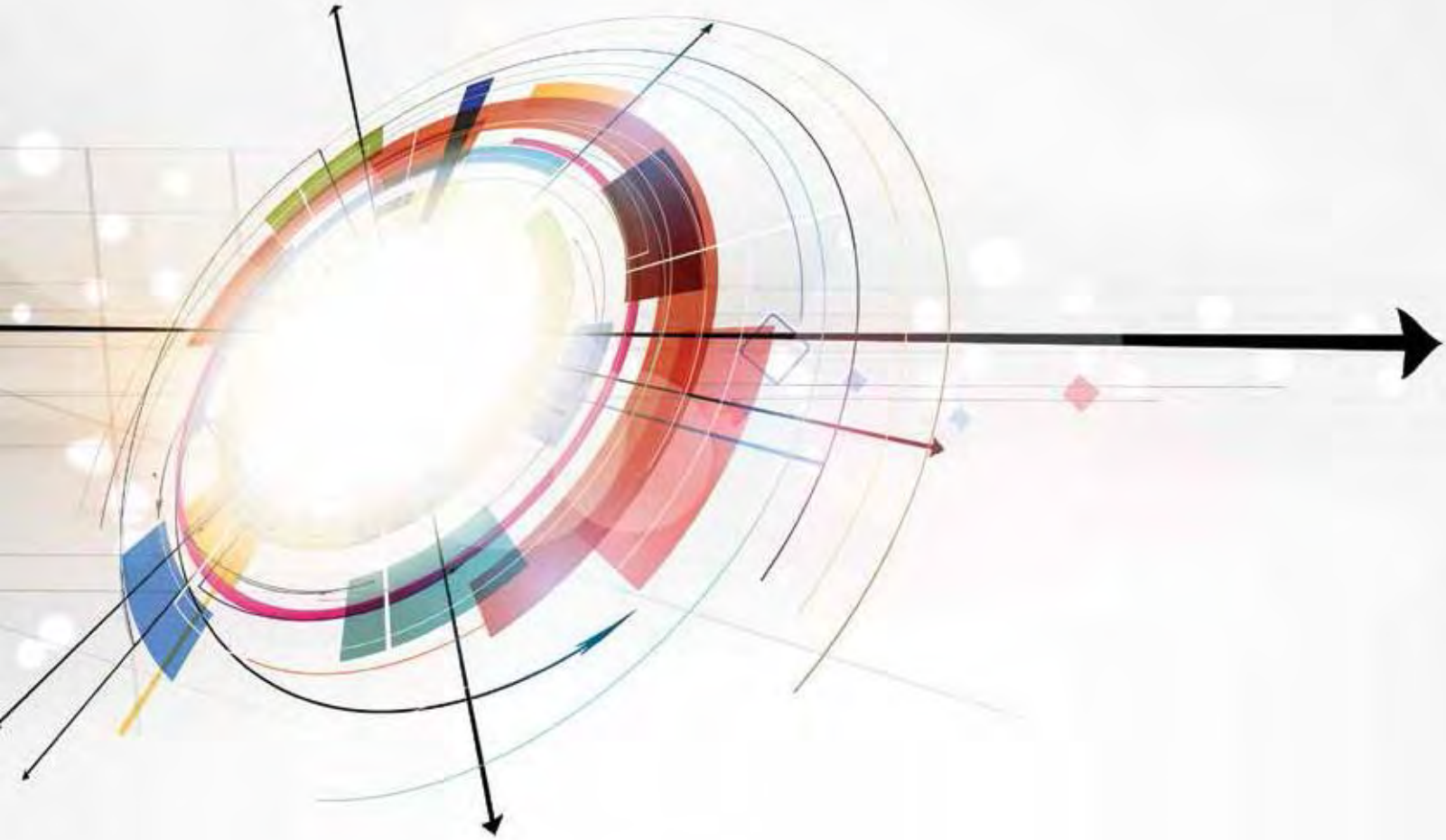

# GLOBAL BAKIŞ AÇILARI VE ANLAYIŞLAR

## 2018 Global Risk Raporu

İç Denetim Yöneticilerinin Karşılaştıkları En Büyük Riskler

The Institute of Internal Auditors

## Eski Sayılar

Global Perspektifler ve Anlayışlar yayınının eski sayılarına ulaşmak için şu adresi ziyaret ediniz: www.theiia.org/gpi.

## Okuyucu Geribildirimi

Soru veya görüşlerinizi şu adrese gönderiniz: globalperspectives@theiia.org.

## İçindekiler Tablosu

# Giriş

2018'i — yeni bir yılı ve bu yeni yılla birlikte, yeni kanunları, yönetmelikleri, fikirleri, görüşleri, teknolojiyi ve riskleri sunmak. Günümüzün iş ortamı, geçmişte olduğundan önemli oranda farklı ve artık daha karmaşık ve daha fazla bağlantılı… Kuruluşlar yeni ve bilinmeyen risklerle, fakat aynı zamanda da yeni ve hiç kullanılmamış fırsatlarla karşı karşıyalar. Önümüzdeki yılın getireceği yeni fırsatlar ve mevcut bir dizi potansiyel zorluk ve riskler dikkate alındığında – bu risklerin bazıları beklenen bazıları da tamamen 2018'e özgüdür –, denetim planlarının da bozucu ve yıkıcı nitelikte olaylar gerçekleştikçe değişecek çerçeveler olarak görülmeleri gerekir.

Kurumun tamamını kapsayan görüş alanıyla, iç denetim birimi, risk yönetimi, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve iyileştirmek için sistemli ve disiplinli bir yaklaşım getirerek kurumun hedef ve amaçlarına ulaşmasına yardımcı olur. Düzenleyici otoriteler ve denetim komiteleri, risk yönetimi çabalarının zorlu rakiplerin, gelişen teknolojilerin, değişen piyasa eğilimlerinin ve mevzuattaki gelişmelerin yarattığı tehdit ve tehlikelerle başa çıkabilmek için yeterli olmasını isterler ve bu konuda güvence almaya gereksinim duyarlar (İç Denetimin Gelecek Eğilimleri: Yeni Ortaya Çıkan Eğilimler ve Yüksek Etkili Odak Alanlarına bakınız).

İç denetimin tüm endüstrilere ve sektörlere daha fazla değer katan ve daha stratejik destek sağlamaları gereksinimi mevcut olduğu için, denetçilerin yaptıkları işlerin başta stratejik ve operasyonel riskler olmak üzere tüm önemli risklerle uyumlu olmasını sağlamaları gerekir. İç denetim faaliyeti, dinamik risk ortamına cevap verebilmeli ve uyarlanabilmelidir.

Riskler değişir ve en iyi hazırlanan denetim planlarının bile, kurumun her seviyesinde yeni riskler ortaya çıktıkça esnek olması ve değişime açık olması gerekir. Bu makalede, iç denetim yöneticilerinin (CAE) karşılaştıkları ve IIA global bağlı şirketlerinin belirlediği en büyük beş risk (iç denetimin veya kurumun riskleri) tartışılmaktadır. Bu riskler şunlardır: Yetenek Yönetimi, Veri Analitiği, Siber, Mevzuat ve Piyasa Bozulmalarına Cevap Verme.

# Yetenek Yönetimi

Yetenek yönetimi, iç denetim yöneticileri ve iç denetim profesyonelleri için her zaman bir ilgi alanı ve kaygı sebebidir. Son birkaç yıldır, CAE'ler yeni kadroları doldurmak ve yeni ve mevcut riskleri karşılamak için gereken becerilere sahip adaylar bulmaya kafa patlatmaktadırlar. İç denetimin artan gereksinimlerini karşılayacak becerilere sahip adayların havuzunun sınırlı bir havuz olduğu açıktır. Ek olarak, çalışma ortamını, destek ve takdir konusunda daha büyük ve farklı beklentileri bulunan, akıllarında spesifik bir çalışma ortamı bulunan ve daha esnek çalışma programlarını tercih eden y kuşağı işgücünün kendine özgü özniteliklerine uyarlama zorunluluğu da vardır (4 İç Denetim Yetenek Boşluğunu Kapatmak İçin Stratejilere bakınız).

"İç denetim geleceğe hazırlanmak istiyorsa, yerine getirmesi gereken beş temel şarttan biri de çevikliktir. Yeni ortaya çıkan riskleri tanıyabilmek ve karşılayabilmek için ve riskleri kesintisiz değerlendirebilmek için yeterince çevik olmamız ve denetim işimizin kapsama alanını da buna göre uyarlamamız gerekmektedir. Ve yeteneklerimizdeki açıkları ve boşluklara anlayabilmek ve bunları hızla kapatabilmek için de yeterince çevik olmamız gerekir. Gelecekte ancak ve sadece dinamik bir yetenek yönetim stratejisi bulunan iç denetim departmanları başarılı olacaklardır."

Richard Chambers,
IIA Başkanı ve CEO

2015 yılında, global IIA anketine cevap verenlerin yüzde 40'dan fazlası için *yetenekleri cezbetmek ve elde tutmak* yüksek ya da kritik bir öncelikti ve ankete cevap verenlerin yarıdan fazlası *mevcut bilgi açığını* becerikli denetçiler havuzunun sınırlı olmasına atfetmişlerdi. Yine 2017 yılında, bir IIA Denetim Yönetim Merkezi® (AEC®) anketine cevaben, yaklaşık 200 CAE'nin açık çoğunluğu (yüzde 79) yetenek yönetimini iç denetim mesleği için çok öncelikli / çok önemli bir risk olarak tanımladılar ve yorumladılar. KPMG'ye göre, yönetim kurulları, yeteneği — ya da yeteneğin yokluğunu — bir *kurumsal risk* olarak görmektedirler. Kurumlar daha fazla globalleştikçe, kurumları destekleyen işgücü de evrim göstermeye devam etmektedir; yetenek yönetiminin bu kadar kritik olmasının sebebi de budur. Global yetenek eksikliğinin potansiyel etkisi ve yansımaları arasında, liderlik becerilerinin sürdürülememesi de bulunur, çünkü gelecek liderleri sağlayan sağlıklı bir boru hattı artık mevcut değildir ve iş stratejilerinin sonuçları kuşkuludur, çünkü adaylar bu kritik rol ve görevleri üstlenebilecek kapasitede değildirler. Kurumlar, yeni nesilleri yetiştiremediklerini ve yönlendiremediklerini ve üst düzey veya uzmanlaşmış yetenekleri ellerinde tutamadıklarını ve bu sebeple, entelektüel sermayeyi ve rekabet avantajlarını kaybettiklerini görmektedirler. Üstelik ve sürekli olarak, yaşlanan ve emekliye ayrılan popülasyon beceri kıtlığını da tetiklemektedir (Yönetim Kurulu Soruları: Yetenek Yönetimi mi yoksa Yetenek Riski mi? bölümüne bakınız).

Üstüne üstlük, - veri analitiği, üçüncü taraf yönetimi, siber güvenlik, sürdürülebilirlik ve politik ve diğer belirsizlikler gibi – yeni ortaya çıkan risklerden ötürü, kurumlar iç denetçilerinden artık çok daha fazla şey beklemektedirler. İç denetimin odak noktasının geleneksel finansal ve uyum temelli görevlerle ve konularla sınırlı olduğu günler artık geride kalmıştır.

İç denetim birimi insan kaynakları işinde olmamasına rağmen, yönetimin bu riskleri *iyi yönetip yönetmediğini ve ne kadar iyi yönettiğini de* değerlendirmesi gerekmektedir. Günümüzün kurumları, entegre risk gözetimi ve değer yaratma da dâhil denetim konusunda daha bütüncül bir yaklaşıma gereksinim duymakta ve iç denetçilerinden de böyle bütüncül bir yaklaşım benimsemelerini beklemektedirler. Bu sebeple, iç denetim için yetenek, beceri ve kuvvet arayışı çok daha rekabetçi bir hal almış bulunmaktadır.

Yeterli becerilerle donatılmamış bir iç denetim birimi, teknoloji, jeopolitik, ekonomi, gelişmekte olan kurumsal raporlama, kültür ve yerli ve global mevzuat gibi, geleneksel olmayan spesifik riskleri ihmal etme veya yeterince denetlememe riskine çok açık ve yatkın olur. İnsan Kaynakları Yönetimi İçin Toplum isimli bölüme göre, iç denetim biriminin geleneksel finans, operasyonel ve genel BT beceri setlerinin ötesine geçme ve daha büyük resme odaklanma kabiliyeti yaşamsal öneme sahiptir.

Yetkinlik ve uzmanlıklarını ileri görüşlü bir şekilde genişleten ve işlerini kurumun risk profili hakkında daha kapsamlı bir bilgi ve anlayış temeline dayandıran bir iç denetim birimi, kuruma hizmet etmeye daha iyi hazırlanmış demektir. Bu hazırlığın bir parçası da, spesifik alanlarda uzmanlığın ya da sektöre-özgü bilgi birikiminin yanı sıra, ileri eleştirel-düşünme kabiliyetlerine ve keskin bir iş zekasına sahip insanları kuruma kazandırmaktır. Geleneksel olmayan ve yeni gelişen riskler denetim ortamı ve evrenini de etkileyeceklerdir; bu sebeple, iç denetim biriminin gereken tüm yeni becerilere ulaşabilmesi ve mevcut becerilerinin genişliğini ve derinliğini artırması önemlidir. CAE'lerin denetim planlarını değerlendirirken ve uygularken "yeni normal" riskleri de göz önünde bulundurması, denetçilere de tecrübe ve becerilerini bu yönde geliştirmeleri konusunda önderlik etmesi gerekmektedir.. Şüphesiz ki, geleneksel denetim eğitimi önemlidir ve daima da önemli olacaktır, fakat kesintisiz eğitim ve maruz kalma, uyarlanabilir, iyi sosyal beceriler ve süreç ve operasyon bilgi birikimi de yeni iş dünyasını idare etmek için olmazsa olmaz şartlardır.

Tüm yetenekleri yönetebilme kabiliyeti, iç denetimin başarısı için hayati önemi haizdir ve sadece dönemsel kadro açıklarını kapatmanın ötesinde birtakım uzun vadeli faydalar da sağlayabilir. Yetenek yönetimi çabalarını optimize edebilmek için, CAE'ler ve üst yönetim, işgüçlerini yeniden yapılandırmaya ve zenginleştirmeye odaklanmış, iyi düşünülmüş ve iyi geliştirilmiş yaklaşımlar benimsemelidirler. Yeni risklerin ışığında olabilecek en iyi iç denetim birimini inşa etmek, elde tutmak ve bağlılığını sağlamak için ve etkinlik mülahazasıyla, CAE'ler, mevcut personelinden istenenleri, kadroya olası ilavelerden beklenenleri ve en az onlar kadar önemli olmak üzere, personelin gelişebilmek ve başarılı olabilmek için liderlerinden ne görmeleri ve ne duymaları gerektiğini ölçmeyi ve tespit etmeyi sağlayan stratejiler geliştirmelidirler.

Sağlam bir yetenek yönetim stratejisi, bir yaklaşımlar kombinasyonuna dayanır. CAE'ler bir yetenek kıtlığında işe alım konusunda çıkış yollarını *bulamayabileceklerdir*. Yarının risklerini – veri bilimi, yaratıcı düşünce, analitik / eleştirel düşünce, iletişim ve benzeri diğer konulardaki beceriler de dâhil – karşılayabilmek için gereken becerilere sahip aday sayısı gerekenden azdır. Etkili bir strateji, hangi becerilere ve özniteliklere gereksinim olduğunun anlaşılmasını ve en iyi yetenekleri kazanmak, geliştirmek ve elde tutmak için kesintisiz çaba gösterilmesini kapsar.

### Amaçlar

- İç denetim biriminin gereksinim duyduğu kolektif yetkinlikler, iç denetimin kapsamını belirleyen risklere bağlı olarak belirlenir.
- CAE'ler, denetim komitesi ve üst yönetimin hem örgütsel amaç ve hedeflere ulaşmak için gereksinim duyulan becerileri hem de iç denetim personelinin toplam maliyetini çok iyi şekilde anlamaları gerekir.
- İç denetim, tutarlı ve istikrarlı bir performans yönetim süreci uygulamalıdır.
- İç denetim liderleri, yeni nesillere ya da herhangi bir nesilden olup da iç denetim mesleğinde yeni olan kişilere liderlik edebilme, akıl hocalığı yapabilme ve onları işe bağlayabilme kabiliyetine sahip olmalıdırlar.
- Tüm iç denetim personeli için resmi kariyer planları mevcut olmalıdır.
- İç denetim birimi, yeni çalışanları çekebilmek ve herkesi kurumsal kültür, risk iştahı ve stratejik yönelim hakkında kesintisiz eğitebilmek için gereken programları kurmuş olmalıdır.

### Eylemler

- Risk değerlendirmesi ve denetim planını gözden geçirmek ve planı hayata geçirmek için gereksinim duyulan becerileri tanımlamak. Mevcut beceriler ile gereksinim duyulan beceriler arasında bir boşluk analizi yapmak ve mevcut boşlukları doldurmak amacına yönelik bir strateji geliştirmek.
- Performans incelemelerini; spesifik iş yetkinliklerini, kurumun stratejik planına uyumlu ve hayata geçirilebilir hedefleri ve veri analistleri gibi uzman profesyonellere yönelik maaş yapılarını kapsayacak şekilde yapılandırmak veya yeniden yapılandırmak.
- Mevcut kadronun sahip olduğu becerileri, işte olabilecek en az kesintiye yol açacak ve mevcut kurumsal bilgi birikimini yeni ihtiyaç duyulan becerilere entegre edecek bir tarzda geliştirmek ve geliştirme sürecine akıl hocalığı yapmak.
- Piyasadan sürekli olarak yeni beceriler kazanmak. Sadece finans ve muhasebe diplomalarını değil, farklı bilimsel disiplinlerden gelen adaylar da aramak. Karmaşık ve uzmanlaşmış riskleri karşılamak için gereksinim duyulan becerilere hızla ulaşabilmek için bir kaynak olarak üçüncü taraf hizmet sağlayıcılarını düşünmek.

## Denetim Odağı

**IIA Standart 1210: Yetkinlik**

İç denetçiler, kişisel olarak, sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer vasıflara sahip olmalıdırlar. İç denetim birimi de, toplu olarak, kendi sorumluluklarını yerine getirmek için gereken bilgi, beceri ve diğer vasıflara sahip olmalı ya da bunları edinmelidir.

**IIA Standart 1230: Sürekli Mesleki Gelişim**

İç denetçiler, mevcut bilgi, beceri ve diğer vasıflarını sürekli mesleki gelişim yoluyla artırmalı ve güçlendirmelidirler.

## Denetim Odağı

**IIA Standart 1220: Azami Mesleki Özen ve Dikkat**

İç denetçiler, makul sınırlar içinde tedbirli ve ehil bir iç denetçiden beklenen becerilere sahip olmalı ve azami özeni ve dikkati göstermelidirler. Azami mesleki özen ve dikkat, tabii ki, hiç hata yapılmayacağı anlamına gelmez.

**1220.A2 –** Azami mesleki özen ve dikkati gösterirken, iç denetçiler, teknolojiye dayanan denetim tekniklerini ve diğer veri analiz tekniklerini kullanmayı da düşünmelidirler**.**

- Etkin ve etkili bir işe alım, işe alıştırma ve bilgi aktarma programı yapmak ve uygulamak.

### Veri Analitiği

Veri analitiği, verilerin toplanması ve analiz edilmesinden ve ardından, analiz sonuçlarının daha iyi karar almak için kullanılmasından oluşan bir süreçtir *(Internal Auditing, 4. baskı, 11-2,* İç Denetim Vakfı, 2017*)*. Kurumlar işle ilgili faaliyetleri sonucunda büyük veri depoları yaratmaktadırlar ve bu da iç denetim için iki büyük sorun yaratmaktadır. Birincisi, iç denetim birimi yönetim kuruluna ve yönetime bu verilerin nasıl toplandığını, yönetildiğini, korunduğunu ve kontrol altına alındığını anlamasında nasıl yardımcı olacaktır. İkincisi, analiz araçlarının mevcut denetim süreçlerine uygulanmasında ve rutin denetimlerin otomatiğe bağlanmasında ve yeni gelişen risk alanları üzerinde odaklanmak konusunda giderek artan verilerden iç denetim perspektifiyle nasıl istifade edilecektir (Odak Noktasındaki Risk: İç Denetim İçin Sıcak Konular 2018 isimli bölüme bakınız).

Temelde, veri analitiği süreci veri depolarını önce parçalarına ayırır, sonra daha küçük külçeler halinde yeniden inşa eder ve böylece, verilerden anlam ve sonuç çıkartabilme fırsatına kavuşur. Bu bilgiyle, iç denetim birimi *toplam popülasyon* risklerini ve potansiyel bağıntıları analiz edebilir; içgörü ve öngörü (sağduyu) elde edebilir ve paydaşların takip etmekle ilgilendikleri ve kaygı duydukları sorunlar hakkında rapor sunabilir. Veri analitiği sürecini ve onunla bağlantılı riskleri yönetmek ürkütücü olabilir. Bu verilerden anlamlı sonuçlar çıkartmak – ve bu bilgileri eyleme dönüştürmek – bazen sözle ifade edildiği kadar kolay olmayabilir. Veri analitiğinin etkin ve etkili olabilmesi için, doğru insanlar, formatlar, süreçler ve teknolojilerin mevcut olması ve kullanılması gerekir.

Derhal kullanabileceği eskisinden çok daha fazla veriyle, yönetim ve yönetim kurulu, muazzam miktarlarda verinin kurumu veriyle ilişkili finansal risklere ve finans-dışı risklere maruz bıraktığını fark etmeli ve anlamalıdırlar. Analitik insiyatifi ve çalışmasında çeşitli farklı risk alanları ele alınmalıdır (Analitik Risklerini Anlamak ve Yönetmek isimli bölüme bakınız):

- **Veri ve Bilgi Kalitesi Riski** — Karar alıcılar, karmaşık bir bütünün anlaşılmasını kolaylaştıran ve gerekli iletişimi sağlayan verilere gereksinim duyarlar. Tüm veri ve bilgiler için açık tanımlar ve kalite standartları mevcut olmalıdır.**Veri ve Bilgi Uyum Riski** — (Genellikle eyalet, federal veya uluslararası bağlantılı) bir tanınmış ve yetkili kurumun koşullarına uyulmaması para cezası, ek çalışma veya şahsi sorumluluk gibi olumsuz sonuçlara yol açabilir.
- **Veri ve Bilgi Yönetişim Riski** — Veri ve bilgiler, mahremiyeti, güvenliği, kaliteyi ve denetlenebilirliği sağlamak için uygun seviyelerde risk yönetim prensipleri ve süreçleri kullanılarak dikkatle kontrol edilmelidirler.
- **Analitik Riskin Uygun Olmayan Şekilde veya Vaktinden Önce Kullanılması** — Verileri toplamak, işlemek ve yorumlamak için zaman yoksa; kararlarda kullanılabilecek tarihi veriler veya emsaller yoksa ya da tarihi veriler yanıltıcı ise ya da anahtar değişkenler ölçülemiyorsa veya yüksek bir belirsizlik derecesine sahipse analiz çalışması faydalı olmaz.
- **Karşıt Kültürel Etki Riski** — Veri odaklı olmayan bir kurum kültürüne analitik inisiyatiflerin empoze edilmesi liderler açısından önemli bir risk oluşturabilir; analitik inisiyatifleri, kurumsal karar alma sistemi hakkında ve kurumsal kültürün ne kadar veri-odaklı olduğu konusunda bir değerlendirme çalışmasını da içermelidir.

- **Veri Etiği Riskleri** — Data analitik inisiyatifleri, kurumun temel değerlerine, karar alma sürecine ve davranışlarına uyumlu olmalıdır. Verilerin etik toplanması ve kullanılmasını temin etmek amacına yönelik kontroller mevcut olmalıdır.

İç denetim birimi, özellikle personelin gereken bazı becerilerden yoksun olduğu durumlarda, kurumların büyük veri projelerinde karşılaşabilecekleri tehlikelerin daima farkında olmalıdır. Veri analitiği talebi artmaktadır ve – henüz olmamışsa bile - yakında *her* kurumun tamamlayıcı bir parçası ve unsuru haline gelecektir. Kurumların rekabet edebilmek ve geride kalmamak için büyük veri projelerine iştirak etmeleri önemli olmasına rağmen, bu durumda dikkate almaları gereken belirli riskler de vardır:

- Veri güvenliği.
- Veri mahremiyeti.
- Maliyetler.
- Güvenilmez, geçersiz, yetersiz veya anlamsız (bağlantısız) veriler.
- Güvenilmez, geçersiz, yetersiz veya anlamsız (bağlantısız) analitik süreçler.

Teknoloji, dünyamızı şimşek hızıyla değiştirmektedir ve bu değişime yeterince hazırlıklı olmazsak, bu değişim hızının neticeleri en hafif deyimiyle moral ve sinir bozucudur. Teknoloji çok daha büyük miktarlarda veri yaratmaktadır ve iç denetim birimi bu verileri riskleri daha derinlemesine değerlendirmek, denetimlerin sonuç ve sunumlarını iyileştirmek ve sağladığı güvence seviyesini muhtemelen artırmak için kullanabilir.

Son yapılan vaka etütlerinden elde edilen sonuçlar, veri analitiğinin iç denetime sağladığı temel faydalar arasında etkinlik artışı, verimlilik artışı, geliştirilen güvence, stratejik risklere daha fazla odaklanma, daha büyük denetim kapsama alanı ve uzun vadede zaman ve para bakımından önemli tasarrufların bulunduğuna işaret etmektedir. Bununla birlikte, bu faydalardan istifade edebilmek için, iç denetim biriminin veri analitiği programının birimin daha üst ve genel hedeflerine ve arzu ettiği faaliyetlere ne kadar faydalı olduğunu da gözden geçirmesi ve değerlendirmesi gerekmektedir.

Veri analitiği iç denetim biriminin araç takımı için hayati önemi haizdir, çünkü hem verilerin çok derininde gömülü bulunan içgörüleri sağlayabilir hem de daha etkin ve verimli test yapılmasına olanak sağlar. Pek çok iç denetim ekibi, daha sofistike veri analitiği teknolojilerine henüz geçmemişlerdir; hâlâ hesap tablosu ve çizelgesine dayanan araç ve uygulamalara bel bağlamaktadırlar. Denetim komitesinin desteği şarttır. İç denetim birimi, denetim komitesinin veri analitiğinin önemi hakkında eğitilmesini mutlaka sağlamalıdır (Veri Analitiği: İlk Adımı Atmanın Zamanı Geldi mi? başlıklı bölüme bakınız).

Bir veri analitiği programı inşa etmek veya mevcut programı geliştirmek için, CAE'ler arzu edilen sonuçlar hakkında paydaşlarla müzakerelere girmeli, analitik çalışmasının amaçlarını tanımlamalı ve hangi *yetkinliklere* ve teknolojilere gereksinim olacağını belirlemelidirler.

Etkin bir veri analitiği programı inşa etmenin önündeki en büyük engellerden biri – ve iç denetim için devamlı mevcut risklerden biri – büyük verileri işleyebilecek becerikli personelin yetersiz olmasıdır. Bu uzmanlık alanındaki açıktan dolayı, iç denetim biriminin analitik programları optimum düzeyin altında olabilir – mutlaka programın kendisinden dolayı değil, fakat programın tam potansiyelinde kullanılmamasından da dolayı bu böyledir. Tüm yeni iş

inisiyatiflerinde olduğu gibi, büyük veri projeleri de bir risk unsuru içerirler. Büyük verileri yönetmek için gereken yetenekler eksikse, bu durum risk unsurunu daha da çok artırır.

## Amaçlar

- İç denetim birimi veri analitiği ve teknolojisi hakkında ve gelişmiş teknolojilerin iç denetimin etkinliğini ve verimliliğini nasıl artırabileceği konusunda derin bir bilgi ve anlayışa sahip olmalıdır.
- İç denetim birimi, iyi yönetimin veri analitiğinin genişletilmiş kullanım alanının yarattığı yeni risklere nasıl cevap ve karşılık verdiğini değerlendirmelidir.
- İç denetim birimi, veri analitiği programlarının gelişmiş kabiliyetlerinden kurumun komple menfaati ve yararı için (örneğin, yüksek riskli plan ve davranışların validasyonu ve izlenmesi, kuruma özgü risk değerlendirme süreçlerinin değerlendirilmesi ve hassasiyeti, vb.) istifade etmelidir.
- İç denetim birimi, teknolojiyi, anormallikleri ve sahtekârlık eylemleri risklerini erken tespit etmek için kullanmalı ve temel bulgularını bildirmeli ve açıklamalıdır.
- İç denetim birimi, teknolojiyi, kurumun genel risk karşılığını daha düşük işçilik saatiyle ve daha düşük işçilik maliyetiyle iyileştirmek için kullanılır.

Kısmen şu yayından adapte edilmiştir: Kendi İç Denetim Ekibiniz İçin Bir Veri Analitiği Programı İnşa Etmenin İlk Adımları

## Eylemler

- Veri analitiği programı için temel ve spesifik gereksinimlerin neler olduğuna karar vererek, analizlerin hangi sonuçlarının iç denetim biriminin amaç ve hedeflerine en iyi hizmet edeceğini belirlemek.
- Analitik programların kuruma ve iç denetim birimine inovasyon ve fırsat bakımlarından sağlayabileceği faydaları anlamak. Programları optimum düzeyde uygulamak ve faydalarından istifade edebilmek için ihtiyaç duyulan becerileri tespit etmek.
- Veri analitiğini kritik bir iş unsuru olarak görmek ve denetim görevini kurumun uyum ve kontroller çerçevesinin tamamının yönetimine ilişkin olabilecek en iyi, sürdürülebilir kalite yaklaşımını elde edecek şekilde uyarlamak.
- Usulsüzlükleri veya sahtekârlık eylemlerini doğru bir şekilde tespit edebilecek spesifik kurallar, veri noktaları, kodlar ve varsayımlar konusunda yönetimle mutabakata varmak.

# Siber

İster kurumlara karşı acımasız bilgi ihlâlleri ve saldırıları biçiminde isterse asla sona ermeyen kişisel kimlik hesapları hırsızlığı biçiminde olsun, siber suçlular – sofistike ve iyi fonlanmış – aşılması zor ve çetin düşmanlardır. Karşılıklı bağlılık, sanki siber suçlular için özel olarak hazırlanmış karmaşık ve risk tabanlı bir dünya yaratmaktadır. Siber suçluların kullandıkları teknikler sürekli genişlemekte ve evrim göstermektedir; tabii ki ve aynı şekilde, onlara ayak uydurmak da günlük hafif ve tatsız bir iş haline gelmektedir.

Siber saldırılara karşı bir savunma planını devreye sokmak ve planın etkin ve işler halde olmasını sağlamak 24 saatlik bir iştir; sorun, bir saldırının *olup olmayacağı* meselesi değil, *ne zaman* olacağı meselesidir. Siber risk bilincine sahip olmak ile siber risklere karşı *hazırlıklı olmak* arasında büyük bir fark vardır. Herkes bu risklerin *farkındadır;* bu risklerin yarattığı gerçekle her gün karşı karşıyayız. Ancak hazırlıklı olmak, bir saldırı teşebbüsünü tamamen *püskürtme* yeteneğini ya da bir saldırıya *direnme* ve saldırıdan nispeten az zararla veya tamamen zararsız kurtulma kabiliyetini kapsar. Kurumların bir ihlâl belasına karşı küçük bir parça bile olsa korumadan istifade edebilmek için siber saldırılara karşı direnebilmeleri, reaksiyon gösterebilmeleri ve saldırıdan kurtulabilmeleri gerekir – *siber dirençlilik.*

Siber risklere (yani, bilgisayar korsanlığı/izinsiz girişler, şifre avcılığı, ekonomik casusluk, vb.) ilişkin kaygı ve endişeler arttıkça, paydaşlar da kendi kurumlarının siber güvenlik risk yönetimi programlarına daha fazla görünürlük talep ediyorlar ve yönetim kurulu da iç denetim biriminin siber riskleri ve siber programları bağımsız, objektif ve kapsamlı bir şekilde incelemesini ve gözden geçirmesini istiyor. Bu nedenle, iç denetim birimi de olası riskler hakkında bilgili olmalı ve siber dirençlilik konusunda önemli bir rol üstlenmeli ve oynamalıdır.

Maalesef, siber güvenlik riskleri sadece dış tehditlerle sınırlı değildir; kurum çalışanları veya iş ortaklarının eylemlerinden kaynaklanabilecek potansiyel tehditler de vardır. Bu sebeple, siber dirençliliğin yaşamsal bir unsuru da hem kurumun kültürünün uygun ve etkin bir biçimde yönetilmesi hem de kurumun *risklerinin* uygun ve etkin değerlendirilmesidir. Kültürü düşünürken, yönetim kurulları *risk kültürünü* de değerlendirmeye alırlar, çünkü kurumun tamamında alınan tüm kararların, yapılan uygulamaların ve alınan tüm risklerin temelinde bu *risk kültürü* yatmaktadır. İç denetim, risk kültürünü de standart operasyonel ve finansal denetimlerin kapsamı içinde gerekli verileri toplayarak ve gayri resmi incelemeler yaparak denetleyebilir.

Mücadelenin en ön saflarında olan iç denetim birimi, tüm alanlarda, hatta kurumun kültürünün koşulları, süreçleri ve yetenekleri etkilediği seviyede bile, yönetimin siber güvenlik kontrollerinin etkinliği ve verimliliği hakkındaki bilgi ve anlayış düzeyini kuvvetlendirebilir. Kültür bir kurum içerisinde üretkenliği, değerleri, davranışları ve uygulamaları yönlendirir ve pek çok farklı faktörle şekillenir ve sürdürülür; bu sebeple, iç denetim riskle ilgili kültürü de bir kurumun diğer alanlarını değerlendirdiği gibi aynı şekilde ve aynı yolla değerlendirebilir (İç Denetimin Gelecek Trendleri başlıklı bölüme bakınız). İç denetim, kültürü nasıl değerlendireceğini anlayarak ve yönetimi kültürün önemi konusunda eğiterek kendi değerini azami düzeye yükseltebilir.

Kültür de dâhil siber-ilişkili riskleri aşmak ve çözümlemek için, liderlik ekibinin önleyici tedbirler geliştirmesi, bu tedbirleri eğitim ve bilinçlendirme programlarıyla birlikte uygulamaya sokması ve ardından bunların davranışlarda kesintisiz ve sürekli gösterilmesini sağlaması kritik önemi haizdir. Bu sebeple, çalışanlar, tedarikçiler, ortaklar ve yükleniciler de aynı şekilde eğitilmeli ve siber güvenlik tedbirleri ve protokolleri konusunda onlardan neyin beklendiğini tam olarak anlamaları sağlanmalıdır.

İç denetim biriminin risk değerlendirme stratejileri, siber güvenliğe özgü tüm riskler için geliştirilmeli ve politikalara ve iç kontrollere uyulmasını temin etmelidir. İç denetim biriminin siber sorunların etkili olabileceği tüm alanlarda kurumun ve paydaşlarının gereksinimlerini karşılayan yoğun bir denetim yaklaşımı geliştirmesi gerekmektedir. Etkin olabilmesi için, bu, en azından

"Yöneticilerin siber risk gözetimi ve denetiminde etkin bir rol oynayabilmek için teknoloji uzmanları olmaları gerekmez— fakat her yönetim kurulu siber-gözetim uygulamalarının etkinliğini artırma ve geliştirme fırsatına ve olanağına sahip olabilir."

NACD Siber-Risk Gözetimi Hakkında Yönetim Kurulu Üyesinin Elkitabı, Ulusal Kurumsal Yöneticiler Birliği (NACD), 2017

Kaynak: Görünürlüğün Değeri: Siber Güvenlik Risk Yönetimi İncelemesi

kontrol faaliyetleri, bir kontrol ortamı, risk değerlendirmesi, iletişim ve izleme süreçlerinin kurulmasını ve aynı zamanda siber güvenlik tedbirlerinin değerlendirilmesi için bir çerçevenin kurulmasını gerektirir (Odak Noktasındaki Risk: İç Denetim İçin Sıcak Konular 2018 isimli bölüme bakınız).

Üçüncü savunma hattı olarak, iç denetim birimi, kurumun siber güvenlik risklerini tespit etme ve azaltma kabiliyetlerini geliştirmek amacına yönelik siber güvenlik stratejileri ve politikaları geliştirme çabalarında yönetimle ve yönetim kuruluyla birlikte çalışmalı; denetim komitesiyle ve yönetim kuruluyla ilişkileri güçlendirmeli ve onların bağlılıklarından emin olmalı ve siber güvenlik riskinin planı uygulamak için gereken becerilerle (kurum içi veya ortak kaynak kullanımı yoluyla) plana *resmen* entegre edilmesini temin etmelidir. Gelişmekte olan teknolojiler ve trendler bir kurumun siber güvenlik risk profilini etkiler; bu sebeple, iç denetim birimi gelişen teknolojilerden de haberdar kalmalı ve kurumun kırılganlık seviyesini değerlendirmeli ve kurumun risk faaliyetlerini tercih edilen siber güvenlik planına kıyasla gözden geçirmelidir.

## Amaçlar

- Kurumun bir siber dirençli kültürü bulunmalıdır.
- İç denetim birimi, siber güvenlik incelemesi ve hazırlıklı olmak açısından kritik öneme sahip olan kilit komponentlere katkıda bulunmalıdır:
  - Koruma ve Teşhis: İç denetim birimi, bir kurumun hangi noktalarda kırılgan olabileceğinin tespiti konusunda bütüncül bir yaklaşım uygular ve veri analitiğini de kendi sorumluluk sahasına alır ve bu da yanlış giden bir şeyler olduğunda gereken alarmı verir.
  - İşin Devamlılığı: İç denetim birimi, siber saldırılar, doğal afetler veya halefiyet sorunları da dâhil devam eden operasyonları etkileyebilecek risk senaryoları hakkında tavsiyeler vermeli ve bu senaryolarla baş etme ve sorunları aşma çcabalarında yönetimle birlikte çalışmalıdır.
  - Kriz Yönetimi / İletişim: İç denetim birimi, kriz yönetimi planlaması ve iletişim hazırlıklarına, etkinlik ve zamanındalık hakkında güvence kontrolleri yaparak, analizler yaparak ve plan uygulamaları hakkında eleştirilerde bulunarak yardımcı olur.
  - Kesintisiz Gelişme: İç denetim birimi, siber saldırılara karşı daha hazırlıklı olmak amacıyla gereken içgörüyü sağlayarak ve strateji ve protokolleri geliştirerek değer katar.

## Eylemler

- Kurum kültürünü siber dirençlilik bakımından değerlendirmek.
- Güvenlik modelleri ve siber güvenlik süreçlerinin risk değerlendirmelerini yapmak ve geliştirme tavsiyelerinde bulunmak.
- Üçüncü tarafların belirlenen protokollere uyma kabiliyetlerini tespit etmek ve değerlendirmek amacıyla BT ile ve üçüncü taraf yüklenicilerle veri penetrasyon testi yapmak.
- Siber dirençlilik boşluk analizleri yapmak, telafi ve çözüm yolları tavsiye etmek ve telafi ve çözüm faaliyetlerini takip etmek.

- Siber güvenlik izleme ve cevabını birinci öncelikler olarak ön plana çıkartmak ve vurgulamak suretiyle kültürü etkilemek.
- İş devamlılık planının periyodik olarak test edilmesini ve tespit edilen eksiklikler için gereken düzeltici tedbirlerin alınmasını sağlamak.
- Kurum çapında, zaman içerisinde siber güvenlik tedbirlerini ve protokollerini etkileyecek ve artıracak nitelikte güçlü bir siber kültür ve risk kültürü uygulamak ve uygulanmasını teşvik etmek.

# Mevzuat

Global düzeyde, kurumlar kısmen tüketicileri veya kamu menfaatlerini korumak amacına yönelik yeni veya değiştirilmiş mevzuat gereklilikleri ve koşullarıyla karşı karşıya kalmaktadırlar. En yüksek profilli mevzuat belgeleri finansal risk ve kontroller ve veri mahremiyeti ve güvenliği üzerine odaklananlardır ve tüm sektörlerden kurumları etkilemektedirler.

## Kripto Kurlar

CNBC'ye göre, kripto kurlar. dijital paralar arasında yeni yapılan yoğun bir elden çıkarma işleminden sonra işlem değeri bakımından trilyon dolar seviyesini geçebilirler. Bitcoin değeri dalgalıdır: 2018 başlarında, $6.000 ile $10.000 arasında değişmiştir. Kripto kur borsası Gatecoin'de APAC iş geliştirme bölümü başkanı olan Thomas Glucksmann şunu söylemektedir: "Kripto kur borsalarının resmi kurumlarca tanınmasında artış, kurumsal sermayenin uygulamaya sokulması ve büyük teknolojik gelişmeler, bu pazarın tekrar sıçramasını sağlayacak ve kripto kur fiyatlarını bu yıl içinde tüm zamanların en yüksek seviyesine sıçratacaktır. Bitcoin'in Aralık (2018)'e kadar $50.000 seviyesine ulaşmaması için hiçbir sebep yoktur."

Global düzeyde, büyük finans kuruluşları, blok zinciri teknolojisine ve kripto kur alım satımına daha fazla girdikçe, çalışanları dijital paraları kendi kişisel hesaplarına alıp sattıklarında ortaya çıkabilecek menfaat çatışmalarını nasıl çözümleyeceklerini düşünmek ve bir çare bulmak zorunda kalmaktadırlar. Dijital paraların yükselen fiyatları sadece yatırımcıların ve bankaların ilgisini tetiklemekle kalmadı, aynı zamanda uyum departmanları da bu paralara artık daha fazla dikkat ediyorlar. Kripto kur alım satımını yapan – ya da kripto kura yatırım yapmak isteyen – çalışanlar haksız menfaat yaratacak şekilde bahis oynarlarsa menfaat ç atışmaları doğabilir. Genelde, çalışanların bir menfaat çatışması yaratan menkul kıymetlerin alım satımını yapmadan önce bir izin almaları gerekir; bununla birlikte, alım satım işlemleri parçalı bir borsa ağı yoluyla – bazen anonim olarak – gerçekleştirildiği ve izlemek zor olduğu için kripto kurlarla ilgili politikaları uygulamak çok daha zordur. Ek olarak, global düzenleyici otoritelerin açık ve net kuralları mevcut değildir ve bu da finans kuruluşlarının kendi kurallarını belirlemelerini daha güç hale getirmektedir. Bazıları kripto kurları emtia olarak görmekte, bazıları ise bazı kripto kurların menkul kıymetler olabileceklerini söylemekte, fakat hangilerinin menkul kıymet olduğunu söylememektedirler. Global düzenleyici otoriteler Bitcoin ve diğer dijital kurların değerindeki son patlayıcı uçuculuktan ve değişkenlikten ötürü endişe duymuşlardır ve bu konuda sert ve etkili yasal düzenlemeler çıkartılabilir (Kripto Kur Alım Satımı Yaygınlaştıkça Uyum Memurları Terliyorlar başlıklı bölüme bakınız).

## Denetim Odağı

**IIA Standart 2130: Kontrol**

İç denetim birimi, kontrollerin etkinliğini ve verimliliğini değerlendirmek ve sürekli gelişimi teşvik etmek suretiyle, kurumun etkin kontrollere sahip olmasına yardımcı olmalıdır.

**2130.A1 –** İç denetim birimi, kurumun yönetişim, operasyonlar ve bilgi sistemleri içerisinde, kontrollerin aşağıda sayılan konularla ilgili risklere cevap ve karşılık verme konusundaki yeterliliğini ve etkinliğini değerlendirmelidir:

- Kurumun stratejik amaç ve hedeflerine ulaşma kabiliyeti.
- Finansal ve operasyonel bilgilerin güvenilirliği ve doğruluğu.
- Operasyonlar ve programların etkinliği ve verimliliği.
- Varlıkların muhafazası ve korunması.
- Kanunlara, yönetmeliklere, politikalara, prosedürlere ve sözleşmelere uyum.

## Global Veri Koruma Mevzuatı

Bir dizi hükümet, verilerin mahremiyeti hakkında giderek etkisini artıran mevzuat koymaktadırlar. Bunun iki örneği Avrupa Birliği (AB) ve Çin'dir.

Dört yıllık hazırlık ve tartışma evresinden sonra, 95/46/EC sayılı Veri Koruma Direktifinin yerine geçmesi plananan AB Genel Veri Koruma Yönetmeliği (GDPR) Nisan 2016'da AB Parlamentosu tarafından onaylandı. GDPR, yıllar geçtikçe veri ihlâllerinin giderek daha büyük, daha müdahaleci ve daha maliyetli bir hale geldiği bir zamanda, Mayıs 2018'de yürürlüğe girecektir. Veri ihlâlleri, 2015'den 2016'ya yüzde 40 oranında rapor edilen veri artışından sonra 2017 yılında önemli oranda artmış bulunmaktadır. (Bu konuda ek detaylı bilgiler için, gelecek sayfadaki "2017 Veri İhlâlleri" bölümüne bakınız.)

Pek çok şirketin eski direktifle uyumlu mahremiyet politikaları bulunmasına rağmen, yeni GDPR, AB verileri için bir dizi yeni koruma önlemi getirmekte ve yürürlüğe girdikten sonra kurallarına uymayan veri kontrolörleri ve işlemcilerine para cezaları ve başka cezalar getirmektedir. Basit bir ifadeyle, Avrupa'da iş yapan veya AB mukimlerinin kişisel verilerini kullanan (yerel ya da uluslarlarası) tüm şirketler bu yeni kurallara uymak zorundadırlar.

Temel hükümlere yönelik çok zarar verici aykırılık ve ihlâllerde, düzenleyici otoriteler bir önceki yılın global yıllık cirosunun yüzde 4'üne ya da 20 milyon €'a kadar (hangisi daha büyükse) çıkabilen tutarlarda para cezası verme yetkisine sahiptirler. Kademeli bir para cezası yaklaşımı benimsenmiştir (örneğin, bir şirket düzenli kayıt tutmamaktan (Madde 28), bir ihlâli veri süjesine ve gözetim otoritesine ihbar etmemekten ya da bir etki değerlendirmesi yapmamaktan ötürü yüzde 2 oranında para cezası alabilecektir). Bu kuralların hem kontrolörlere hem de işlemcilere uygulanacağını not etmek önemlidir – bu da, bulut sunucularının da GDPR uygulamasından muaf tutulmadıkları anlamına gelmektedir. Bu kategoriye giren diğer örnekler, kişisel verileri işlemekle ilgili temel prensiplere uymamak; veri süjelerinin haklarına tecavüz etmek ve kişisel verileri yeterli seviyede veri koruması sağlamayan üçüncü ülkelere veya uluslararası teşkilatlara transfer etmektir. (AB Genel Veri Koruma Yönetmeliğine bakınız).

"Genel Veri Koruma Yönetmeliği ve bu yönetmeliğin etki ve müdahaleleri giderek yaygınlık kazanıyor. Bir güvence perspektifinden bakıldığında, denetim komitesi bizim öncelikle programın kendisini değerlendirmemizi, fakat daha sonra kurumun mevzuata uymaya devam edebilmesi için doğru süreçlere sahip olduğundan emin olmak için devamlılık temelinde kendi programımızı geliştirmemizi isteyecektir."

Bir çokuluslu bankacılık grubunun İç Denetim Yöneticisi

Kaynak: Odak Noktasındaki Risk: İç Denetim İçin Sıcak Konular 2018

| 2017 Veri İhlâlleri | | |
|---|---|---|
| **Ay** | **Kurum** | **İhlâl / Aykırılık** |
| **8 Ocak 2017** | E-Sports Entertainment Association (ESEA) | Veritabanına 1.503.707 kayıt eklendi ve kişisel/özel bilgiler de dâhil kayıtlar sızdırıldı. |
| **2 Şubat 2017** | Xbox 360 ISO and PSP ISO | 1,2 milyon Xbox 360 ISO kullanıcısı ve 1,3 milyon PSP ISO etkilendi; kişisel / özel bilgiler çalındı. |
| **15 Mart 2017** | Dun & Bradstreet | A.B.D. Savunma Bakanlığı ve A.B.D. Posta İdaresi de dâhil 33 milyondan fazla kurumsal ilişki internet ortamında paylaşıldı; kişisel / özel bilgiler sızdırıldı. |
| **6 Nisan 2017** | FAFSA: IRS Data Retrieval Tool | 100.000'e kadar vergi mükellefi/öğrencinin kişisel/özel bilgileri çalınmış olabilir. |
| **10 Mayıs 2017** | Bronx Lebanon Hospital Center | 2014 ile 2017 yılları arasında en az 7.000 hastanın bağımlılıkları, akıl sağlığı ve medikal sağlık durumları, tanıları, HIV durumları ve saldırı raporları da dâhil aşırı kişisel bilgileri suiistimal edilmiş olabilir. |
| **20 Haziran 2017** | Deep Root Analytics | Cumhuriyetçi Ulusal Komitesi'nin görevlendirdiği Deep Root Analytics firması özel/kişisel bilgileri şifre koruması olmaksızın bir bulut sunucuya koyduğu ve bu bilgiler iki hafta süreyle herkesin erişimine açık kaldığı için kabaca 198 milyon Amerikan vatandaşı bu saldırıdan etkilenmişlerdir. |
| **13 Temmuz 2017** | Verizon | Kayıtlar güvenliksiz bir sunucuda tutuldukları için 14 milyon aboneyle ilgili bilgiler erişime açık kalmıştır; elde edilen veriler, müşteriler telefonla Verizon'u aradıklarında üretilen günlük dosyalarıydı. |
| **30 Ağustos 2017** | Online Spambot | Bir güvenliksiz sunucudan alınan 711 milyon email adresi ve şifresi |
| **7 Eylül 2017** | Equifax | Korsanların websitesi yazılımındaki bir zayıf noktadan istifade ederek sisteme erişebilmelerinden ötürü 143 milyon müşteri etkilenmiş olabilir; sosyal güvenlik numaraları ve kredi kartı numaraları da dâhil özel/kişisel bilgiler saldırıya açık hale gelmiştir. |
| **12 Ekim 2017** | Hyatt Hotels | 11 ülkede 41 otelde kullanılan (okutulan) banka ve kredi kartlarına ilişkin kredi kartı numaraları, dâhili doğrulama şifreleri ve kart hamili isimleri de dâhil ödeme bilgilerine yetkisiz erişim olayı. |
| **21 Kasım 2017** | Uber | 57 milyon sürücü ve müşterinin isimler, eposta adresleri ve telefon numaraları da dahil kişisel bilgileri saldırıya açık hale geldi. |
| **10 Aralık 2017** | TIO Networks (PayPal) | 1,6 milyonun üzerinde müşterinin banka hesabı bilgileri, ödeme kartı bilgileri, şifreleri, kullanıcı isimleri ve sosyal güvenlik numaraları da dâhil kimlik bilgileri açığa çıkmıştır. |

Şu yayından adapte edilmiştir: 2017 Veri İhlâlleri – Bugüne Kadarki En Kötüsü

## Denetim Odağı

**IIA Standart 2120: Risk Yönetimi**

İç denetim birimi, risk yönetim süreçlerinin etkinliğini değerlendirmeli ve bu süreçlerin iyileştirilmesine katkıda bulunmalıdır.

**2120.A1 –** İç denetim birimi, kurumun yönetişim, operasyonlar ve bilgi sistemleriyle ilgili maruz kaldığı riskleri aşağıda sayılan açılardan değerlendirmelidir:

- Kurumun stratejik amaç ve hedeflerine ulaşma durumu.
- Finansal ve operasyonel bilgilerin güvenilirliği ve bütünlüğü.
- Operasyonlar ve programların etkinliği ve verimliliği.
- Varlıkların korunması.
- Kanunlara, yönetmeliklere, politikalara, prosedürlere ve sözleşmelere uyum.

"Rıza" kelimesinin tanımı ve koşulları bile önemli oranda kısıtlanmıştır. Önceden, veri kontrolörlerinin bazı durumlarda zımni ve "istisna tutma" rızalarına dayanarak işlem yapmalarına izin veriliyordu. 25 Mayıs 2018 tarihinden itibaren, GDPR, rıza için aranan koşulları güçlendirmektedir ve şirketler artık hukuk jargonuyla dolu uzun ve okunaksız şart ve koşullar kullanamayacaklar, çünkü o rızaya bağlı veri işleme amaçlarıyla rıza talebinin kolay erişilebilir bir formda verilmesi gerekmektedir. Rızanın açık olması ve başka hususlardan ayırt edilebilir olması ve net ve düz bir lisanla ifade edilmiş olması gerekmektedir. Rızayı geri çekmek de rızayı vermek kadar kolay olmalıdır. Ayrıca, rızalarını geri çektikten sonra, veri sujeleri kendi kişisel verilerinin *silinmesini* ve veri işleme için artık kullanılmamasını isteme hakkına da sahiptirler (AB'nin Genel Veri Koruma Yönetmeliğinin En Büyük 10 Operasyonel Etkisi isimli bölüme bakınız).

GDPR, Almanya'nın siber güvenlik çabalarını önemli oranda etkileyecektir. Mayıs 2017'de, yasama organı, 25 Mayıs 2018 tarihinde AB GDPR ile birlikte yürürlüğe girecek olan Federal Veri Koruma Kanunu'nun gözden geçirilmiş bir versiyonunu çıkartmıştır. 300.000 €'ya kadar çıkan para cezalarıyla kuvvetli ulusal veri koruma kanunlarıyla tanınan Almanya, artık katı siber güvenlik standartlarına geçiyor ve kullanıcıları koruma ve siber bilgilerin güvenliğini sağlama sorumluluğunu kritik altyapının işletmecilerine ve hizmet sağlayıcılarına veriyor. Yeni kanun, birkaç tanesi AB GDPR'ye çapraz atıfta bulunan 85 madde içermektedir. Kritik altyapı işletmecilerinin bu koruma tedbirlerini düzenleyen ikincil mevzuatın yürürlüğe girmesinden itibaren iki yıl içerisinde *tekniğin en gelişmiş düzeyine* uygun olarak gereken tüm uygun organizasyonel ve teknik koruma tedbirlerini ve diğer önlemleri almaları ve uygulamaları gerekmektedir. Ek olarak, kritik altyapı işletmecilerinin güvenlik koşullarını yerine getirdiklerini düzenli olarak kanıtlamaları ve BT sistemleri, komponentleri ve süreçlerinin emre amadeliği, bütünlüğü, güvenilirliği ve gizliliğinde meydana gelebilecek ve kendilerinin işlettiği kritik altyapının fonksiyonunda bir kesintiye veya bozulmaya yol açabilecek veya yol açmış olabilecek önemli ihlâlleri derhal *Bundesamt für Sicherheit in der Informationstechnik*'e (BSI) bildirmeleri de gerekmektedir (Almanya'nın Siber Güvenlik Kanunu Hakkında Bilmeniz Gerekenler başlıklı bölüme bakınız).

Çin, bilgi güvenliği konusunda zaten katı ve sıkı kanunları, kuralları ve yönetmelikleri bulunmasına rağmen, siber güvenlik ile veri koruma arasındaki boşluğu kapatan ve AB'nin GDPR'sine uygun hükümler getiren (Haziran 2017'de yürürlüğe giren) kapsamlı bir kanun daha çıkartmıştır. Çin Halk Cumhuriyeti'nin Siber Güvenlik Kanunu (CSL) pek çok bakımdan GDPR'ye uyumludur (Odak Noktasındaki Risk: İç Denetim İçin Sıcak Konular 2018 başlıklı bölüme bakınız). CSL, kişisel bilgilerin ve bireysel mahremiyetin korunmasına daha fazla dikkat eden ve kişisel bilgilerin toplanması ve kullanılmasını standardize eden değişiklikler yapmıştır. Örneğin, eskiden, yabancı şirketler bilgilerini Çin dışına çıkartabiliyorlardı; artık, bu yeni kanuna göre, hassas verilerin ülke içinde saklanması gerekmektedir ve kanunun ihlâlinde ticari faaliyetlere son verilmesi de dâhil ağır cezalar uygulanacaktır. Para cezaları 1.000.000 RMB'ye kadar ulaşabilmektedir. (Konu hakkında ek bilgi almak için, gelecek sayfadaki "CSL'de Yapılan Değişiklikler" bölümüne bakınız.)

| CSL'de Yapılan Değişiklikler | | |
|---|---|---|
| Madde | **Nihai Versiyon** | **Önemli Değişiklikler** |
| **31** | Siber güvenlik koruması hakkında, devlet, hem ***kamu iletişim ve bilgi hizmetleri, enerji, finans, ulaşım, suların korunması, kamu hizmetleri ve e-yönetişim*** alanlarında kritik bilgi altyapısının hem de imha edildiği, işlevselliğini kaybettiği ya da veri sızdırdığı takdirde ulusal güvenliğe, ulusal ekonomiye ve kamu menfaatlerine ciddi zararlar verebilecek başka kritik bilgi altyapılarının korunması gerektiğini vurgulamaktadır. | Bu madde, kritik bilgi altyapısının korunmasına öncelik verilecek olan sektör ve endüstrileri belirtmektedir. |
| **43** | Kişiler, ağ operatörlerinden topladıkları veya sakladıkları kişisel bilgilerinde olabilecek hataları düzeltmelerini isteme hakkına sahiptirler. ***Ağ operatörleri de bu hataları düzeltmek veya silmek için gereken önlemleri alacaklardır.*** | Bu madde, vatandaşlara kişisel bilgilerini korumaları için daha fazla hak tanımakta ve ağ operatörlerinin hataları zamanında düzeltme yükümlülüklerini artırmaktadır. |
| **46** | Bireyler veya kurumlar ***kendi ağlarının kullanımından sorumludurlar*** ve sahtekârlık yapmak amacıyla veya başka yasadışı faaliyetler için web siteleri veya iletişim grupları kurmayacaklardır. | Bu madde, bireylerin ve kurumların kendi ağlarının kullanımından sorumlu olduklarını vurgulamaktadır. |
| **76(5)** | "Kişisel bilgiler"terimi, bunlarla sınırlı kalmaksızın ve fakat bir ***gerçek kişinin*** ismi, doğum tarihi, kimlik numarası, kişisel biyometrik bilgileri, adresi ve telefon numarası da dâhil olmak üzere, o gerçek kişinin kim olduğunu tek başına ya da başka bilgilerle birlikte belirlmeyebilecek nitelikte olan ve elektronik ortamda veya başka yol ve araçlarla kaydedilen her türlü bilgiye atıf yapar. | Bu madde, kişisel bilginin korunmasının kapsamını "vatandaş"tan "doğal kişi"ye genişletmektedir |
| **63** | Kanun'un 27. Maddesini ihlâl eden ve siber güvenliği tehlikeye sokan faaliyetlere girişen insanlar, eylemin şiddetine bağlı olarak, 5 ile 15 gün arasında hapsedilebilirler ve ***100.000 RMB ile 1.000.000 RMB*** arasında para cezasına çarptırılabilirler. | Siber Güvenlik Kanunu'nun ihlâl etmenin azami cezası 1.000.000 RMB'ye artırılmış ve yükseltilmiştir. |
| Kaynak: Çin'in Siber Güvenlik Kanunu'na Genel Bakış | | |

Fakat CSL'ye de tabii ki itirazlar gelmektedir. The New York Times'ın Mayıs 2017'de bildirdiği gibi, "Avrupalı, Amerikan ve Asyalı şirketleri temsil eden ticari lobi gruplarının bir koalisyonu, Çin'den, bu Kanun'un yürürlüğe girişini ertelemesini istediler; Çin'deki Avrupa Birliği Ticaret Odası ise, şirketlerin 'önemli uyum yükümlülüklerinden' ötürü Kanun'a kendilerini adapte edebilmeleri için ek süre verilmesi talebinde bulundu."

İster AB'de, ister Çin'de, isterse veri mahremiyeti mevzuatı giderek artmakta olan bazı başka ülkelerde faaliyet göstersinler, kurumlar bu gelişmenin etkilerini hissetmektedirler. Yönetim kurulları kendi kurumları içinde yönetişim çerçevelerinin geliştirilmesi için baskı yapmaktadırlar ve yönetim kurullarına da genel süreçlerinin etkinliğinden onları sorumlu tutan düzenleyici otoriteler, yatırımcılar ve başta paydaşlar baskı yapmaktadırlar (Kurumsal Yönetişim, Risk Yönetimi ve İç Denetim başlıklı bölüme bakınız). Yeni mevzuat, risk yönetimi, kontrol ve yönetişim süreçlerinin karmaşıklık düzeyini artırarak maliyeti artırmakta ve kurumlara baskı yapmaktadırlar.

Yönetim kurulları üzerindeki baskı arttıkça, iç denetime de baskı yapılmaktadır. Kurumlar, iç denetime artık büyük beklentilerle bakmaktadırlar. Kurumlar,

## Denetim Odağı

**IIA Standart 2210: Görev Amaçları**

Her görev için uygun amaçlar belirlenmelidir.

**2210.A3 –** Yönetişim, risk yönetimi ve kontrolleri değerlendirmek için yeterli kriterlere gereksinim vardır. İç denetçiler, yönetimin ve / veya yönetim kurulunun hedeflere ve amaçlara ulaşılıp ulaşılmadığını belirlemek için yeterli kriterler tespit edip etmediğini değerlendirmeli ve anlamalıdırlar. Bu kriterler yeterli ise, iç denetçiler de değerlendirmelerinde bu kriterleri kullanmalıdırlar. Yeterli değilse, iç denetçiler yönetimle ve/veya yönetim kuruluşla müzakereler yoluyla uygun değerlendirme kriterleri belirlemelidirler.

**IIA Standart 2050: Koordinasyon ve Güvenmek**

İç denetim yöneticisi; aynı çalışmaların gereksiz yere tekrarlanmasını asgariye indirmek ve işin kapsamını en uygun şekilde belirlemek amacıyla, diğer iç ve dış güvence ve hizmet sağlayıcılarla bilgi paylaşmalı, faaliyetlerini koordine etmeli ve onların işlerine güvenmeli ve onlara danışmalıdır.

piyasa bozucu kuvvetleri fırsatlara dönüştürdükleri ve aynı zamanda da sürekli değişen mevzuata uymaya devam ettikleri için iç denetimin kendilerine tavsiye ve güvence hizmeti vermesinin öneminin farkına varmaktadırlar (KPMG İç Denetimi: 2016'de En Büyük 10 Risk başlıklı bölüme bakınız).

Piyasa bozucu kuvvetlere rağmen ayakta kaymanın anahtarı, yönetişim, risk yönetimi ve mevzuat uyumunu başarmak ve bir performans dengesi sağlamaktır. Bu güçlükleri aşmak, işin değerini koruyabilir ve hatta artırabilir ve operasyonel verimlilikleri iyileştirebilir.

### Amaçlar

- Projeleri ve stratejileri değerlendirirken risk iştahının açıklığa kavuşturulması gerekir.
- Güncel ulusal ve uluslararası mevzuat hakkında kurum çapında farkındalık yaratılması gerekir.
- Güncel ulusal ve uluslararası mevzuata uyumu sağlamayı amaçlayan tedbirler alınmalıdır.
- İç ve dış güvence sağlayıcıların eşgüdümü sağlanmalıdır.

### Eylemler

- Uluslararası uyum çerçevelerini ve güvence standartlarını anlamak.
- Mevcut düzenleyici organlar ve onların koşulları hakkında bir envanter çalışması yapmak.
- Kurumun yeni devralınan kurumların entegrasyona da dâhil global uyum faaliyetlerini yönetme konusundaki yaklaşımını değerlendirmek.
- Kurumun kayda değer aykırılık olayları ve eylemlerine verdiği cevabı ve karşılığı değerlendirmek.
- Uyum eğitim programlarını incelemek ve ilgili roller için uygunluğunu değerlendirmek.
- Aynı çalışmaların gereksiz yere tekrarlanmasını asgariye indirmek ve işin kapsamını en uygun şekilde belirlemek için iç ve dış güvence sağlayıcılarla eşgüdüm sağlamak.
- Bir uyum kültürünü teşvik etmek amacıyla kurumun ilgi ve önceliklerine uyarlanmış iletişim faaliyetlerini ustalıkla yönetmek.
- Kurumun sorumluluk ve görev dağılımını mevzuata uyum açısından değerlendirmek.

# Piyasa Bozulmalarına Cevap Vermek

Yeni bir gün — yeni bir zil, yeni bir düdük. Günümüzde teknoloji sürekli değişmektedir; artık daha hızlı, daha güçlü ve daha büyüktür (ve daha küçük); daha ileri menzillere ulaşmaktadır ve daha yoğundur. Hiç olmadığı gibidir artık. Her gün iç denetçiler paydaşlarına içgörü ve öngörü sağlamak için yeni fırsatlarla karşılaşmaktadırlar, fakat eleştirel düşünme ve yaratıcılık gibi inovasyonla ilişkili beceriler geliştirememiş olabilirler. Neticede, inovasyon

olmadan, kendilerini kayıtsızlığa karşı kırılgan ve beklenmedik şeyleri yapamayan bir halde bulmaktadırlar. İç denetciler metodolojilerini teknolojiden istifade edecek şekilde – daha çevik ve proaktif hale gelecek şekilde uyarlamalı ve inovasyona ayak uydurmak için gerektiğinde hızla yön değiştirebilmelidirler.

Yeni teknolojiler gibi inovasyonlar iç denetimin denetim görevlerini yerine getirebilmesi için büyük fırsatlar sunmalarına rağmen, pek çok durumda, inovasyona, iç denetimin endişe ve kaygılarına eklemeler yapan yeni riskler, tehditler ve *piyasa bozulmaları* da eşlik etmektedir. Örneğin, (geleneksel olarak) sadece riskler üzerine odaklanmak yerine, iç denetçilerin artık ileride meydana gelebilecek bozulmaları da hızla *tespit edebilmeleri* ve derhal veya ek ilgi gerektirenleri de fark edebilmeleri gerekmektedir.

Bir kurumun inovasyon yapmasını gerektiren ana sebeplerden biri de kendisini rakiplerinden ayırt edebilmektir – ve iç denetim bu konuda liderlik edebilir. 2018 Kuzey Amerika İç Denetimin Nabzı çalışmasına göre, inovasyon, iç denetime iki seçenek sunar: ya bir kurumda giderek önemi artan bir görevi yerine getirme kabiliyetlerini yeniden düşünmek ya da geçmiş uygulamaları kabul etmek ve onları geleceğe taşımak. Bu ikincisi neredeyse gelecekteki bir başarısızlığa karşı verilmiş bir garantidir; bu nedenle, iç denetim yaratacı (ve hatta radikal) fikirlere açık olmalı ve ilişkili risklerin etkin yönetimi üzerinde odaklanmaya hazır ve istekli olmalıdır.

Tabii ki zorluklar olacaktır. Yönetim, olayları farklı düşünme ve değerlendirme konusunda rahatsız olabilir; iş ortamı ve koşulları bütçeyi kısıtlamış olabilir ve aday havuzu ihtiyaç duyulan beceriler konusunda sığ olabilir. Fakat iyi haber şu ki, iç denetim tek başına ve yalnız değildir. İç denetim daha önce inovasyon sürecini yönetmek için spesifik teknikler geliştirmiş bulunan başka birimler, kurumlar veya iç denetim birimlerinden öğrenebilir.

İnovasyon — doğru yöntemle yapıldığında — hem iç denetim hem de tüm kurum için son derece değerlidir:

- Maliyetler azalır.
- Değer artışı sağlanır.
- Büyüme ve performans artışı gerçekleşir.
- Ürünler ve hizmetler daha erken piyasaya sunulur.
- Müşteri deneyimi ve tatmin düzeyi gelişir.
- Örgütsel esneklik ve çeviklik artırılır.
- Paydaş tatmini artırılır.

İnovasyon, sadece daha iyi ve daha etkin denetime imkan sağlamakla kalmaz, aynı zamanda bozulmaya karşı daha hızlı, daha akıllı ve daha odaklı bir cevap verdiği zaman çevikliği de doğrudan destekler (2018 Kuzey Amerika İç Denetimin Nabzı Araştırması: İç Denetim Dönüşüm Zorunluluğu başlıklı bölüme bakınız). IIA'nın Kuzey Amerika Yönetim Kurulu Başkanı Shannon Urban, iç

"İç denetimin kurumlarımızın başarısında çok önemli ve hayati bir rol oynadığına samimiyetle inanıyorum. Fakat aynı zamanda göreve uygun olabilmek için iç denetimde inovasyona bağlılığımızı tazelememiz gerektiğine de inanıyorum. İnovasyon, kurumlarımızdaki gelişmelere ayak uydurmak ve daha ötesine geçmek istiyorsa iç denetimin görev alanının tam ortasında yer almalıdır."

Shannon Urban, IIA Kuzey Amerika Yönetim Kurulu Başkanı (2017 – 2018)

Kaynak: Internal Auditor

denetimde inovasyonu hem büyüme için yaşamsal öneminden hem de paydaşların sürekli değişen gereksinimlerini karşılamak için gerekli olmasından dolayı teşvik etmektedir. Biraz rahatsızlık verici ve sinir bozucu olabilir, fakat devam etmektedir ve bağlılık ve cesaret ister. İnovasyon, çok ödüllendirici de olabilir. İç denetim, paydaşlarını anlamak ve onları geleceğe iyi hazırlamak istiyorsa, inovasyonu kucaklaması tek seçeneğidir (İnovatif İç Denetçi başlıklı bölüme bakınız).

## Amaçlar

- İç denetimin iş ortamındaki değişiklikleri fark etmesi ve anlaması gerekir.
- İç denetim, bir inovasyon kültürü geliştirmeyi ve kabiliyetlerini ve performansını güçlendirmeyi hedefler.
- İç denetim, inovasyon yoluyla elde edilebilecek gelişmeleri ve en iyi uygulamaları hedefler.
- İç denetim, inovasyon yoluyla etkinlik ve verimliliğini artırmak için çaba gösterir.

## Eylemler

- Yeni fikirler tasarlamak ve uygulamak ve inovasyonu iç denetim pratiğinin temel bir uygulaması ve merkezi yapmak.
- Liderlik rolü üstlenmek; işte olabilecek kesintileri önceden tahmin etmek; iş ortamındaki değişiklikleri izlemek ve daha geniş bir cevap yelpazesi sunmak.
- Yeni ilişkiler kurmak ve yeni ilişkilere yatırım yapmak. İşe bağlı kalmak ve inovasyonun yapıldığının ve gerçekleştiğinin farkında olmak.
- Hangi bozulmaların ek ilgi ve dikkat gerektirdiğini tespit ederek gelişen risk manzarasını ve resmini açıkça belirlemek.
- Piyasa bozuucu olaylarla bağlantılı yeni gelişen ve ortaya çıkan riskler etrafında bir bakış açısı ve içgörü sağlamak.
- Yeni veya gelişen risklere hızla ve kararlı bir biçimde cevap verebilmek için doğru yetkinlik ve uzmanlıklara sahip adaylar bulmak ve bu adayları cezbetmek.
- Başka risk yönetimi ve uyum fonksiyonları ve birimleriyle işbirliği yapmak.

# Kapanış Düşünceleri

Bu raporda ışık tutulan ve bahsi geçen riskler – IIA'nın global bağlı kuruluşları tarafından en temel kaygı ve endişe alanları olarak tanımlanmış olmalarına rağmen – kurumların veya iç denetimin karşılaştığı risklerin tümünü temsil etmemektedirler. Bu alanlara ek olarak, global bağlı kuruluşlar, denetim komitesine, bütçeye, savunma hatlarına ve stratejiye özgü ve bağlı riskler de tanımlamışlardır – örgütsel yönetişimin kabul edilmesi ve incelenmesi gereken tüm olmazsa olmaz şartları. Risk, bir kurumun misyonunu ve stratejik amaçlarını gerçekleştirememesine kapı açar ve kurumun toplam değerini tehdit eder. Bu sebeple, - risk yönetimi, kontrol ve yönetişim süreçlerine yardımcı olan güvenilir bir danışman olarak – iç denetimin sorumluluğu, tüm risk fırsatlarının değerlendirilmesini ve doğru tavsiyelerin yapılmasını gerektirir.

Dünya çapında, tüm kurumlar iç denetim birimine ve onun yaptığı değerlendirmelere güvenmektedirler. Yararlı olabilmek ve güvenilir bir danışman olarak kabul edilebilmek için, iç denetimin hem kendi amaçlarının hem de kurumun amaçlarının gerçekleştirilmesine engel olan riskleri düşünmek ve değerlendirmek gibi bir yükümlülüğü vardır. Bu sebeple, iç denetim sonuç-odaklı olmalı ve kabiliyetlerini bir bütün olarak kurumun yararına geliştirmeyi amaçlamalıdır. Bu da, eleştirel düşünmek; bağımsızlığını ve objektifliğini korumak; çevik kalmak; risklere – gerçek veya varsayılan – karşı *liderlik* üzerinde odaklanmak; gerektiğinde bir danışman olarak işlev göstermek suretiyle "zamanı" idare etmek ve tüm sistemler, süreçler, yönetmelikler ve operasyonların iç bağımlılıklarını anlamak da dâhil mevcut zorluklar ve engellerin ötesine çıkabilme kabiliyetine sahip olmayı gerektirir.

## IIA Global Bağlı Kuruluşları

**IIA Bağlı Kuruluşları, IIA'nın yapı taşlarıdır.** IIA, misyonunu yerine getirmek, iç denetim mesleğini daha da geliştirmek ve global düzeyde 190.000'den fazla üyesine hizmet etmek için 170'den fazla ülke ve bölgede kurulu IIA Bağlı Kuruluşlarıyla ortaklık etmektedir. IIA Bağlı Kuruluşları, kendi iç denetim toplumlarında etik ve mesleki uygulamalar konusunda yüksek standartları teşvik ederek toplu olarak iç denetim mesleğinin sesi olan tek yetkili IIA temsilcileri olarak faaliyet göstermektedirler.

## IIA Hakkında

Uluslararası İç Denetçiler Enstitüsü (IIA), iç denetim mesleğinin en tanınmış savunmanı, eğitmeni ve standart, kılavuz ve sertifika sağlayıcısıdır. 1941 yılında kurulan IIA, bugün itibariyle, 170'den fazla ülke ve bölgeden 190.000'den fazla üyeye hizmet etmektedir. Enstitü'nün global genel merkezi Lake Mary, Fla., ABD'de bulunmaktadır. Daha fazla bilgi için, www.globaliia.org adresini ziyaret ediniz.

## Sorumluluğun Reddi

Bu Global Perspektifler ve Anlayışlar dokümanında açıklanan fikirler, yayına bireysel katkıda bulunanların veya onların işverenlerinin fikirleri olmayabilirler.

## Telif Hakkı Uyarısı

The Institute of
Internal Auditors

globaliia.org