

# at the TONE TOP®

Üst yönetime, yönetim kurullarına ve denetim komitelerine yönetimle ilgili konular hakkında kısa ve öz bilgiler sunar.

110. Sayı | Nisan 2022

## Yönetim Kurulları için Risk Konuları

Yönetim kurulları daha riskli bir dünyada nasıl faaliyet göstereceklerini düşünürken iç denetimin ve denetim planlarının nasıl kullanıldığına ilişkin önceliklerin incelenmesi önemlidir. IIA'nın [2022 İç Denetimin Nabızı, Kuzey Amerika \(2022 North American Pulse of Internal Audit\)](#) raporu bir dizi riskin iç denetim yöneticilerinin (İDY'lerin) aklında birinci sırada kalmaya devam ettiğini teyit etmektedir. Aynı zamanda, [Gartner anketi](#)'ne göre yönetim kurullarının çoğunluğu bu yıl risk iştahını yükseltmiştir veya yükseltmeyi ummaktadır. Yerel ve küresel ekonomileri etkileyen son iki yıllık belirsizlik ve sürekli devam eden beklenmedik gelişmeler göz önünde bulundurulduğunda bu durum şaşırtıcı değildir.

Ancak, bu riskler net bir biçimde denetim planlarına yansıtılmıyor olabilir.

Bu sayı, iki önemli alandaki — siber güvenlik ve sürdürülebilirlik konuları — riskleri ele almakta ve kurumların ve yönetim kurullarının endişelerini denetim planlarına dâhil edilmesi için iç denetime nasıl yansıtıklarını incelemektedir.

İç denetimin yönetim kurullarına sunduğu değeri ve yönetim kurullarının bu değerden en iyi şekilde yararlanmalarını nasıl sağlayabileceklerini de ele alacağız.

## Siber Riskler Artıyor

**Nabız anketinde**, İDY'lerin bahsettiği en yüksek riskli ilk üç alanın hepsi teknolojiyle alakalıdır: siber güvenlik, BT ve üçüncü taraf ilişkileri (sıklıkla BT hizmetlerini içerir). Bu üç alandan biri göze çarpmaktadır: siber güvenlik. Nabız verileri, İDY'lerin %85'inin siber güvenliği kurumlarında yüksek veya çok yüksek risk olarak derecelendirdiklerini göstermektedir.

İç denetimin siber güvenlik riskine verdiği önem yönetim kurullarının karşı karşıya olduğu beklentilerle aynı doğrultudadır. PwC'nin Yönetişim İç Görüler Merkezi'ne göre, "Paydaşlar şirketlerin tüketici verilerini korumak ve ayrıca bir ihlâl veya kritik kesintiden hızlı şekilde kurtulmak için ellerinden gelen her şeyi yapmalarını talep etmektedir." [Siber Riskin Gözetilmesi: Yönetim Kurulunun Rolü \(Overseeing Cyber Risk: The Board's Role\)](#) yayınında, veri güvenliği ve mahremiyetin "bu günlerde birden fazla paydaşın yoğun odaklandığı bir alanın" altında yer aldığını not etmiştir. Yöneticiler, bunu akıllarında tutarak "güncel risklerin niteliğini anlamak ve kurumun bu risklere karşı korunmasında stratejik yön sağlamak için yeterli düzeyde siber bilgiye sahip olmak ve bu düzeyi korumak" zorundadırlar.



Siber risk konularının raporlanması odağın arttığı bir alandır. Mart ayında, ABD Menkul Kıymetler ve Borsa Komisyonu (SEC) halka açık şirketlerin [siber güvenlik risk yönetimi, strateji, yönetim ve olay raporlama](#) hakkında yaptıkları açıklamaları artırmak ve standartlaştırmak amaçlarıyla kurullarında değişiklik ve iyileştirmeler teklif etmiştir. Diğerlerinin yanı sıra, bu teklif önemli siber güvenlik olayları hakkındaki güncel raporların yanı sıra rapor edenin siber güvenlik risklerinin tanımlanmasına ve yönetilmesine yönelik politika ve prosedürleri hakkında periyodik açıklamaları, yönetimin bu politika ve prosedürlerin uygulanmasındaki rolünün detaylandırılmasını ve yönetim kurulunun siber güvenlik uzmanlığının ve siber güvenlik riski gözetiminin değerlendirilmesini gerektirecektir.

Bu alanda sürekli devam eden siber tehditler ve yönetim hakkında artan beklentiler ile karşı karşıya olan yönetim kurulları iç denetim de dâhil olmak üzere ulaşabildikleri kaynaklardan en yüksek değeri sağladıklarından emin olmak zorundadırlar. PwC raporunda "Yönetim kurullarının iç denetim gibi gruplardan siber riskler hakkında bilgi alması gereklidir..." demiştir. "Birçok şirket direnç ve yanıt verme de dâhil olmak üzere siber süreç ve kontrolleri gözden geçirmek için iç denetimden faydalanır."

## IIA Hakkında

The Institute of Internal Auditors, Inc. ((Uluslararası İç Denetçiler Enstitüsü), 170'ten fazla ülke ve bölgede 210.000'i aşkın üyesi bulunan küresel bir meslek örgütüdür. IIA, iç denetim mesleğinin baş savunucusu, uluslararası standart koyucusu ve baş araştırmacısı ve eğitmeni olarak hizmet verir.

## IIA

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

## Ücretsiz Abonelik

[www.theiia.org/Tone](http://www.theiia.org/Tone)  
adresini ziyaret ediniz.

## Okuyucu Geri Bildirimi

[Tone@theiia.org](mailto:Tone@theiia.org) adresine soru ve yorumlarınızı gönderebilirsiniz.

## Sürdürülebilirliğin Önemi

**Nabız anketi tarihinde ilk kez**, sürdürülebilirlik ve finansal olmayan raporlama risk seviyeleri, özellikle de halka açık kurumlar için yukarı yönde hareket etmiştir.

Bu ankette, İDY'lerin %40'ı çevre, toplum ve yönetim (ÇTY) başlığı altında yer alan iki alandan birini yüksek veya çok yüksek risk düzeylerinde tanımlamıştır: yönetim ve kültür (%28) ve sürdürülebilirlik/finansal olmayan raporlama (%12). Aynı zamanda, sürdürülebilirliğe ilişkin güvence ihtiyacı hızlı şekilde artmaktadır. ABD Menkul Kıymetler ve Borsa Komisyonu (SEC), yatırımcılara daha tutarlı, karşılaştırılabilir, karar alma konusunda faydalı bilgi vermek ve ihraççılar için daha tekdüze ve açık kurallar sunmak için **iklimle ilişkili yeni şeffaflık ve açıklama kuralları teklif etmiştir**. Aynı zamanda, yeni **Uluslararası Sürdürülebilirlik Standartları Kurulu** ÇTY raporlamasına daha fazla tutarlılık ve güvenilirlik katmayı amaçlamaktadır ve iklimle ilişkili ve genel raporlama standartlarının şu anda yoruma açık olan taslağını hazırlamıştır. Bu gelişmeler iç denetimin doğrulamasını gerektiren yeni uyum konuları, kontrolleri ve süreçlerinin yanı sıra hesaba katılması zorunlu olan çok sayıda yeni riske de işaret etmektedir.

## Denetim Planı Önceliklerinin Ayarlanması

**Yönetim kurulları da bu konuların önemi konusunda açıkça hemfikirdir.** Gartner, 2022 ve 2023 için başlıca stratejik iş önceliklerini tanımlamaları istendiğinde yöneticilerin %32'sinin ÇTY, sağlık ve sürdürülebilirlikten bahsettiğini söylemiştir. Bu, sıralanan öncelikler arasında en yüksek üçüncü yüzdeydi ve önceki yıla kıyasla %100 artmıştı.

Bununla birlikte, Nabız anketine göre endişedeki artış denetim planlarına henüz yansımamıştır. Bu sonuçlar, İDY'lerin hem siber güvenliği hem de ÇTY'yi risk olarak tanımlamış olmalarına rağmen yönetim kurullarının bu risklerin denetim planlarında yeterince temsil edilmesini sağlamak için yeterli desteği sunmuyor olabileceğini göstermektedir. Gerçekten de bu anket İDY'lerin %85'i siber güvenliği kurumlarında yüksek veya çok yüksek risk olarak derecelendirirken siber güvenlik denetimlerinin ortalama denetim planının sadece %11'ini oluşturduğunu ortaya koymuştur. Benzer şekilde, sürdürülebilirliği yüksek veya çok yüksek risk olarak tanımlayan İDY'lerin sayısı artmasına rağmen (2020'de %4 olan oran 2021'de %12'ye yükselmiştir) sürdürülebilirlik denetimleri ortalama denetim planının sadece %1'ini oluşturmaktadır.

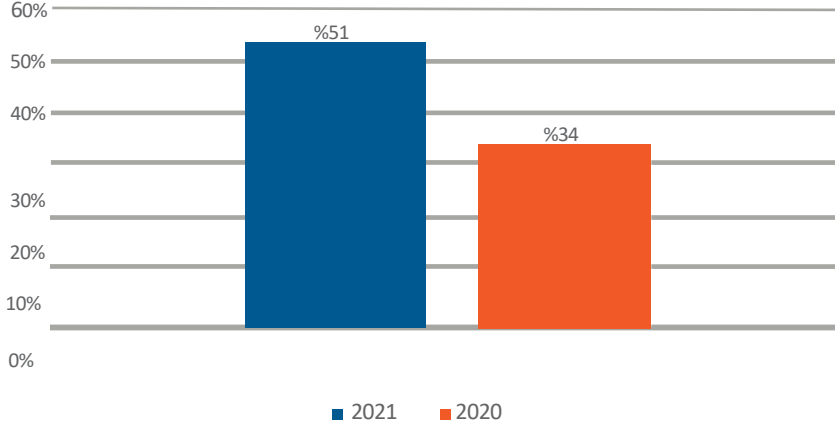
Denetim planlarının yönetim kurulunun endişelerini uygun şekilde yansıtması gereklidir ve siber güvenlik ve ÇTY mutlaka listede olmalıdır. Yönetim kurullarının siber güvenlik, sürdürülebilirlik ve diğer başlıca risklerin denetim planlarına yeterli düzeyde dâhil edilmesini savunması ve desteklemesi gereklidir. İç denetim fonksiyonu bu alanlarda ihtiyaç duyduğu içgörü ve bilgiyi elde edebildiğinde, yönetim kurulu ve yönetimin kurumun karşı karşıya olduğu tehditler hakkında kapsamlı ve objektif bir anlayış kazanmasını sağlamaktadır. Burada, yönetim kurullarının kurumun siber güvenlik ve sürdürülebilirlik/finansal olmayan raporlama konusunda ihtiyaç duyduğu tüm güvenceyi dış denetimin sağladığını varsayması kritik bir hata olacaktır. İç denetimin içeriden sağladığı perspektif, hedefinde de yansıtıldığı üzere, risk ve kontroller hakkında dış denetimin gözden geçirmesinden önce daha derin ve daha geniş bir içgörü ve bağımsız güvence sağlamaktadır.

Bir sonraki bölümde, iç denetim kaynaklarına yapılan yatırımların artırılmasının stratejik faydaları vurgulanacaktır.

## YÖNETİM KURULU ÜYELERİNE SORULAR

- » İç denetimin ÇTY değerlendirme sürecimize ve stratejimize, siber güvenlik değerlendirmemize güncel katılımı nasıldır?
- » Yönetim kurulumuz iç denetimin ÇTY ve siber güvenlik strateji değerlendirme ve geliştirme sürecine sağlayabileceği faydaları anlıyor mu?
- » İç denetime yaptığımız yatırım iç denetimin ÇTY ve siber güvenlik gibi başlıca risk alanlarında perspektif sunmak için ihtiyaç duyduğumuz kaynakları sağlamaya yeterli midir?

## ÇTY/sürdürülebilirlik gözetimini açıklayan yönetim kurulları



**Şekil 1** - Kaynak: [2021 Halka Açık Şirket Yönetim Kurulunda 2021 \(Inside the Public Company Boardroom\)](#), Ulusal Yönetim Kurulu Üyeleri Derneği (National Association of Corporate Directors - NACD)

## Akıllı Yatırımların Önemi

Yönetim kurulları, iç denetim fonksiyonunun ihtiyaç duyduğu insanlara ve kaynaklara sahip olması durumunda iç denetimin sunabileceği tavsiye ve içgörülerden en iyi şekilde yararlanacaktır. Nabız anketinde olgunluğu artırma veya sürdürme konusunda iç denetim fonksiyonuna hangi tür desteğin en çok yardım edeceği sorulduğunda teknoloji araçları (%56) ve daha yetenekli veya yetkin personel istihdam etme becerisi (%52) İDY'lerin ilk tercihleri olmuştur. Altı çizilmelidir ki İDY'lere ilave bütçe fonlarını nasıl harcayacakları sorulduğunda katılımcıların %25'i teknolojinin iyileştirilmesini tercih ettiğini ifade ederken katılımcıların neredeyse yarısı (%48) ilk önceliğinin personel sayısını artırmak olacağını söylemiştir. Ortaya çıkan diğer sorunlar aşağıdakileri içermektedir:

• **Kadro oluşturma.** “Büyük İstifa” dalgası veya gönüllü iş değiştirmede küresel salgının zirveye ulaştığı andan beri gözlemlenen artış iç denetimi vurmuş gibi görünmektedir. Nabız anketine göre, pandemi boyunca bazı iç denetim kadrolarındaki personel sayısı kesintilerden sonra normale dönerken bütçe ve personel düzeyleri artmamaktadır. Bu durum, geleceğe yönelik özgüvenin azalması veya belirsizliğin artmasından ya da yetenek bulmanın zor olmasından kaynaklanıyor olabilir. Her iki durumda da yüksek düzeyde becerili iç denetçilerden oluşan yeterli bir ekip, kurumun yatırımına karşılık en iyi değeri sağlayabilir.

• **Teknoloji.** Nabız anketinde, İDY'lere ilave fonları teknoloji bütçelerinde nasıl kullanacakları sorulduğunda katılımcıların %68'i bu fonları veri analizi yazılımına harcayacaklarını söylemiştir. Robotik süreç otomasyon yazılımı (%34) ve yapay zekâ (%31) diğer seçenekler arasındadır. Bu durum, Dünya Ekonomik Forumunun (World Economic Forum, WEF) en yeni bulgularıyla tutarlıdır; Dünya Ekonomik Forumunun [Dördüncü Sanayi Devrimi Teknolojileri Şirketlerin COVID Krizinde Hayatta Kalmasına Nasıl Yardımcı Oldu? \(How Fourth Industrial Revolution Tech Helped Companies Survive the COVID Crisis?\)](#) başlıklı raporuna göre, çok çeşitli dijital ve ilişkili “dördüncü sanayi devrimi” teknolojileri “esnek ve dirençli tedarik zincirlerinin temel itici gücü olarak ortaya çıkmış ve şirketlerin küresel salgından sağ çıkmasına yardımcı olmuştur”. Dünya Ekonomik Forumu (WEF), “Bu teknolojilere yatırım yapan şirketlerin tasarruf yapabildiğini ve gelecek zorluklarla baş etmede çevikliğini artırdığını,” belirtmiştir. Yönetim kurullarının, ileri teknoloji kaynakların iç denetimin gerçek zamanlı, kapsamlı analiz sunmasını ve çevikliğini artırmasını sağlayabileceğinin farkında olmaları gereklidir.

Ekipleri son 12 ayda küçülen Nabız anketi katılımcıları hem bütçelerin hem de kadroların neredeyse COVID-19 öncesi düzeylere geri döndüğünü söylemiştir. Bununla birlikte, küresel salgın öncesi düzeylerin üzerinde bütçe artışları rapor eden az sayıda kişi vardı. Hatta bazıları 2021 yılında 2020 yılından daha düşük yüzdede büyüme görmüştü.

## İç Denetim Fonksiyonundan Faydalanma

İç denetim küresel salgını iyi yönetmiştir. Bununla birlikte, iç denetim ekiplerinin ve çalıştıkları kurumların karşı karşıya kaldıkları zorluklar göz önünde bulundurulduğunda, yönetim kurullarının iç denetim bütçeleri, denetim planı öncelikleri ve kadro oluşturma ile ilgili kısıtlamalara karşı tetikte olmaları gereklidir. En nihayetinde, iç denetim fonksiyonundan ve onun sağladığı bağımsız güvence ve iç görülerden en iyi şekilde faydalanmak yönetim kurulunun sorumluluğudur. İç denetim, yönetim kurulu için güçlü bir araçtır ve yöneticilerin kurumlarını halihazırda mevcut olan ve yeni ortaya çıkan çok çeşitli riske karşı korumalarına yardımcı olabilir.



### Hızlı Anket Sorusu

Yönetim kurulu iç denetim planının kurumun risk önceliklerini yansıtıp yansıtmadığının farkında mıdır?

- Evet  
 Hayır

Cevaplamak ve diğer cevapları da görmek için [www.theiia.org/Tone](http://www.theiia.org/Tone) sayfasını ziyaret ediniz.



Copyright © 2022 by The Institute of Internal Auditors, Inc. Tüm hakları saklıdır.

"Uluslararası İç Denetçiler Enstitüsünün (Institute of Internal AuditorsInc., "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 AuditorsInc., "IIA") 1035 Greenwood Blvd. Suite 149 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 2022 bülteni Sayın Tuğrul Bozbey ve Sayın Alp Buluç (SMMM, CIA, CRMA, CCSA), tarafından gözden geçirilmiş ve "edit" edilmiştir.