TONE at the TOP®

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

**107. Sayı | Ekim 2021**

# *OnRisk 2022*: Kilit Önemdeki Risklerle İlgili Güncel İçgörüler

**Covid 19 salgını** ve yol açtığı pek çok aksaklık, kurumlar için, karşı karşıya oldukları çok çeşitli riskleri ve belirsizlikleri anlama gereksinimi konusunda çok önemli bir uyarı işareti oldu. Uluslararası İç Denetçiler Enstitüsü'ne (IIA) ait *OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk ("OnRisk 2022: Riski Anlama, Hizalandırma ve Eniyileme Rehberi")* başlıklı bir rapor, şu anda kurum için en ilgili ve anlamlı riskler hakkındaki uyum durumlarını belirlemek (3. sayfadaki kutuya bakınız) ve bu risklerle en iyi nasıl başa çıkılacağına dair bakış açılarını öğrenmek amacıyla kurumsal yönetişim bünyesindeki başlıca paydaşlardan – yönetim kurulu, icrai yönetim ve iç denetim yöneticileri (İDY) – alınan girdileri bir araya toplamıştır. Tecrübeli bir Genel Müdür (Chief Executive Officer-CEO) ve kamu şirketlerinde ve özel şirketlerde yönetim kurulu üyeliği görevinde bulunmuş olan Cristina Steele "Yönetim kurulları, bu raporu kurumlarında hangi sorunların veya kaygıların söz konusu olduğu ve hangi alanların daha fazla ilgi ve dikkat gerektirebileceği konusunda açık bir diyalog başlatmak için kullanabilirler" ifadelerini kullanmıştır.

Raporun en önemli gözlemlerine bir göz atmak kurumları bekleyen tehditleri göz önüne sermekle yetinmez, ayrıca, kurumların bunları çözme kabiliyetlerini engelleyebilecek bariyerleri de gösterebilir.

## Kilit Önemdeki Alanlarda Kayda Değer Farklılıklar

***OnRisk 2022*** anket katılımcılarının, birtakım risklerin kurumları için ne kadar ilgili ve anlamlı olduğuna inanmaları ve kurumlarının söz konusu riskleri ele alacağından ve çözeceğinden ne kadar emin oldukları arasındaki önemli farklar da dâhil olmak üzere **birkaç kilit gözlem sunmaktadır** (4. sayfadaki grafiğe bakınız)**.** Bu, kişisel bilgi, kurumsal kabiliyet ve kapasite ve her bir risk için ilgililik ve anlamlılık konusunda katılımcıların verdikleri puanların analiz edilmesiyle belirlenmiştir. Puanlar her bir risk alanında en yüksek puanları (7 puanlık bir ölçekte 6 veya 7 puan) veren katılımcıların yüzdesine dayanmaktadır.


Kilit önemdeki gözlemler aşağıda sayılanları kapsar:

**Risk yönetimi, kurumların bu görev için yeterli ve uygun kabiliyetlere ve kapasiteye sahip olmasını gerektirir.** Siber güvenlik her üç katılımcı grubu tarafından da kurumlar için en önemli ilgili risk olarak tanımlanmasına karşın, *OnRisk 2022* raporu, endişe verici bir şekilde, siber güvenliğin kurumları için son derece ilgili ve anlamlı olduğuna inananlar (%87) ile kurumlarının bu alanda güçlü ve sağlam bir kapasitede ve yeterlilikte olduğunu düşünenler (%42) arasında 45 puanlık bir fark olduğunu ortaya çıkarmıştır.
Başka risk alanlarında da önemli ve anlamlı İlgililik – Kapasite farkları olduğu belirlenmiştir. Salgın, vasıflı çalışanları yönetmenin değerinin altını çizmişse de, Yetenek Yönetimi için 46 puanlık bir İlgililik-Kapasite farkı olduğu görülmüştür. Katılımcıların önümüzdeki üç ilâ beş yıl içinde ilgililiğinin ve öneminin artmasını beklediği ve aralarında Kültür (36 puan), Yıkıcı İnovasyonlar (34 puan) ve Ekonomik ve Siyasal İstikrarsızlığın da (32 puan) bulunduğu birtakım risklerin hepsinin İlgililik-Kapasite farkları büyüktür.

**Birkaç risk alanında risk ilgililiği ve kurumsal kapasite ve yeterlilik konusunda üst düzey yöneticiler, yönetim kurulu üyeleri ve iç denetim yöneticilerinden alınan cevaplar arasında anlamlı farklılıklar tespit edilmiştir.** Bu durum rahatsız edicidir, çünkü paydaşların kurumsal kapasite ve yeterlilik ile risk ilgililiği konusundaki görüşleri birbiriyle uyumlu olduğunda sağlam ve güçlü bir risk yönetimini kotarmak daha kolaydır.

## IIA Hakkında

The Institute of Internal Auditors, Inc. (IIA), 170'ten fazla ülke ve bölgede 200.000'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 149
Lake Mary, FL 32746, ABD

## Ücretsiz Abonelik

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

## Okuyucu Geri Bildirimi

Sorularınızı/yorumlarınızı Tone@theiia.org adresine gönderiniz.

Risklerin ilgililiği söz konusu olduğunda, üst düzey yöneticilere kıyasla daha fazla sayıda yönetim kurulu üyesi Yıkıcı İnovasyonu ilgililik düzeyi yüksek bir risk olarak tanımlamıştır (%50'ye kıyasla %77) ki bu da, ankete katılan üç grup içerisinde risk ilgililiği puanları arasındaki en yüksek fark olmuştur. Siber güvenlik mevzusunda ise, katılımcılar yalnızca kurumlarına kapasite ve yeterlilik bahsinde düşük puanlar (%42) vermekle kalmamışlar, aynı zamanda bu riskin ilgililik düzeyi konusunda da tam olarak hemfikir olmadıklarını göstermişlerdir. İç denetim yöneticilerinin (İDY) (%97), yönetim kurulu üyelerine (%87) veya yönetime (%77) nazaran bu sorunu yüksek düzeyde ilgili bir risk olarak görme ihtimali daha yüksek bulunmuştur. Bunun yanı sıra, yönetim kurulları (%60) ve üst düzey yöneticiler (%67) ile karşılaştırıldıklarında İDY'ler (%77) Tedarikçi ve Satıcı Yönetimi konusundaki risklerin daha ilgili ve anlamlı olduğunu ifade etmişlerdir ve İDY'lerin (%80) Ekonomik ve Siyasi İstikrarsızlık konusunda kaygılanma olasılıklarının yönetim kurulu üyelerine (%63) veya üst yönetime (%67) kıyasla daha fazla olduğu belirlenmiştir.

Birtakım risk alanlarında kurumsal kapasite ve yeterlilikle ilgili puanlar konusunda üst düzey yöneticiler kurumlarından daha fazla emin olma eğilimi göstermişlerdir. Buna istisna teşkil eden durumlardan birisi Yıkıcı İnovasyon olmuştur, zira bu başlıkta %43 olan yönetim kurulu üyeleri oranına göre üst yöneticilerin yalnızca %20'si kurumlarının kapasite ve yeterliliğini yüksek olarak tanımlamışlardır ve bu oran da herhangi bir konudaki kapasite ve yeterlilik için verilen en düşük puan olmuştur. Bu, kapasite ve yeterlilik bahsinde bu iki grup arasındaki en büyük ayrışmadır.

Kurumun, Yetenek Yönetimi ve Çevresel Sürdürülebilirlik (her biri için 20 puanlık bir fark bulunmuştur) ve Kurumsal Yönetişim (13 puan) ile ilişkili riskleri yönetme kapasitesi ve yeterliliği söz konusu olduğunda, yönetim kurullarının güveni üst düzey yöneticilere kıyasla daha az olmuştur. Her durumda, yönetim kurulları İDY'ler ile daha yakın bir uyum içinde olmuşlardır.

**ÇTS konuları hakkındaki algılarda farklılıklar saptanmıştır.** Rapor üç tane ilgili risk alanını gözler önüne sermiştir: Çevresel Sürdürülebilirlik, Toplumsal Sürdürülebilirlik ve Kurumsal Yönetişim. Anketin katılımcıları bu üç alan içinden Kurumsal Yönetişimi diğer ikisinden çok daha ilgili ve anlamlı görmüşlerdir. Yatırımcılar ve düzenleyici otoriteler arasında bu risk alanına yönelik giderek artan ilgi düşünüldüğünde, yönetim kurulları kendi kurumlarının içinde bu alandaki tüm sorunların anlaşıldığını ve yeterli düzeyde ele alındığını temin etmek için ÇTS risk yönetimine yönelik bir iç denetim değerlendirmesi yapılmasını talep edebilirler.

### Yeni Risk Yönetimi Fırsatları

**Salgın,** mali riskler ve uyum ile ilgili risklerin dışındaki alanlarda da güvence alınmasının gerekliliği hakkındaki **farkındalığı artırmıştır.** Dış denetimler çoğunlukla bu bahsedilen alanlara (mali riskler ve uyum) odaklanır, ancak iç denetim yönetim kurulu ve icrai yönetimin desteğiyle daha geniş bir görev yetkisine ve tanımına sahip olabilir. "Bu görev yetkisi, jeopolitik riskler, operasyonel riskler, mali riskler, uyumla ilgili riskler ve hukuki ve kültürel riskler de dâhil olmak üzere çok geniş bir yelpazedeki riskleri kapsar," diye belirtiyor Steele. Bu salgın ışığında, *OnRisk 2022* katılımcıları operasyonel ve kurumsal riskler ile ilgili daha fazla güvence alma fırsatlarına ilgi duyduklarını ifade etmişlerdir ve riskleri proaktif şekilde ele alma ihtiyacına yönelik olarak yeni bir idrak ve takdir kapasitesi göstermişlerdir.

# YÖNETİM KURULU ÜYELERİNE YÖNELİK SORULAR

- Kurumunuzu uyumla ilgili riskler ve mali riskler dışında hangi riskler beklemektedir?
- Kurumumuz Covid-19 salgınının açığa çıkardığı yeni zorlukları ele alan bir kurumsal risk değerlendirmesi yaptı mı?
- Kurumumuz karşı karşıya kaldığı risklerle başa çıkacak kapasiteye sahip midir?
- Yönetim kurulumuz iyi yönetişim için ihtiyaç duyduğu kurumsal risk yönetimi bakış açısını ediniyor mu?

Steele, iç denetimin kuruma makro düzeyde ve kuş bakışı bakma imkânının olduğunu belirtmiştir. "Yukarıdan yolu ve etrafı görebilir" demiştir. Buna ek olarak, "Dünyanın veriye boğulduğu bir dönemde yönetim kurulu odasına hangi bilgilerin gelmesi gerektiği konusunda içgörüler sunabilir". Tüm paydaşlar risk yönetimi kaynaklarını bu kaynaklara en çok ihtiyaç duyulan alanlara odaklayacak stratejileri belirlemek amacıyla aynı gerçeklere dayalı verilerle çalışabilirler.

Steele, denetim planının kurumun stratejik inisiyatiflerini yansıtmasını sağlamak için İDY'nin de üst düzey yöneticilerle aynı masada yer almasını tavsiye etmiştir. İç denetim hizmetlerinin daha fazla ve daha geniş bir alanda kullanılması özellikle salgın nedeniyle daha fazla dikkati cezbeden Siber Güvenlik, Yetenek Yönetimi ve Kurumsal Yönetişim gibi yüksek düzeyde ilgili risk alanlarında yönetim kuruluna değer katabilir.

## Yönetim Kurulu Üyeleri için İzlenecek Diğer Adımlar

**Salgın, kurumları** risk yönetimi sorunlarına daha detaylı ve kapsamlı bakmaya ve iyileştirilebilecek alanları aramaya **zorladı.** Risklerin etkilerinin etki aralığı ve yoğunluğu arttıkça, iç denetim hizmetleri karar almaya yönelik bağımsız ve tarafsız güvence sunarak tehditleri tespit etmeye ve hafifletmeye yönelik devam eden çabalarda kilit bir partner işlevi görebilir. Yönetim kurulları gelecekteki adımlarını düşünürken, *OnRisk 2022, pek çok* şirketi pençesine alabilecek sorun alanlarına yönelik bir yol haritası ve yönetim kurullarının kendi İlgililik-Kapasite farklarını dikkate almak için kullanabilecekleri bir model sunmaktadır.

### *ONRISK 2022*'NİN EN ÖNEMLİ RİSKLERİ

On iki risk, 2022 yılında kurumları etkileyebilecek olası tehditlere ilişkin geniş ve kapsamlı bir listeden seçilmiştir ve yönetim kurulu üyeleri, icrai yönetim ve İDY'lerle derinlemesine görüşmeler yoluyla incelenmiştir. Burada ilgili kaygıları özetleyen bir soruyla birlikte *OnRisk 2022* katılımcılarının verdikleri puanlara göre birleşik risk ilgililiği sırasıyla gösterilmektedir.

**Siber Güvenlik:** Kurumlar operasyonlarını kesintiye uğratabilecek ve itibarlarına zarar verebilecek siber tehditleri yönetmeye hazır mıdır?

**Yetenek Yönetimi:** Uzaktan yürütülen çalışmalara ve dinamik istihdam koşullarına geçiş düşünüldüğünde, kurumlar hedeflerine ulaşmak için ihtiyaç duydukları yeteneği tespit etme, elde etme, eğitme ve elde tutma zorluklarıyla yüzleşebilirler mi?

**Kurumsal Yönetişim:** Yönetişim — kuralları, uygulamaları, süreçleri ve kontrolleri — bu hedeflere ulaşılmasını kolaylaştırıyor mu ya da engelliyor mu?

**Veri Mahremiyeti:** Giderek daha karmaşık ve dinamik bir hal alan uluslararası düzenleyici ortam ve koşullar ışığında, kurum, hassas verileri yeteri kadar koruyor mu ve tüm ilgili güncel mevzuata uyumu temin ediyor mu?

**Kültür:** Uzaktan ve esnek çalışma düzenlemelerinin artışı düşünüldüğünde, kurum, tüm çalışanlarda arzu edilen davranışları güdüleyen tonu, teşvikleri ve eylemleri anlıyor, izliyor ve yönetiyor mu?

**Ekonomik ve Siyasi İstikrarsızlık**: Kurum, dinamik ve potansiyel olarak istikrarsız ve değişken bir ekonomik ve siyasi ortamda ilgili zorlukları ve belirsizlikleri izliyor ve ele alıyor mu?

**Düzenleyici Ortamdaki Değişiklik:** Kurum sıkı ve katı düzenlemelere tâbi olsun olmasın dinamik ve belirsiz bir düzenleyici ortamdaki riskleri ele almaya ve çözmeye hazırlıklı mıdır?

**Tedarikçi ve Satıcı Yönetimi:** Kurum, faydalı ve etkili üçüncü taraf ilişkileri geliştirmek ve bu ilişkileri izlemek için ne derece donanımlıdır?

**Yıkıcı İnovasyon:** Kurum, inovasyonun sektörde yol açacağı köklü değişime ve yıkıma ayak uydurabilir mi ve/veya bundan faydalanabilir mi?

**Toplumsal Sürdürülebilirlik:** Kurum, eylemlerinin bireyler ve topluluklar üzerindeki doğrudan ve dolaylı etkilerini anlayabilir ve yönetebilir mi?

**Tedarik Zincirinde Köklü Değişimler:** Kurum, mevcut ve gelecekteki tedarik zinciri köklü değişimine uyum sağlamak için gereken esnekliği kendi bünyesinde oluşturmuş mudur?

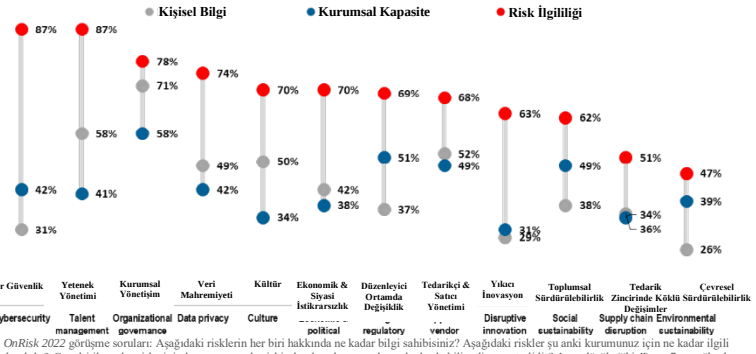
**Çevresel Sürdürülebilirlik:** Kurum, bıraktığı çevresel etkiler hakkında güvenilir ölçümler yapabilir, değerlendirmelerde bulunabilir ve doğru raporlama yapabilir mi?

# Metodoloji: *OnRisk* Yaklaşımı

***OnRisk* metodolojisinde** 90 farklı kurumdan 30 yönetim kurulu üyesi, 30 üst düzey yönetici ve 30 İDY ile yapılan nitel görüşmeler kullanılmaktadır. Bu araştırma, kurumların karşı karşıya oldukları risklere sağlam bir bakış sağlar ve risk yönetimi liderlerinden alınan yanıtlara göre hem objektif veri analizine hem de sübjektif içgörülere imkân tanır. Bu görüşmeler kapsamında, katılımcılardan üç alanda 12 kilit riski değerlendirmeleri istenmiştir: Her bir riske ilişkin kişisel bilgileri, kurumlarının her bir riski ele alma ve çözme kapasitesine ilişkin algıları ve her bir riskin kurumları açısından ilgililiği ve anlamlılığı konusundaki görüşleri.

**Risk Alanı Başına Düşen Ortalama Puanlar**

1 ilâ 7 ölçeğinde 6 veya 7 puan verenlerin yüzdeleri




*Not: OnRisk 2022* görüşme soruları: Aşağıdaki risklerin her biri hakkında ne kadar bilgi sahibisiniz? Aşağıdaki riskler şu anki kurumunuz için ne kadar ilgili ve anlamlıdır? Genel itibarıyla, şirketiniz kurum çapında riski ele alma konusunda ne kadar kabiliyetli ve yeterlidir? 1 en düşük ("hiç") ve 7 en yüksek ("aşırı") olmak üzere, anket katılımcıları 1 ile 7 aralığındaki bir ölçekte bir puan seçebililer. Katılımcıların toplam sayısı n = 90.

*Note: OnRisk 2022* interview questions: How knowledgeable are you about each of the following risks? How relevant are each of the following risks to your current organization? Overall, how capable is your company when it comes to handling enterprisewide risk? Respondents could choose a rating from a scale of 1 to 7, with 1 being the lowest ("not at all") and 7 being the highest ("extremely"). All respondents. *n* = 90.

## Hızlı Anket Sorusu

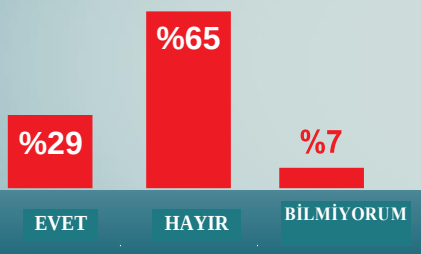
**Yönetim kurulumuz, karşı karşıya olduğumuz risklerin ilgililiği konusunda icrai yönetimin görüşleriyle uyum içindedir:**

- ❑ Her zaman
- ❑ Çoğunlukla
- ❑ Nadiren
- ❑ Asla
- ❑ Bilmiyorum

Soruyu cevaplamak ve başkalarının bu soruya nasıl cevap verdiğini öğrenmek için www.theiia.org/Tone adresini ziyaret ediniz.

## HIZLI ANKET SONUÇLARI

Yönetim kurulunuzda siber güvenlik uzmanı bir üye var mı?




Kaynak: Tone at the Top Ağustos 2021 anketi.