları, bu fonksiyonun yönetim ve risk yönetimi etkinliği konusunda bağımsız bir değerlendirici olarak üstlendiği rolünü güçlendirme fırsatları sağlamaktadır.

Bu raporda, yanıt verenlerin %90'ının ikinci ve üçüncü hatlar arasındaki koordinasyonun aşağıdakiler de dâhil faydalarını gördüğü not edilmektedir:

- Risk kapsamının iyileştirilmesi.
- Mükerrer çaba ve çalışmaların azaltılması.
- Kurumsal hizalanmanın güçlendirilmesi.
- Yönetim kuruluyla iletişimin iyileştirilmesi ve daha etkili raporlama.

Rapora yanıt verenlerin yüzde otuz dokuzu son beş yılda iç denetim ve risk fonksiyonları arasında daha fazla entegrasyon gördüklerini söylerken %60'ı bu sayının gelecek beş yılda yükseleceğini söylemektedir. Bu rapora göre “Bilgi paylaşımı, eşgüdümlü faaliyetler ve hizalanmış öncelikler yoluyla dikkatli bir şekilde tasarlandığında bu tür yaklaşımlar yönetim kurullarının bilgiye dayanan kararlar alabilmek için güvenilir bilgiler edinmelerine yardımcı olmaktadır.”

Net Bir Bakış

KRY her şeyden önce değişimi fark edip öngörmek ve değişimin kurum için ne anlama geldiğine karar vermektir. COSO'ya göre, değişim konusunda net bir bakış kurumların, örneğin yeni yatırımlar yapmanın mı yoksa çekilmenin mi en iyi yol olduğu gibi zor sorular karşısında mantıklı ve makul kararlar almasını sağlamaktadır. COSO'nun da belirttiği üzere, “Kurumsal risk yönetimi, yönetim kurullarına riski değerlendirmeleri ve dayanıklı bir zihniyet benimsemeleri için doğru çerçeveyi sunmaktadır.”

Teknoloji ve KRY

Yapay zekânın (AI) KRY’de daha geniş bir rol oynama potansiyeli büyüktür. Baker Tilly ve İç Denetim Vakfı tarafından hazırlanan *Geliştirilmiş Kurumsal Risk Yönetimi ve Stratejik Karar Alma (Enhanced Enterprise Risk Management and Strategic Decision-Making)* başlıklı yayına göre, ankete yanıt veren 10 katılımcının birinden daha azı riskleri belirleme sürecine yardımcı olması için yapay zekâyı sık kullandığını bildirmektedir (%6) ya da risk yönetimi faaliyetlerine veri girişi sağlamak için yoğun bir şekilde kullandığını söylemektedir (%3).

Bütünleşik yönetim, risk ve uyum (Governance Risk Control / GRC) platformları KRY süreçlerini destekleyebilir. Baker Tilly ve İç Denetim Vakfı tarafından yapılan KRY Olgunluk Anketi, ankete yanıt veren profesyonellerden sadece %21’inin bu platformları kullandığını ortaya çıkarmıştır. Birçok kurumun KRY programları, örneğin kelime işlemci ve elektronik tablo programları (%59) ya da kurum içi teknoloji araçları (%20) gibi basit araçlara dayanmaktadır.

Geliştirilmiş Kurumsal Risk Yönetimi raporu şöyle uyarmaktadır: “Dijital dönüşümün operasyonların ve yeniden tanımlanan stratejilerin tüm yönlerinde teknolojiye bağımlılığı hızlandırdığı bir çağda, KRY’nin gelişmelere ayak uydurmaması tehlikelidir.”

Bu göz önünde bulundurularak:

- Hizmet olarak yazılım (SaaS) ve GRC araçları, temel KRY programlarını geliştirebilir ve risklerin kurum genelinde daha derinden kavranmasını teşvik edebilir. Bunlar verileri merkezde toplayabilir, iş akışlarını otomatize edebilir ve risklerin belirlenmesini kolaylaştırabilir; bu da karar alma sürecini iyileştirebilir ve risk maruziyetini en aza indirebilir.
- Bu rapor kurumlara kurum bünyesinde güvenli yapay zekâ kullanımının keşfedilmesini ve araştırılmasını, kolaylaştırmalarını ve izlemelerini; ve ayrıca yapay zekâyı KRY süreçlerinde kullanmanın yollarını bulmalarını tavsiye etmektedir.

Rapora göre “İş birliğine dayalı araçlar, harici risk taraması, fonksiyonlar arası entegrasyon ve en son teknolojilerin yardımıyla geleneksel KRY yaklaşımlarını aşmak ve ilerlemek, tüm KRY programlarının hedefi olmalıdır.”

Ankete katılan küresel uzmanlar arasında, %50’si önümüzdeki iki yıl boyunca küresel risk görünümünün çalkantılı ya da fırtınalı olmasını beklerken, bu oran önümüzdeki 10 yıl içinde %57’ye çıkmaktadır.” Sadece %1’i sürecin sakin geçeceğini öngörmektedir.

– Dünya Ekonomi Forumu
Küresel Riskler Raporu 2026 .
(World Economic Forum
Global Risks Report 2026.



Uluslararası İç Denetçiler Enstitüsünün (Institute of Internal Auditors Inc., "IIA") Telif Hakkı © 2013 kesinlikle saklıdır. IIA isminin veya logosunun çoğaltılmasında ABD federal ticari marka tescil sembolü olan ® kullanılacaktır. Bu materyalin hiçbir kısmı IIA tarafından öncesinde yazılı izin verilmeksizin çoğaltılamaz. Değiştirildiği onaylanmadıkça tüm maddi yönlerden orijinali ile aynı olan bu çevirinin yayımlanması için telif hakkı sahibi olan Uluslararası İç Denetçiler Enstitüsü (Institute of Internal Auditors Inc., "IIA") 1035 Greenwood Blvd. Suite 401 Lake Mary, FL 32746, ABD isimli kurumdan izin alınmıştır. Bu belgenin hiçbir kısmı IIA tarafından öncesinde yazılı izin verilmeksizin çoğaltılamaz, bir geri alma sisteminde depolanamaz veya hiçbir formda veya elektronik, mekanik, fotokopi, kaydetme veya başka bir şekilde hiçbir suretle aktarılamaz. İşbu belge Türkiye İç Denetim Enstitüsü tarafından çevrilmiştir. Tone at the Top Nisan 2026 bülteni Sayın Tuğrul Bozbey ve Sayın Alp Buluç (SMMM, CIA, CRMA, CCSA), tarafından gözden geçirilmiş ve "edit" edilmiştir.