Üçüncü taraf kaynaklı teknoloji ve siber risklerinizi nasıl yönetiyorsunuz?

EY Türkiye Üçüncü Taraf Kaynaklı Teknoloji ve Siber Risk Yönetimi Değerlendirme Raporu

Kasım 2020

The better the question. The better the answer.
The better the world works.

Building a better working world

İçindekiler

Rapor hakkında

Günümüzün daha dijital, birbirine bağlı ve rekabete dayalı şartları altında, üçüncü taraf firmalar ile yapılan iş birlikleri, organizasyonlara üretim ve teslimat süreleri ile birlikte maliyetleri de azaltma imkânı sunmaktadır. Ancak, birbirlerine bağımlı bu ekosistemlerin, organizasyonlara müşteri deneyimi ve kârlı büyüme açısından büyük fırsatlar sunarken birçok yeni riski de beraberinde getirdiği gözlemlenmektedir.

Yaşadığımız dijital çağda, organizasyonların başarılı ve etkin bir şekilde faaliyetlerini yürütebilmeleri için, iş ve tedarik zinciri yönetimi açısından, karşı karşıya oldukları risklerden değer yaratacak kabiliyetlere sahip olmaları gerektiğine inanıyoruz.

Son zamanlarda birçok organizasyonun, siber saldırılar, veri ihlal vakaları, düzenleyici otoriteler tarafından uygulanan idari yaptırımlar ve hatta yürütülen yasal işlemler ile üçüncü taraf firma kaynaklı risklerle gündeme geldiğini görmekteyiz. Bu durum, ciddi itibar kayıplarına neden olarak müşterilerin organizasyonlara olan güvenini sarsmaktadır. Organizasyonlar rekabetçi piyasa koşullarında ayakta kalabilmek için sadece karşılaştıkları risklerin barındırdığı tehditleri yönetmekle kalmayıp, yine bu risklerin beraberinde getirdiği fırsatlardan da yararlanabilmelidir. Tüm bunlar göz önüne alındığında, güçlü ve sürdürülebilir bir üçüncü taraf risk yönetimi programına sahip olunması, organizasyonların birbirlerine olan bağımlılığının arttığı bu dönemde daha da kritik hale geliyor.

Bu bağımlılık, organizasyonların tabi olduğu yasal yükümlülükler bir yana, iyi bir yönetişim yapısının gereği üst yönetimleri, üçüncü taraf firma eylemlerinden de sorumlu hale getirmektedir. Örneğin; 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında verinin gizliliğinden ve güvenliğinden, veri sorumlusu organizasyon ve veri işleyen üçüncü taraf firma müştereken sorumlu hale gelmiştir.

Bu sorumluluk, üçüncü taraf firmaları denetleme gereksinimini ortaya çıkarmış ve böylelikle organizasyonların hem kendisini hem de diğer paydaşlarını güvence altına almalarını hedeflemiştir. Düzenleyici otoriteler tarafından yayımlanan mevzuat ve yönetmelikler de, üçüncü taraf firmalar ile yürütülen ilişkilerde hesap verebilirlik ilkesinin daimî olarak öncelikle organizasyonun kendisi ile ilişkili olduğunu göstermektedir.

Ayrıca, paydaşların ve düzenleyicilerin beklentileri uyarınca, organizasyonun dünyanın hangi noktasında tam olarak ne yaptığının, hangi üçüncü taraf firmaların organizasyon adına faaliyet gerçekleştirdiğinin ve bu faaliyetlerin neler olduğunun bilinmesi ve bunların kayıt altına alınması önem taşımaktadır.

Organizasyonun ve paydaşların çıkarlarını tehlikeye atan, sözleşmeye aykırı davranışların meydana gelmesi durumunda ise, taraflar arasında imzalanan sözleşme hükümlerine bağlı olarak her iki taraf için de geri dönüşü oldukça zor ve maliyetli sonuçlar ortaya çıkabilecektir.

Buradan hareketle üçüncü taraf firma risk yönetimi, dış kaynaklı ürün/hizmet tedariki yürüten ve yöneten bütün organizasyonları ve sektörleri doğrudan ilgilendirmektedir. Özellikle birçok düzenleyici yönetmelik, mevzuat ve standarda tabi olan bir sektör olması göz önüne alındığında, üçüncü taraf firma risk yönetiminin finans sektöründe ilk sıralarda yer aldığı gözlemlenmektedir (Bkz. 5 Kasım 2011 tarih ve 28106 Resmi gazete sayılı Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik).

EY Türkiye olarak, derlediğimiz bu raporun üçüncü taraf firma risk yönetiminin Türkiye ve dünyadaki uygulamaları, üçüncü taraf kaynaklı riskleri ve bunlara ilişkin geliştirilen önerileri, teknoloji ve siber riskler odağından detaylandırmayı hedefleyerek bu alanda kılavuzluk etmesini amaçlıyoruz.

Takip eden sayfalarda, öncelikle üçüncü taraf firma risk yönetimi alanında öne çıkan terminolojiyi açıklayarak üçüncü taraf firmalarla ilişkili öne çıkan riskleri ele alacak, ardından söz konusu üçüncü taraf firmalara duyulan ihtiyaçları detaylandırarak ilgili düzenlemeler, siber güvenlik ve veri güvenliği perspektifleri kapsamında bilgiler paylaşacağız. Sonrasında, üçüncü taraf firma risk yönetimi alanında gözlemlenen iyi uygulamalar göz önünde bulundurularak alınan önlemlerden bahsedecek ve bulut bilişim konusunu detaylandıracağız.

Keyifli okumalar dileriz.

Saygılarımızla,

Ümit Yalçın Şen
EY Türkiye Şirket Ortağı
Siber Güvenlik Hizmetleri Lideri

Yönetici özeti

Organizasyonlar, yapılarına ve önceliklerine göre birtakım hizmetlerini diğer firmalardan tedarik etmeye ihtiyaç duyarlar. Bu ihtiyaç, bazı organizasyonlar açısından yer yer yüzlerce, hatta binlerce tedarikçi ile küresel ölçekte çalışmayı gerektirmektedir. Bu nedenle, zaman içinde tüm ilgili üçüncü taraf firmaların bir risk yönetimi filtresinden geçirilmesi ve bunun için ayrı bir yönetim disiplini oluşturulması zorunlu hale gelmiştir.

Çalışılan üçüncü taraf firmalar, niteliklerine göre temizlik işlerinden şubeler arası nakit para transferine kadar pek çok farklı önem seviyesindeki konuda hizmet sağlamakta ve hizmetlerin gerçekleştirilmesi esnasında farklı riskleri de beraberlerinde getirmektedirler. Bu nedenle, risk yönetimi ve bu risklerin doğru bir şekilde tespiti ile gerekli kontrollerin sağlanması kritik önem taşımaktadır.

Organizasyonların operasyonel, stratejik, finansal ve itibar risklerini korumanın yanında kullandıkları teknolojinin, yazılımın ve bunlardan faydalanarak işledikleri verilerin güvenlik riski de büyük önem taşımaktadır. Dünyada ve ülkemizde birçok düzenleyici kurum tarafından belirli standartlar ve çerçeveler ile potansiyel ve mevcut riskleri kabul görmüş metodolojilerle yönetmek de organizasyonların kurumsal faaliyetleri arasında yer almaktadır.

İçinde bulunduğumuz, verinin değerinin giderek arttığı dijital çağda, NATO siber uzayı 5. savaş alanı olarak ilan etmiştir. Ülkeler bir diğeri hakkında ne kadar gizli veri toplarsa, kendilerini o kadar güçlü saymaktadırlar. Bu durum rekabetçi piyasada yer alan organizasyonlar için de geçerlidir. Bunu bir risk olarak tanımlayan bir organizasyonun teknoloji, siber güvenlik ve bilgi güvenliği risklerini de tanımlamış ve gerekli aksiyonları almış olması beklenmektedir. Gerekli teknolojik yatırımları yaparak kendi sistemlerini korumak bu işin başında gelse de hiçbir zaman %100 güvenliğe ulaşılamamaktadır. Burada önemli olan tüm varlıklarımızı kapsayan bir risk yaklaşımıyla riskleri tespit etmek ve gerekli tedbirleri almaktır. Bir organizasyonun en önemli varlıklarından biri olan tedarikçiler ise genelde üzerinde durulmayan ama en büyük risk kaynaklarının başında gelen paydaşlardandır.

Dünyada ve ülkemizde yaşanan birçok siber saldırının ve veri ihlalinin büyük bir kısmının üçüncü taraflar kaynaklı olduğunu görebiliriz. Özellikle bilgi güvenliği ve veri mahremiyeti kapsamında birçok mevzuat ve standart, birlikte çalışılan üçüncü tarafların denetimi maddesini içerse de yaşanan ihlallerin sebebini bu denetimlerin eksikliğinde bulabiliriz. Ülkemizde KVKK da organizasyonlara, veri paylaştıkları üçüncü taraf firmaları, kanunda veri işleyen olarak geçmektedir, denetleme hakkı vermiştir. Örneğin; bir banka, hizmet aldığı üçüncü taraf çağrı merkezini, veri merkezini, kullandığı üçüncü taraf yazılımları denetleme hakkına sahiptir ve tarafların imzaladığı sözleşmede tüm bunlar güvence altına alınmaktadır.

Üçüncü taraf firma risk yönetimi, üçüncü taraf firmaların kontrollerine, performansına ve aktivitelerine ilişkin göstergelerin takibini sağlayarak karşılıklı ilişkilerin daha iyi anlaşılabilmesini sağlar. Etkin bir yönetim ile risklerin, üçüncü taraf firmalar ile iş yapış maliyetini aşıp aşmadığı tutarlı bir şekilde değerlendirilebilir. Bu doğrultuda, organizasyonların, üçüncü taraf firma risk yönetimi yetkinliklerini etkin ve tutarlı bir biçimde tasarlayıp uygulamasına olanak sağlayan 10 öncelikli aksiyon derlenmiştir.

Organizasyonların üçüncü taraf firma risk yönetimi uygulamaları kapsamında; yönetişim ve gözetim yapısı kurgulaması, firma envanterini oluşturarak güncelliğini sağlaması, risk çerçevesini kurgulaması, risk yönetimi süreçlerini tasarlaması ve işletmesi, resmi politika ve standartları oluşturması, risk yönetimi çalışmalarına teknoloji desteğini sağlaması, teknik kontrolleri belirleyerek düzenli güvenlik değerlendirmeleri ve denetimleri gerçekleştirmesi, kişisel veri mahremiyeti düzenlemelerine uyum kontrolünün sağlanması, bahse konu etkin altyapıya ulaşmalarına yardımcı olacaktır.

Kısaltmalar

5651 sayılı Kanun	Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
APO	Align, Plan, Organize
BCR	Binding Corporate Rules (Tr. Bağlayıcı Şirket Kuralları)
BSA / AML	Bank Secrect Act/Anti Money Laundering
BT	Bilgi Teknolojileri
CCPA	California Consumer Privacy Act (Tr. Kaliforniya Tüketici Mahremiyeti Kanunu)
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology
DPIA	Data Privacy Impact Assessment (Tr. Kişisel Veri Etki Analizi)
DPO	Data Protection Officer (Tr. Veri Koruma Sorumlusu/Yöneticisi)
FCA	Financial Conduct Authority
FinCEN	Financial Crimes Enforcement Network
GDPR	General Data Protection Regulation (Tr. Genel Veri Koruma Tüzüğü)
HIPAA	Health Insurance Portability and Accountability Act
ISO	International Standards Organization (Tr. Uluslararası Standardizasyon Kuruluşu)
KVKK	6698 sayılı Kişisel Verilerin Korunması Kanunu
NIST	National Institute of Standards and Technology
OFAC	Office of Foreign Assets Control
PCI DSS	Payment Card Industry Data Security Standard
POS	Point of Sale
PRA	Prudential Regulation Authority (Tr. İhtiyati Düzenleme Kurumu)
SCRM	Supply Chain Risk Management (Tr. Tedarik Zinciri Risk Yönetimi)
SLA	Service – Level Agreement (Tr. Hizmet Seviyesi Anlaşması)
TPRM	Third Party Risk Management (Tr. Üçüncü Taraf Risk Yönetimi)
MITM	Man In the Middle (attack)

1

Üçüncü taraf firmalara duyulan ihtiyaç

Üçüncü taraf firmalara duyulan ihtiyaç gün geçtikçe artmaktadır ve organizasyonun iş süreçlerine dahil olması anından itibaren kendi risklerini de beraberinde getirmektedir.

Üçüncü taraf firma risk yönetimi disiplini, oluşan bu risklerin nasıl kontrol altına alınacağını araştırır. Bu kapsamda en sık başvurulan yöntemin **anket ile değerlendirme**[1] olduğu gözlemlenmektedir. Söz konusu anket yöntemi; doğrudan bir anket gönderimi şeklinde olabileceği gibi pratikte soru-cevap ile mülakat, karşılıklı ilişkilerin kullanımı gibi şekillerde de gerçekleşebilmektedir. Organizasyonlar ayrıca üçüncü taraf firmaları kendi iç denetçileri ya da bağımsız denetçiler yoluyla da denetleyebilmektedir.

Üçüncü taraf risk yönetimi uygulamasında kullanılmakta olan temel tanımlara bakılacak olursa; **tedarikçi, üretici, hizmet sağlayıcı** ve **üçüncü taraf** gibi terimlerin birbirinin yerine kullanıldığı sıkça görülmektedir.

Tedarikçiler, organizasyonun ana hizmet kaynağına doğrudan etki etmeyen ancak operasyonların başarılı bir şekilde sürdürülebilmesini sağlayan hizmetleri sunan organizasyonlardır. Örneğin; e-ticaret sitelerinde satılacak olan ürünlerin temin edildiği organizasyonlar tedarikçi konumundadır. **Üreticiler**, organizasyonların ana hizmet kaynağına doğrudan etki eden ürün ve hizmetleri sunan organizasyonlardır. Üretilen malın hammaddesinin satın alındığı organizasyonlar buna örnek verilebilir. **Hizmet sağlayıcılar** ise; veri işleme, operasyon, altyapı gibi hizmetleri organizasyonlara sağlayan organizasyonlardır. Personel servisleri, tesis güvenliği, temizlik gibi hizmetlerin temin edildiği firmalar buna örnek verilebilir. **Üçüncü taraf firma** kavramı, işte bu tedarikçi, üretici ve hizmet sağlayıcı firmaların tamamını kapsamaktadır.

Mevcut durumda tüm sektörleri ve organizasyonları farklı şekillerde etkileyen COVID-19 salgınından kaynaklanan ekstra tedarikçi ihtiyaçlarının yanı sıra, organizasyonlara güvenlik hizmetleri sağlayan tedarikçilerin de etkilenmiş olmasından dolayı organizasyonların normal operasyon seviyesinde hizmet sağlamakta zorlandığı görülmektedir[2].

Dış kaynak kullanımı arttıkça ve tedarik zinciri uzadıkça iş karmaşıklığı da artmaktadır. Özellikle finansal hizmetlerde, halihazırda uluslararası düzeyde düzenleyici otoritelerin de beklentilerinin arttığı görülmektedir. Örneğin; İngiltere'de bulunan İhtiyati Düzenleme Kurumu (PRA), dış kaynaklı operasyonel fonksiyonlar ve faaliyetler için Reçeteli Sorumluluk önermiş ve sigorta organizasyonlarının dış kaynak kullanımına ilişkin sorumluluk payını artırmıştır. Böylece, bu çerçevede iyi pazar uygulamaları gelişmeye devam etmekte, sigorta ve yatırım organizasyonları risk yönetimi süreçlerini sadece düzenleyici otoritelerin talep ettiği gereksinimleri karşılamak için değil, aynı zamanda hem müşterilerin hem de paydaşların çıkarlarını korumak için etkin bir şekilde yürütmektedir.

Son yıllarda üçüncü taraf risk yönetimi, global olarak artan maliyetler, dijitalleşme ve düşük faiz oranları ile dış kaynak kullanımının artması nedeniyle; sigorta ve yatırım organizasyonları için marjlar üzerinde aşağı yönlü baskı yaratan birincil endişe kaynağı haline gelmiştir. Dış kaynak kullanımına talebi artıran birçok fayda olsa da artan verimlilik ve ölçek, neticede üçüncü taraf ilişkilerinin risk seviyesini ve karmaşıklığını da arttırmaktadır. Buradan hareketle, uzayan anlaşma süreleriyle birlikte, söz konusu üçüncü taraf firmaların sürekli performans yönetimine olan ihtiyacının da artması kaçınılmazdır.

---

1 ISACA, 2016. Effective Third-Party Risk Assessment – A Balancing Process. [Çevrimiçi] Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/effective-third-party-risk-assessment-a-balancing-process

2 Gartner, 2020. Be Resilient: Prepare to Treat Cyber Risk Following the Coronavirus (COVID-19) Outbreak by Focusing on These 7 Areas. [Çevrimiçi] Available at: https://www.gartner.com/document/3983694?ref=solrResearch&refval=252530775

2 Üçüncü taraf firma kullanımının getirdiği riskler

Organizasyonlar üçüncü taraf firmalara tedarik, hizmet alımı ve diğer aşamalarda gittikçe daha fazla ihtiyaç duymaktadır. Bu nedenle üçüncü tarafların kullanımı ile öne çıkan riskler daha önemli hale gelmiştir. Günümüzde **üçüncü taraf firmaların** aynı zamanda **hizmet alan** taraf da olabildiği unutulmamalıdır. Bu kapsamda üçüncü taraf firmalardan kaynaklanabilen riskler aşağıdaki şekilde gruplanabilir:

Hukuki uyum riski: Özellikle sıkı düzenlemelere tabi sektörler açısından, çalışılan üçüncü taraf firmalar, konuya göre hukuki uyum konusunda daha fazla risk oluşturabilmektedir. Bankacılık, otomotiv, elektronik haberleşme gibi düzenlemelere sıkı bir şekilde tabi olup çok fazla tedarikçi, servis sağlayıcı ve iş ortağı gibi üçüncü taraf ile çalışan organizasyonların önemli miktarda kritik bilgi paylaşıyor olması, birtakım kontrollerin tesisini zorunlu kılmaktadır.

Özellikle bankacılık ve haberleşme gibi alanlarda hizmet veren organizasyonlarda uyum birimleri ile satın alma ve tedarik konusunda çalışan iş birimlerinin, söz konusu hizmet alım süreçlerinde birbirinden haberdar olmaları riskin doğru yönetimi açısından kritik önem taşımaktadır.

Operasyonel risk: Bu riskin kapsamına organizasyonların operasyonlarını etkileyen her tür risk girmektedir. Günümüz şartlarında buna verilebilecek en popüler örneklerden biri siber saldırı ile verilerin sızması riski olacaktır[3]. 2019 yılında veri sızıntısının bir organizasyona dünya ortalama maliyeti 26,844 Mio TRY ($3.92 Mio) olarak raporlanmıştır[4].

Veri sızıntısı ve etkileri

26,844 Mio TRY

2019 yılında veri sızıntısının bir organizasyona dünya ortalama maliyeti ($3.92 Mio)[4]

3 Aravo, 2017. [Çevrimiçi] Available at: https://www.aravo.com/blog/third-party-risk-a-unique-kind-of-operational-risk/, Ayrıca bknz: https://www.risk.net/risk-management/7450731/top-10-operational-risks-for-2020

4 IBM, 2019. Cost of a Data Breach Report. [Çevrimiçi].

Günümüzde toplanan verilerin fazlalığı ve özellikle kişisel veriler ile ilgili getirilen KVKK, GDPR, CCPA gibi global etki yaratan mevzuatlar sonucunda bu tip veri sızıntıları sonucunda operasyonel riskin yanı sıra uyum ve itibar risklerinin de ortaya çıktığı gözlemlenmiştir.

Operasyonel risk değerlendirilirken, tedarikçi risklerinin de mutlaka değerlendirmeye alınması gerekir. Aynı şekilde, tedarikçi riskleri değerlendirilirken de operasyonel riskler birlikte değerlendirilmelidir.

Operasyonel riske dair raporlar; denetim bulgularını, iş sürekliliği planlarını ve testleri, SLA'leri, bilgi güvenliğine dair bilgileri (Örn. üçüncü taraf TS EN ISO/IEC 27001:2017 lisanslı olması), finansal duyuruları vb. diğer bilgileri içermelidir.

İtibar riski: Çalışılmakta olan üçüncü taraf firmaların çalışma etiği ya da toplum nezdindeki itibarının durumu, organizasyonun kendi itibarına olası negatif durumların yansıması riskini doğurabilir.

Üçüncü taraf firmalarca sağlanan pek çok hizmetin ifası, itibar riski oluşturabilir. Sosyal medya pazarlaması ya da çağrı merkezi gibi doğrudan gerçek kişi olan müşteriye dokunan işler açısından bu durumun özellikle söz konusu olduğu görülmektedir.

Bu anlamda, reklam ajansları ya da çağrı merkezleri üzerinden gelebilecek hatalı bir geri bildirim ya da bir siber saldırıya uğraması (bkz. siber güvenlik riski) hallerinde, aynı zamanda itibar riski de oluşacaktır.

Bu tip bir ihtimalde hem saldırıya uğrayan organizasyon ticari zarar görecek, hem de hizmet alan organizasyonun itibarına yönelik bir risk oluşacaktır.

Siber güvenlik riski: Organizasyonların ticari bilgilerini, kişisel verilerini ve diğer önem arz eden bilgisini paylaştığı üçüncü taraf firmalar başta olmak üzere, tüm çalıştığı üçüncü taraflar açısından bir siber güvenlik değerlendirmesi yapması, kritik önem taşımaktadır.

Veri sorumlusu ve veri işleyen kavramları

Kişisel verilere dair kanun ve diğer mevzuatta **veri sorumlusu** (Data controller) ve **veri işleyen** (Data processor) olmak üzere iki kavram öne sürülmüştür.

Üçüncü taraf firmaların hizmet alan organizasyonlar açısından genellikle veri işleyen statüsünde kişisel veri işleyebildiği görülmektedir.

Veri işleyen, veri sorumlusunun (ki bu taraf hizmet alan organizasyon olabilir) izin ve yetkilendirmesi sonucunda, veri sorumlusuna ait olan kişisel verileri kullanan, bu kişisel verileri saklayan, duruma göre imha eden ya da doğrudan bir sisteme girişini yapan taraftır.

Veri sorumlusu ve veri işleyen gerek **6698 sayılı Kişisel Verilerin Korunması Kanunu'**nda, gerekse diğer uluslararası mevzuatta ayrı ayrı sorumlu olarak kabul edilmektedir.

Bir başka deyişle **veri işleyen üçüncü taraf firma** tarafında gerçekleşecek bir risk, **veri sorumlusu olan hizmet alan organizasyon** tarafında operasyonel bir riskin gerçekleşmesine neden olabilecektir.

> "Güvenlik konusuna önem veren ve güvenliğin sağlanması konusunda adım atan organizasyonlar, hem kısa hem de uzun vadede çok önemli ticari faydalar görecektir.
>
> **Dave Burg**
> **EY Amerika Siber Güvenlik Lideri**

Siber güvenlik riskleri göz önüne alındığında, organizasyonların çalıştığı tüm üçüncü taraflara yönelik bir güvenlik değerlendirmesi yapması ve uyum aksiyonlarını hayata geçirmesi kritik önem taşımaktadır.

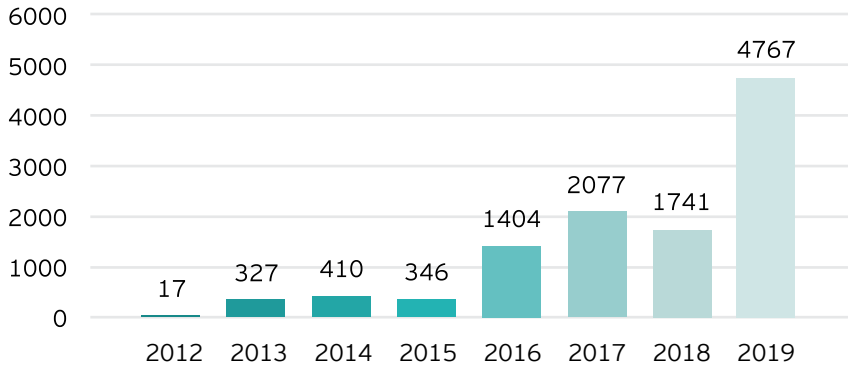
Siber güvenliğe dair risklerde aşağıdaki aksiyon ve süreç adımları ön plana çıkmaktadır:

- Yüksek risk teşkil eden aktivitelerin belirlenmesi
- Kontrollerin hiyerarşik olarak "yukarıdan aşağı" yönlendirilmesi
- Sistemlerin ve bilgi varlıklarının korunmasına yönelik kontroller
- Güncel vaka müdahale süreçlerinin oluşturulması
- İç kontrol ve denetim mekanizmaları
- İş ve bilgi teknolojileri sürekliliği
- Veri güvenliği ve veri koruma stratejilerinin belirlenmesi ve organizasyon düzeyinde uygulanması

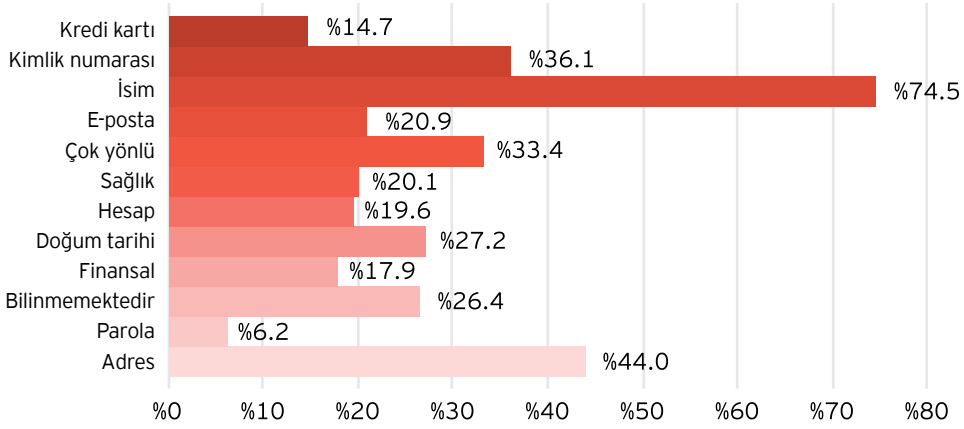
Risk Based Security'nin her çeyrek periyotta yayımladığı Veri Sızıntısı Raporu'na göre, 2018 yılına göre 2019 yılı içerisinde tedarikçiler üzerinden sızan verilerin hacmi %273 artmıştır. Özellikle fazla sayıda tedarikçi ile çalışan sektörler açısından üçüncü taraf firmaların siber güvenliğe ilişkin almış olduğu tedbirlerin sorgulanması bu nedenle kritik önem taşımaktadır.

En son 2014 yılında ciddi şekilde yükseldiği tespit edilmiş olan veri ihlali bildirimlerinin, özellikle GDPR'ın yürürlüğe girmesinden sonra tekrar artma eğilimine girmiş olduğu gözlenmektedir.

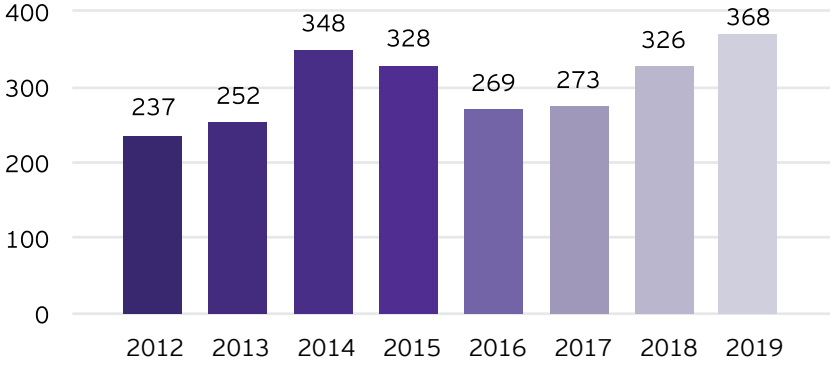
2019'da bildirilen üçüncü taraf veri ihlallerinde kaybedilen kayıt sayısı (milyon)[5]



2019'da bildirilen üçüncü taraf veri ihlallerinden dolayı kaybedilen veri türleri[5]



2019'da bildirilen üçüncü taraf ihlallerinin sayısı[5]



5 Risk Based Security, 2019 Year-End Data breach QuickView Report

Bulut bilişim risklerinin gündemdeki yeri hızlıca yükselmektedir. Günümüz şartlarında, salgın ve getirdiği **yeni normal** durumu göz önüne alınarak bulut teknolojileri kullanımının artmasıyla bu hususun özellikle değerlendirilmesi uzmanlarca önerilmektedir. Bu noktada organizasyonlar, kendileri bulut teknolojilerini kullanmasa da tedarikçilerinin ve diğer üçüncü taraf firmaların bulut teknolojilerini kullanması durumunda karşı karşıya kalınabilecek riskleri mutlaka değerlendirmelidir.

Özellikle bulut kullanımından doğan riskler başta olmak üzere, teknoloji temelli altyapı riskleri incelenirken aşağıdaki hususlar dikkate alınmalıdır:

- Kullanılmakta olan ya da kullanılacak olan bulut çözümünün uyum durumu
- Kimlik hırsızlığına karşı kontroller
- İnsan hatalarını minimize etme amaçlı kontroller geliştirilmesi
- DDoS ve IoT-botnet türevi saldırılara karşı önlemler

Teknoloji riskleri: Organizasyonların sağladığı hizmetler ve duydukları ihtiyaçlara göre teknoloji kaynaklı riskler değişkenlik gösterebilir. Bu kapsamda belli başlı risklerin organizasyonlar tarafından tespit edilerek gerekli görülen önlemlerin alınması kritik önem taşımaktadır.

- **Erişim riski,** en önemli teknoloji risklerinden biri olarak kabul edilmektedir. İş birimlerinin kullanmakta olduğu ana operasyona dair yazılımlara erişilememesi halinde **ciddi maddi kayıplar** yaşanabileceği gibi itibar riski de söz konusu olabilir. Bu açıdan teknolojiye erişim riski beraberinde birden fazla zarar kalemi getirebilir.
- Yazılım geliştirme operasyonu olan organizasyonlar açısından da birtakım riskler söz konusudur. Yazılım geliştirme operasyonlarını üçüncü taraf firmalar aracılığıyla gerçekleştiren organizasyonların özellikle sözleşme metinlerinde dikkatli hareket etmesi gerekmektedir.
- Bu tip organizasyonlar açısından kaynak kodu yönetim sistemi kullanımından doğabilecek birtakım riskler ve dışarıdan kaynak kodlarına eklenebilecek **kötü niyetli kodlara** dair riskler söz konusu olabilir.
- Yazılım geliştirme operasyonlarında ayrıca, **geliştirilen yazılımın canlı ortama alınması** aşamasında birtakım riskler söz konusudur. Programın yanlış sürümünün canlı ortama alınması ya da yeterli test yapılmamasından kaynaklanan problemler bunlara örnek verilebilir.
- Bunlara ek olarak organizasyonların güncel ve yeterli bir **felaket kurtarma yapısına** sahip olmaması da ciddi bir risk oluşturacaktır. Felaket kurtarma senaryolarının güncel tutulmaması ya da planlarda meydana gelebilecek yetersizlikler, olası bir felaket durumunda ciddi zararlara yol açabilir.

Finansal riskler iki şekilde ortaya çıkabilir: Ekstra masraflar ve elde edilemeyen kar.

- **Ekstra masraflar** açısından öncelikli olarak organizasyonların etkin satın alma süreçleri ve dikkatli fiyatlandırma ile bu masrafları en aza indirmeye çalıştıkları görülmektedir.
- **Elde edilemeyen kar riski** ise, organizasyonların kar üreten süreçlerinde destek aldıkları üçüncü taraf firmaların eksik ve/veya hatalı operasyonları nedeniyle ortaya çıkabilen bir risktir. Çeşitli nedenlerle ödemelerde yaşanabilecek gecikmeler bu tip risklere örnek olarak verilebilir.

Üçüncü taraf firma risk yönetimi sürecini genel olarak örneklemek gerekirse aşağıdaki 5 madde değerlendirmeye alınabilir:

- Riskin tespiti
- Riskin değerlendirmesi/ölçümü
- Kontrollerin belirlenmesi ve uygulanması
- Sürekli gözlem ve inceleme
- Raporlama

3 Üçüncü taraflar firmalar ve siber güvenlik

2013'te, ABD merkezli büyük bir perakendecide önemli bir üçüncü taraf siber risk olayı meydana gelmiştir. Oltalama amaçlı bir kampanya (phishing campaign) ile perakendecinin ısıtma, havalandırma ve klima (HVAC) yüklenicisinin sistemlerine Citadel adlı trojan bulaşmış ve saldırganlar bu sayede yüklenicinin sistemleri üzerinde tam kontrol sahibi olmuştur. Çeşitli siber saldırı teknikleri ile saldırganlar yüklenicinin perakendecisine ait faturalandırma ve proje yönetim sistemlerine erişebildiğini keşfetmiştir. Bir perakendecinin satış noktası sistemlerine (POS) sızmayı başaran saldırganlar yaklaşık 100 milyon müşterinin kredi kartı verilerini ele geçirmiş ve 1,4 Mia TRY mali kayba sebep olmuşlardır[6].

POS sistemlerine ilişkin ihlal sonuçları[6]

100 Mio
etkilenen müşteri adedi

1,4 Mia TRY
mali kayıp ($200 Mio)

Bir perakendecinin satış noktası sistemlerine (POS) sızmayı başaran saldırganlar müşterilerin kredi kartı verilerini ele geçirmiştir[6].

Yukarıdaki bahse konu bu ihlal, organizasyonların üçüncü taraf riskini göz önünde bulundurmamış birçok yönetici için bir ders olarak alınıp, ağlarındaki hangi üçüncü tarafların benzer bir ihlale neden olabileceğini de incelemelerine olanak sağlamıştır. Örnekte belirtilen oltalama saldırısı kullanıcıların e-posta adreslerine alışveriş kampanyası göndererek kullanıcıların sahte web sayfalarına yönlendirilmesi ile verilerinin ele geçirilmesinin amaçlandığı bir çevrimiçi saldırı türüdür. Saldırganların organizasyonları doğrudan hedeflemeyip, sosyal mühendislik, ortadaki adam (MITM) saldırıları, kimlik avı kampanyaları, fidye yazılım gibi daha birçok saldırı yöntemi ile organizasyonların çalıştığı üçüncü taraf firmaları hedef aldıkları dünyada yaşanan veri ihlallerinin büyük bir kısmında görülmektedir. Buna ek olarak hem kişisel hem de kurumsal verileri hedefleyen birçok saldırı çeşidi olmakla birlikte, güvenlik tedbirleri ile mevcut risklerin azaltılması mümkündür. Özellikle, üçüncü taraflar ile ortak kullanılan müşteri yönetimi, tedarik zinciri yönetimi, destek hizmetleri ve diğer sistemlerin risk analizlerinin yapılması büyük önem taşımaktadır. Sistemler üzerindeki erişim yetkilerinin düzenlenmemesi, zayıf parola kullanımı, güvenlik araçlarının konfigürasyonlarının eksik ya da hatalı yapılmış olması bu sistemlerdeki zafiyeti artırarak risk ve tehdit unsurunu da artırmaktadır.

6 Managing Third-Party Risk: Cyberrisk Practices for Better Enterprise Risk Management, ISACA & OneTrust VendorPedia,2019

Siber güvenlik alanından bakıldığında, fidye yazılımları (ransomware) gibi zararlı yazılımların birçok küçük ve orta ölçekli organizasyonu zora soktuğu gözlemlenmektedir. 2018 yılında bu tür yazılımların ticari sektöre maliyeti ortalama 59 Mia TRY ($8,5B) olmuş[7] ve 2019 yılı için bu tutarın ortalama 79,7 Mia TRY ($11,5 Mia) civarlarına yükseldiği gözlemlenmiştir. 2021 için ise bu maliyetin yaklaşık 138,6 Mia TRY ($20 Mia) olabileceği öngörülmektedir[8].

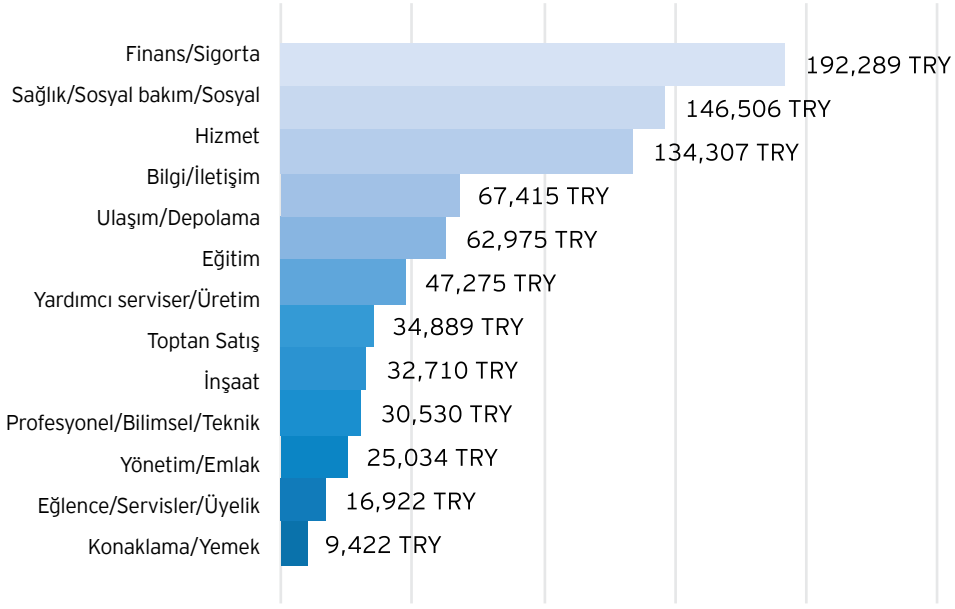
Zararlı yazılımların ticari sektöre maliyeti[7]

59 Mia TRY
2018 yılındaki maliyet

79,7 Mia TRY
2019 yılı için öngörülen maliyet

Siber güvenlik ihlalleri ve saldırılarının oluşturduğu zararlara ilişkin önlemlerin alınabilmesi için ise, organizasyonların bu alanda yatırım yaptığı gözlemlenmektedir. Bu doğrultuda, ortalama 192,289 TRY ortalama tutarındaki yatırımla (£22.050) **Finans/Sigorta Sektörü** 2019'da siber güvenliğe en çok yatırım yapan sektörler arasında yer almaktadır.

İngiltere'de İş Sektörü Gruplaması tarafından yapılan 2019 yılındaki siber güvenliğe ortalama yatırım, 2019[9]



Burada dikkat çeken bir diğer konunun kullanıcı farkındalığı olduğunu vurgulamak faydalı olacaktır. Yapılan yatırımların yanında, kullanıcıların farkındalığının düzenli eğitimlerle ve yapılan testlerle artırılması ve yatırım yapılan siber güvenlik çözümlerini yönetecek kalifiye kişilere de ihtiyacın olduğunu görülmektedir.

7 Güvenlik Portali, U. I., & Bicakci, S. (2019). Siber Güvenlik ve Savunma. ResearchGate.

8 AON, 2020. 2020 Cyber Security Risk Report, s.l.: AON PLC.

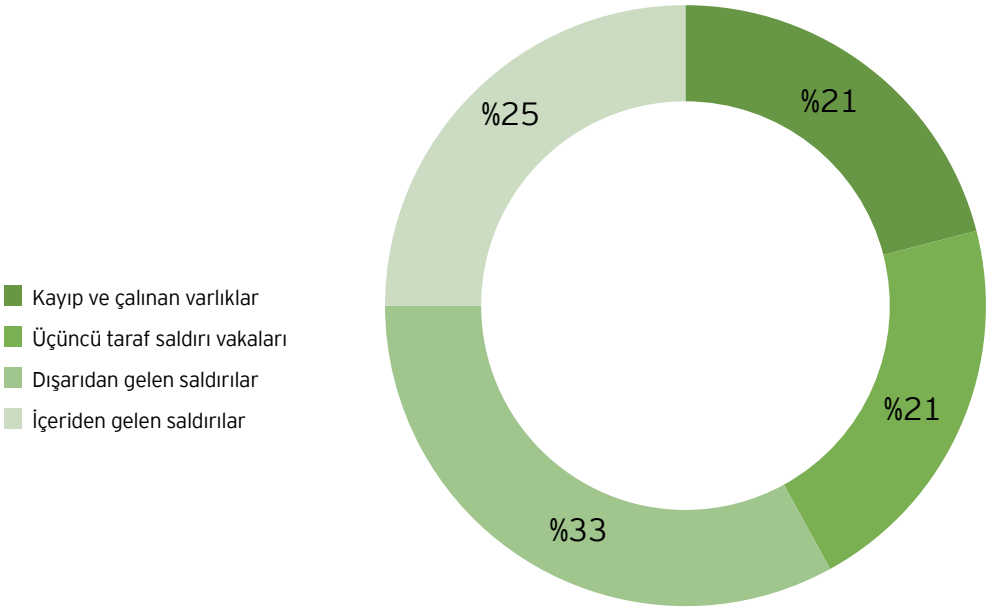
9 https://www.digitalmarketingcommunity.com/indicators/cyber-security-investment-2019/

4 Üçüncü taraflar ve veri güvenliği

Üçüncü taraf firma kaynaklı veri ihlalleri

Güvenlik teknoloji uzmanları tarafından cevaplanan global bir ankette 2019'da bilinen ihlallerin %21'inin üçüncü taraf firma kaynaklı ihlaller olduğu belirtilmiştir[10]. Büyük risk barındıran genişletilmiş ekosistemler üçüncü taraf firmaya bağlı olduğunda, müşterilerin ve diğer paydaşların hiçbirinin, ihlale sebep olan üçüncü tarafı hatırlamayacağı, sadece ana organizasyonun itibarının zedeleneceği düşünülmektedir. Bu sebeple daha sağlam bir güvenlik kültürü oluşturmak için insanlara odaklanılmalıdır. Bu, potansiyel ve mevcut müşterilerin yanı sıra yönetim kurulu, güvenlik personeli, çalışanlar ve üçüncü taraf ortaklar ve tedarikçiler için de dikkate alınmaktadır. Bunun önüne geçip daha sağlam bir güvenlik kültürü oluşturmak için ise, bütçe ve olgunluk değerlendirmeleri, yeni teknoloji incelemeleri, organizasyon için iletişim, güvenlik ve mahremiyet programlarına ek olarak insanlara odaklanmanın 2020 trendleri arasında olduğu görülmektedir. Bu, potansiyel ve mevcut müşterilerin yanı sıra yönetim kurulu, güvenlik personeli, çalışanlar, üçüncü taraf ortaklar ve tedarikçiler için dikkate alınmaktadır.

2019'da bilinen ihlallerin sebepleri[11]



10 Shey, H., DeMartine A. et al (2020), The State of Data Security and Privacy, Forrester

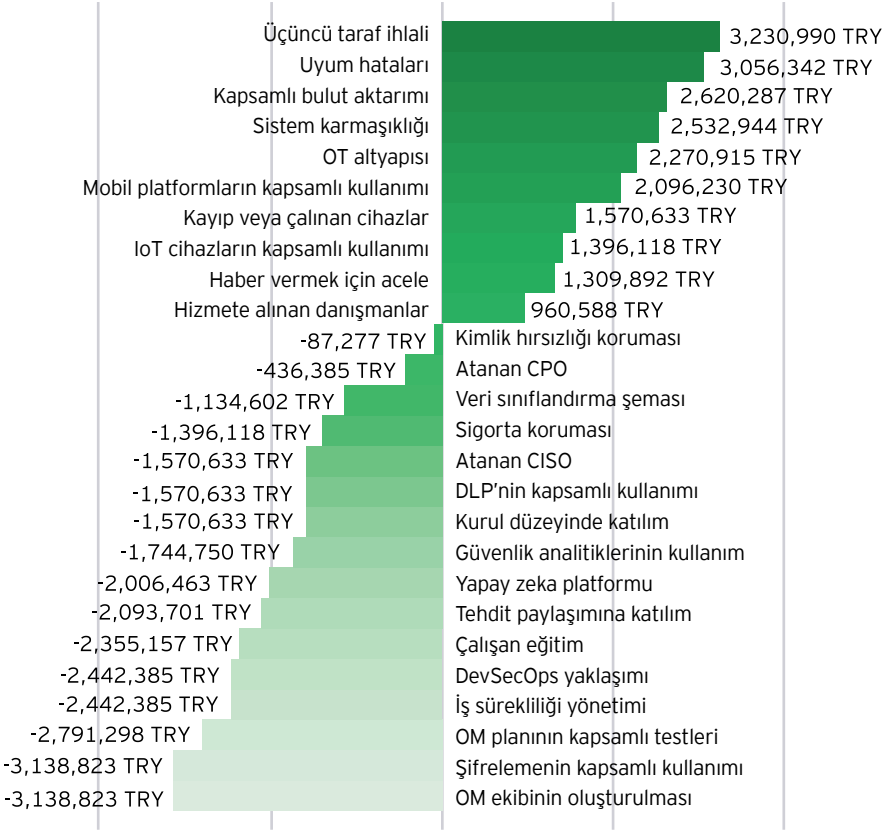
11 Forrester Analytics Global Business Technographics® Security Survey, 2019

Yapılan incelemelerde veri ihlalinin 27,3 Mio TRY ($3,92 Mio) ortalama toplam maliyetini belirlenen 26 faktörün içinden en çok artıranın üçüncü taraf veri ihlalleri olduğu ve uyum hatalarının bunu takip ettiği görülmektedir[12].

Organizasyonların %59'unun üçüncü taraflardan birinin neden olduğu bir veri ihlali yaşadıkları bilinmektedir. ABD'de bu oran %61 olmakla birlikte, geçen yılki çalışmalara göre %5 ve 2016'dan beri de %12 artış göstermektedir. Bu veriler, son 12 ay içinde yaşanan ve **sadece tespit edilebilen** veri ihlallerini göstermektedir. Küreselleşme daha fazla birbirine bağlı tedarik zincirlerinin oluşmasını gerektirdiğinden, bu oranlarda artış beklenmesi yanlış olmayacaktır.

Ponemon Institute araştırmasına göre veri ihlallerinde organizasyonlara yansıyan toplam maliyeti artıran en önemli unsurlardan biri olarak 'uyum hataları' olarak göze çarpmaktadır. Uyum hatalarını buluta kapsamlı seviyede aktarım, sistemlerdeki karmaşıklık, ve teknolojik altyapı takip etmektedir. Buna karşılık maliyetleri düşüren en önemli unsurların ise sigorta ile tamamen koruma sonrasında bir veri sınıflandırma şeması çıkarılması olduğu görülmektedir. Veri sınıflandırmasını CPO atanması, kimlik hırsızlığını önlemeye yönelik koruyucu önlemler takip etmektedir.

Veri ihlallerinde organizasyonlara yansıyan toplam maliyeti artıran ve azaltan unsurlar[12]



Genel olarak bakıldığında, organizasyonların dörtte üçünden fazlası üçüncü taraf kaynaklı siber güvenlik olaylarının arttığı konusunda hemfikir durumdadırlar. Bu artışa sebep olan önemli bir faktör üçüncü taraf bilgi sistemleri ortamlarının artan karmaşıklığı ve yönetim zorluğudur. Organizasyonların üçüncü taraf firmalara olan bağımlılıkları artmaya devam ederken, gizli ve hassas bilgilerin yaklaşık ortalama 583 adet üçüncü taraf firma ile paylaşıldığı görülmektedir. Organizasyonların sadece %34'ünün üçüncü tarafların envanterini tuttuğu anlaşılmakta olup, dördüncü, beşinci, altıncı vb. taraflar için (alt yüklenicilerin alt yüklenicileri ve onların alt yüklenicileri gibi) ise bu organizasyonların sadece %15'i tarafından envanter çalışması yürütüldüğü gözlemlenmiştir.

Birçok organizasyon tarafından envanter kaydı yapılamamasının temel sebebi olarak **merkezi kontrol eksikliği** kabul edilmiş, diğer önemli nedenler arasında ise **kaynak yetersizliği** ve **üçüncü taraf firma ilişkilerinin karmaşıklığı** yer almıştır[11].

12 Ponemon Institute, 2018. Data Risk in the Third-Party Ecosystem, UK: Opus.

Üçüncü taraflar ile KVKK ve GDPR uyumu

Organizasyonların KVKK ve/veya GDPR ile uyumlu olması ne kadar önemliyse, ilişki kurulan üçüncü taraf **veri işleyen**lerin de bu düzenlemeler ile uyumlu olup olmadığı aynı ölçüde önemlidir. Önceki **95/46 Sayılı Direktif** (AB Veri Koruma Direktifi) uyarınca, veri ihlallerinden yalnızca veri sorumluları sorumlu iken; KVKK ve GDPR, veri işleyen üçüncü taraf firmaları da veri gizliliği ihlallerinden sorumlu hale getirmiş durumdadır. Sonuçta, bir kontrolör/veri sorumlusu, kişisel verilerin ilgili mevzuata uygun olarak işlenmesini sağlamak ile sorumludur. Böylece veri sorumlusunun, veri işleyenin söz konusu mevzuata uyumlu hareket ettiğinden emin olması veya para cezaları da dahil olmak üzere düzeltici önlem ve yaptırımlardan sorumlu olabileceğini bilmesi gerekir. Kişisel veri ihlali yaşanan bugüne kadarki en büyük mali yaptırımlardan bazıları, üçüncü taraf hatalı eylemleri sonucunda meydana gelmiş ve büyük maliyetli yaptırımlara sebep olmuştur. Dünya çapında faaliyet gösteren hukuk danışmanlığı firması CMS tarafından tutulmakta olan GDPR ceza takip tablosuna göre, 2019 yılı sonunda GDPR ile ilgili yaptırımlar toplamda ortalama 3,5 Mia TRY (€429 Mio) tutarını geçmiştir. Temmuz 2020 itibarıyla bu meblağın 3,5 Mia TRY (€429 Mio) üzerine çıktığı gözlemlenmektedir[13].

Türkiye'de Kişisel Verileri Koruma Kurulu tarafından verilen kararlara bakıldığında, üçüncü taraf firma kaynaklı veri ihlallerinin etkilerinin büyük olduğu görülmektedir. Örneğin; satış sonrası destek hizmeti veren bir organizasyonun sistemlerine yetkisiz erişim sonucu veri ihlali yaşaması ile birlikte hizmet verdiği birçok organizasyonun da yaşanan ihlalden etkilendiği Kurul'un internet sayfasında duyurulmuştur. Kurul kararlarından da görüleceği üzere hem kamuda hem de özel sektörde bu alanda ciddi etkileri olan ihlaller yaşanmaktadır[14].

Üçüncü taraf bir veri işleyen, KVKK ve GDPR kapsamında "kişisel verileri bir veri sorumlusu adına işleyen gerçek veya tüzel kişi veya kuruluş" olarak tanımlanmaktadır. Bu kavram aslında organizasyonlar adına kişisel verileri işleyen üçüncü taraflar anlamına gelmektedir. Çalışılan bulut teknoloji hizmet firmaları, altyapı ve sistem barındırma ve e-posta organizasyonları, çağrı merkezleri, pazarlama ve reklam ajansları, hukuk büroları ve kişisel verilerin ticari faaliyetlerinin veya yürütmekte olunan herhangi bir projenin bir parçası olarak paylaşıldığı diğer organizasyonlar bu kapsamda sayılabilir. Bu bağlamda veri sorumluları, veri işleyenler tarafından gerçekleştirilen işlemlerden sorumludurlar. Bu nedenle, ilişki kurulan tüm veri işleyenler tanımlanmalı, saklanan ve paylaşılan veriler net bir şekilde anlaşılmalı ve her veri işleyenin bu verilere uyguladığı güvenlik kontrolleri dahil gizlilik politikaları ve kullanım koşulları değerlendirilmelidir.

13 https://www.enforcementtracker.com/?insights

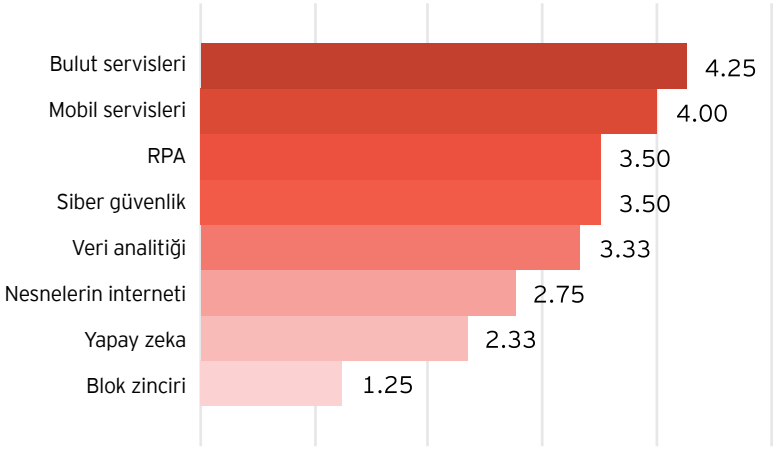
14 https://www.kvkk.gov.tr/Icerik/5419/Kurul-Kararlari

Üçüncü taraf riskleri ve bulut bilişim

Bulut bilişim kullanımına ilişkin Avrupa'da karşılaşılan özel uygulamalar ve engeller

Bulut bilişim, istenildiği anda veri depolama ve işleme kapsamında alternatif bir model sunarak, verilerine ve uygulamalarına internet erişimi olan herhangi bir cihazdan ulaşma imkânı tanıdığından, geleneksel alternatiflere nazaran daha hızlı, daha ucuz ve daha esnek çözümler sunmaktadır. Ayrıca yapay zekâ, yüksek performanslı programlama, nesnelerin interneti (IoT) ve blok zinciri (blockchain) teknolojisi gibi gelişen teknolojilere erişimi sağlayan ana kanal rolünü üstlenmektedir[15]. Bu anlamda diğer teknolojilere nazaran bulut bilişimi sistemlerinin üçüncü taraf firma risk yönetimi üzerinde etkileri kuşkusuz ki yüksek olacaktır. Aşağıdaki şekil ile özetlendiği üzere, **Centre for Outsourcing Research and Education** (CORE) tarafından 2019 yılında yürütülen araştırmalar göstermektedir ki, bahse konu dijital servislerin üçüncü taraf firmalarca yönetişimi ve yönetiminin, başarılı bir dış kaynak sözleşmesi için gerekli olarak değerlendirildiği gözlemlenmekte, ancak bulut servislerinin bu konudaki olgunluğu ve önemi diğerlerine göre öne çıkmaktadır[16].

Dijital servisler için üçüncü taraf firma yönetişimi ve ilişki yönetimi olgunluğu[16]



15 European Commission, 2019. Cloud Computing: A Different Way of Using IT, s.l.: European Union

16 Babin, R., 2020. Governing Vendors for Transformation: Getting the Most from Third-Party Relationships, s.l.: IDC.

Bulut bilişimin geniş kapsamlı sınırları göz önüne alındığında, ilgili ürün ve servislerin güvenilirliğinin ve siber güvenlik, karşılıklı çalışabilirlik imkanı, taşınabilirlik ve pazar davranışına uyumunun sağlanması için Avrupa'da aşağıda listelenen bazı özel uygulamalar yürürlüğe konmuştur:

- **The Free Flow of Non-Personal Data Regulation:** Kişisel veri olmayan verilerin Avrupa Birliği içerisinde serbest akışına ilişkin regülasyondur.
- **General Data Protection Regulation (GDPR):** Avrupa Birliği hukukunda, gerçek kişiler için veri koruma ve gizliliğine ilişkin bir yönetmeliktir.
- **The European Data Flow Monitoring Initiative:** Avrupa Birliği sınırlarında veri akışlarının haritalanmasına aracı olmaktadır.
- **Digital Single Market (DSM) Cloud Stakeholder Working Groups:** Siber güvenlik, kişisel veri olmayan verilerin serbest akışı, bulut bilişim gibi konulara ilişkin olarak oluşturulan çalışma grubudur.
- **European Commission Cybersecurity Certification Schema:** Bilşim ve iletişim teknolojileri alanındaki dijital ürünler, servisler ve süreçlere yönelik risk bazlı AB sertifikasyon çerçevesidir.

Bu doğrultuda bulut bilişim alanında verinin hareketliliğine ilişkin olarak karşılaşılan engeller aşağıdaki gibidir:

- Üye ülkelerin kamu otoriteleri tarafından verinin yerel hale getirilmesindeki kısıtlamalar
- Verinin BT sistemleri arasında hareketine yönelik engeller (örneğin; satıcıya bağımlılık)
- Sınır ötesi veri depolama ve işleme faaliyetlerine temkinli yaklaşmaya sebep olan hukuki belirsizlik
- Verinin sınır ötesi erişebilirliğine yönelik güvenlik riskleri ve endişeleri sebebiyle güven eksikliği

Türkiye'de bulut bilişim

Bulut bilişim alanında Türkiye'deki duruma bakıldığında, organizasyonlar tarafından kullanılan BT servislerinde artık yavaş yavaş bulut bilişim dönüşümüne gidildiği gözlemlenmektedir. Örneğin; altyapı hizmetleri alanında **Hizmet Olarak Altyapı** (IaaS), uygulama hizmetleri alanında ise **Hizmet Olarak Yazılım** (SaaS) ürünleri tercih edilebilmektedir. Geleneksel BT servisleri bile artık sistem entegrasyonları içerebilmekte veya profesyonel hizmetler bulut bileşenlerini kapsayabilmekte; bulutla ilişkili proje hizmetleri artık **Profesyonel Bulut Hizmetler** (Cloud Professional Services) olarak ifade edilmektedir.

Türkiye'de 2018 ve 2023 seneleri arasında Bulut'la ilişkili servislere yönelik gerçekleşen ve tahmin edilen harcalamalara aşağıdaki tablo aracılığıyla ulaşılabilecektir.

Türkiye'de Bulut'la ilişkili servislere (Halka açık, gizli, karma) yönelik harcamalar 2018-2023 (M TRY)[17]

	2018	2019	2020	2021	2022	2023	2018-2023 CAGR (%)
Profesyonel hizmetler	352.144	432.308	480.091	530.742	563.053	636.712	86.2549
Yönetilen bulut	145.058	179.423	201.808	225.083	250.001	277.376	94.4665
Destek ve eğitim	112.470	137.729	153.880	170.993	186.326	204.329	86.9335

17 Eser, E., 2019. Turkey IT Services Market 2019–2023 Forecast and 2018 Analysis, s.l.: IDC.

Bulutla ilişkili hizmetler, halka açık, gizli ve karma olacak şekilde son kullanıcılara ulaştırılmakta olup, Türkiye BT servisleri pazarındaki uygulamaları göreceli olarak küçük bir orandadır (2018 yılında %7.7); nitekim 2023 yılına doğru artış göstererek %10'a yükselmesi öngörülmektedir.

Türkiye'de Bulut'la ilişkili hizmetler[18]

%7.7

2018 Türkiye BT servisleri pazarındaki Bulut uygulamalarına ilişkin oran

%10

2023 Türkiye BT servisleri pazarındaki Bulut uygulamalarına ilişkin öngörülen oran

Bulut güvenliği ve risk yönetimi

Bulut kullanımı birçok avantajı beraberinde getirmekle birlikte, aynı zamanda teknoloji ve siber güvenlik hususunda risk oluşturan ve önlem alınması gereken birçok endişeyi de beraberinde getirmektedir.

Bilgisayar korsanlarının (hacker); çalışanları, üçüncü taraf firmaları ve alt yüklenicileri hedef almaya devam edeceği göz önünde bulundurulduğunda, organizasyonların erişilebilirliği artıran bulut bilişim kapsamında kurumsal gizli bilgiye yetkisiz erişim riskini de değerlendirmeye alması gerekmektedir. Ayrıca, bulut aracılığıyla birbirine bağlı cihazların iş ortamında kullanılmasıyla birlikte söz konusu risk oranı artacak ve eğer kurumsal bilgiye kişisel cihazlar aracılığıyla erişme imkânı da var ise, bu cihazlar organizasyona ait sistemler kadar korunamıyor olduğundan zafiyet oranını yükseltecektir. Her ne kadar bu tip senaryolar rastlantısal vakalar oluşturabilecek olsa da kötü niyetli kullanıcıların oluşturabileceği risklerin de hesaba katılması ve kurumsal bir risk olarak işleme alınması gerekmektedir[19].

18 Eser, E., 2019. Turkey IT Services Market 2019–2023 Forecast and 2018 Analysis, s.l.: IDC.

19 Pollard, J., 2019. Future-Proof Your Digital Business With Zero Trust Security, s.l.: Forrester.

Üçüncü taraf risk yönetimi ile ilgili düzenlemeler

Dış kaynak kullanımının artması ile birlikte otoriteler ve düzenleyiciler, organizasyonların üçüncü taraflarla ilişkilerini nasıl yönettiklerine daha fazla odaklanmış ve daha sıkı düzenleme ve yaptırımlar getirmişlerdir. Bu alanda Para Birimi Kontrolörü Ofisi (OCC) tarafından regüle edilerek düzenleyici incelemeyi artıran, üçüncü taraf risk yönetimi hakkında 2002 yılına kadar sadece bankalar için de olsa düzenleyici bir belgeye sahip olan ilk ülke **ABD'**dir. **İngiltere** girişimleri arasında, genel sigortacılıkta dış kaynak kullanımının Finansal Yürütme Kurumu (FCA) incelemesi ve PRA'nın Kıdemli (sigorta) Yöneticileri rejiminin dış kaynak kullanımı için öngörülen bir sorumluluk içerecek şekilde genişletilmesi bulunmaktadır. **Avrupa**'da ise sigorta organizasyonlarının dışarıdan sağlanan faaliyetlere erişiminin ve kontrolünün nasıl ele alındığını ve kontrol edildiğini düzenleyen bir direktif olarak Solvency II oluşturulmuştur[20]. **Dünyadaki örneklere** bakıldığında da ABD'deki BSA/AML (Bank Secrecy Act/ Anti Money Laundering) uyumundaki en sıcak ve en zor konulardan birinin, üçüncü taraflardan kaynaklanan riskleri yönetmek olduğu düşünülmektedir[21].

Türkiye'de ise, Rekabet Kurulu, rekabet hukukuna tam uyumun, üçüncü taraf firmalardan doğan riskler de dahil olmak üzere tüm risk unsurlarının göz önünde bulundurulmasıyla sağlanabileceğini belirtmektedir. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 15 Mart 2020 tarihli ve 31069 sayılı Resmî Gazete'de yayımlanan **Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik** ise, iş sürekliliği, BT sürekliliği, bilgi güvenliği ve kişisel veriler gibi önem arz eden konularda bankaların kendi iç kontrolleri dışında tedarikçi ve diğer üçüncü taraf firmaların kontrollerinin de denetiminden sorumlu olduğunu belirtmekte, bankaların dışarıdan tedarik ettikleri uygulamaların güvenlik testlerinin yapılması ve düzenli olarak bakımlarının gerçekleştirilmesi gerektiği ifade edilmektedir. 05 Kasım 2011 tarihli ve 28106 sayılı Resmî Gazete'de yayımlanan **Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik**'te ise dış hizmet alımlarının öncelikle bir risk çerçevesinde gizlilik ve güvenliğinin değerlendirilmesi gerektiği belirtilmektedir. Bu yönetmelik ile, hizmet kapsamına göre ilgili hizmetlerin sınıflandırılması, üçüncü taraf firmaların kritiklik ve önem seviyesinin belirlenmesi ve denetimlere tabi tutulması gereklilikleri düzenlenmiştir.

20 ORIC International and McKinsey & Company.(2017). Improving Third-Party Risk Management in the (re) insurance and investment industries

21 Lowers & Associates. (2015) Subject to AML Regulation? Don't Neglect Third Party Risk Management

BT dış kaynak kullanımında ise belirli alanlarda, örneğin; KVKK ve GDPR gibi düzenlemelerin zorunlu kıldığı ek gereksinimler ortaya çıkmıştır. Türkiye, İngiltere ve ABD'de uygulanan yaptırımlar organizasyonların dışarıdan sağlanan faaliyetlerden sorumlu tutulacaklarını ve üçüncü tarafların yetersiz gözetimi de dahil olmak üzere yaşanan ihlaller nedeniyle para veya uyarı cezasına çarptırıldığını göstermektedir.

Ayrıca **NIST, PCI DSS, ISO 27001** ve **COBIT** gibi birçok düzenleyici global standart ve çerçeve belge de üçüncü taraf risk yönetim süreçlerini düzenleyici kontroller içermektedir. **NIST**, güncellenmiş siber güvenlik çerçevesinde tedarik zincirini şu şekilde tanımlamaktadır:

> “Tedarik zincirleri, çok sayıda kuruluş arasında karmaşık, küresel olarak dağıtılmış, birbirine bağlı kaynak ve süreç kümeleridir. Tedarik zincirleri, ürün ve hizmetlerin tedariki ile başlar, ürün ve hizmetlerin tasarımı, geliştirilmesi, üretimi, işlenmesi, yürütülmesi ve son kullanıcıya sunulmasıyla tamamlanır. Bu karmaşık ve birbirine bağlı ilişkiler göz önüne alındığında, tedarik zinciri risk yönetimi (SCRM) kritik bir operasyonel işlevdir.

NIST Siber Güvenlik Çerçevesi

NIST tarafından Tedarik Zinciri Risk Yönetimi (SCRM) faaliyetleri aşağıdaki gibi listelenmiştir:

- Tedarikçiler için siber güvenlik gerekliliklerinin belirlenmesi
- Siber güvenlik gerekliliklerinin resmi anlaşma (Örn; sözleşmeler) yoluyla yürürlüğe girmesi
- Tedarikçilere bu siber güvenlik gerekliliklerinin nasıl doğrulanacağının ve kanıtlanacağının belirtilmesi
- Siber güvenlik gereksinimlerinin çeşitli değerlendirme metodolojileri ile karşılandığının doğrulanması
- Yukarıdaki faaliyetlerin yönetim ve yönetişiminin sağlanması

PCI – DSS, kart sahibi verilerinin işlenmesi ya da donanım/yazılım bileşenlerinin yönetimi için üçüncü taraf desteği alınabileceğini ancak bazı temel önemlerin alınması gerektiğini belirtmektedir:

- Üçüncü taraf firmalarla anlaşmalar yapılan anlaşmalarda PCI-DSS referanslarına uygun maddelerin olması
- PCI-DSS gereksinimlerinin kontrol edilmesi ve bunlardan hangisinin üçüncü taraf firma tarafından karşılanması gerektiğinin belirlenmesi
- Üçüncü taraf firmanın uygunluğunun izlenmesi
- Üçüncü taraf firma ile çalışmadan önce bir risk değerlendirmesi yapılması

TS EN ISO/IEC 27001:2017 içerisinde Bölüm A15, tedarikçi ilişkileri ile ilgili kontrolleri tanımlar ve bu kontrollere dayanarak, üçüncü taraf firmalar ile ilişkili riskleri azaltmak amacıyla, organizasyon tarafından uygulanacak süreç ve prosedürlerin Bilgi Güvenliği Politikasında belirlenmesi, bu taraflarla bir sözleşme imzalanması, tedarikçi hizmetlerinin sürekli izlenmesi, düzenli aralıklarla denetiminin yapılması gerektiğini belirtmektedir.

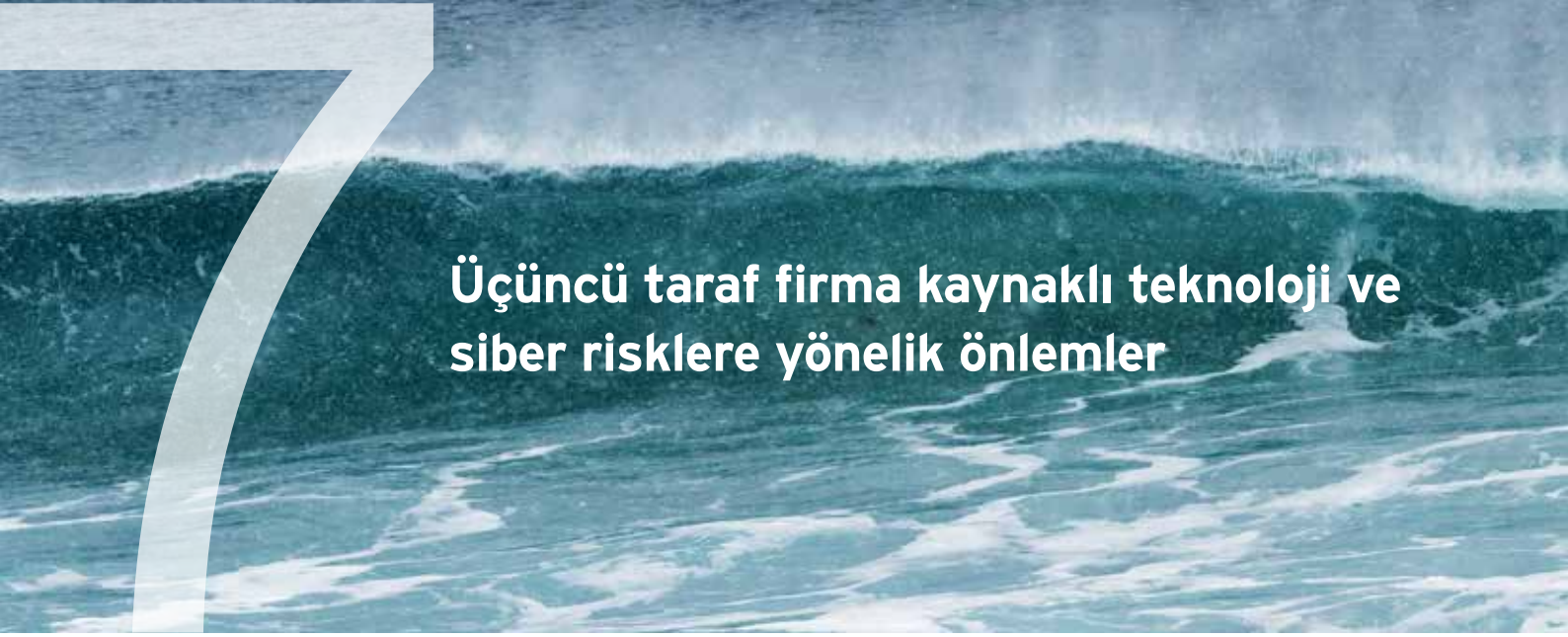
COBIT 2019 çerçevesinde ise üçüncü tarafların BT süreçleri üzerindeki kontrolün yönetilmesinin aşağıdaki yollarla sağlanabileceğini ifade edilmektedir:

- Tedarikçi hizmetlerinin tanımlanması ve sınıflandırılması
- Tedarikçi riskinin belirlenmesi ve risklerin azaltılmasına yönelik aksiyonların alınması
- Tedarikçi performansının, başarı/başarısızlık yüzdesinin ölçümü ve izlenmesi[22]

Aşağıdaki şekilde[22] açıklandığı üzere, COBIT 2019, 0 ile 5 arasında değişen bir Yetkinlik Olgunluk Modeli Entegrasyonu (CMMI) bazlı süreç-yetkinlik planını destekleyerek ilgili sürecin ne kadar iyi uygulandığının ve performans gösterdiğinin bir ölçüsünü de sunmaktadır.

5	Süreç amacına ulaşıp, iyi tanımlanmış olup, performansı, sürekli iyileştirmeyi yerine getirmek amacı takip ediliyor.
4	Süreç amacına ulaşıp, iyi tanımlanmış oluyor ve performansı rakamlara bağlı, metriklerle ölçülüyor.
3	Süreç, organizasyonel varlıkları değerlendirerek, amacına organize bir şekilde ulaşıyor. Süreçler genelde iyi tanımlanmış oluyor.
2	Süreç amacına, temel ve tam faaliyetlerin uygulanmasıyla ulaşıyor. Süreç gerekliliklerini yerine getiriyor.
1	İlgili süreç, tam ve organize olmayan, başlangıç veya sezgiye bağlı faaliyetlerin uygulanmasıyla az - çok amacına ulaşıyor.
0	Temel yetkinlikten yoksun, yönetişim ve yönetim hedeflerine yetersiz yaklaşım gösteriyor. Süreç, pratiklerinin amaçlarını karşılamayabiliyor.

22 COBIT 2019 Çerçevesi: Yönetişim ve Yönetim Hedefleri. (2019). ISACA

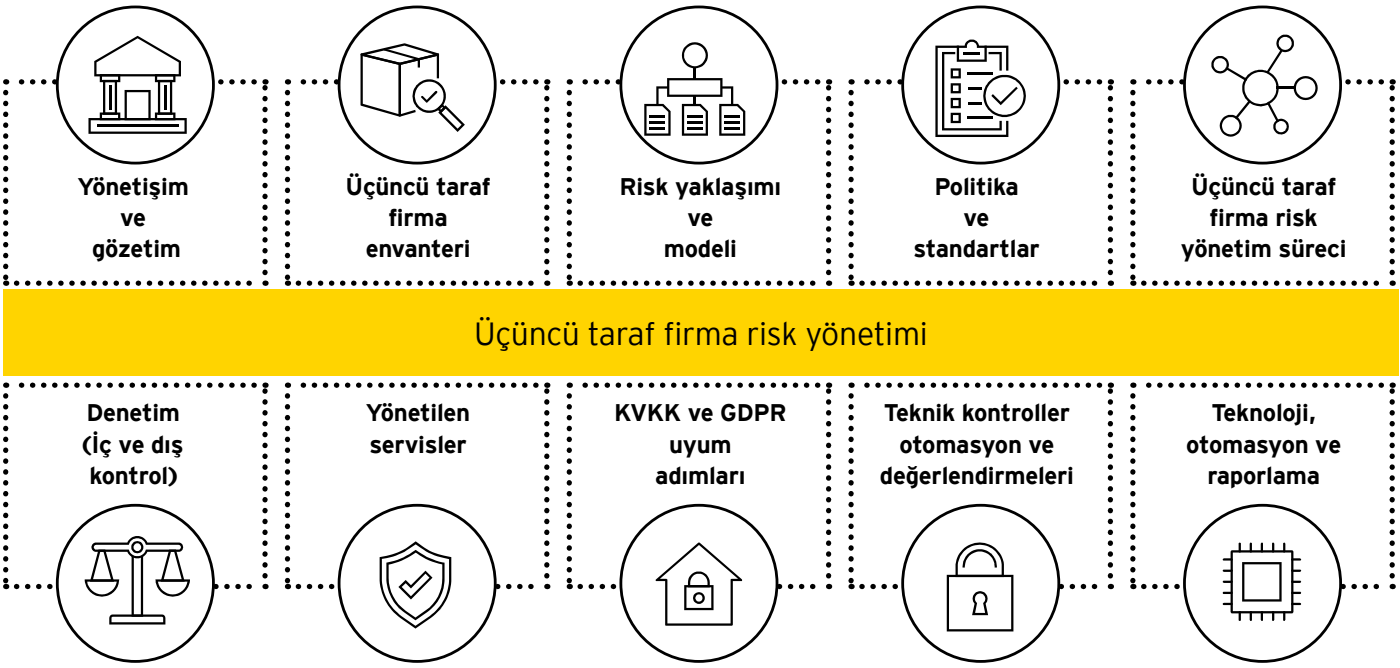


7 Üçüncü taraf firma kaynaklı teknoloji ve siber risklere yönelik önlemler

Üçüncü taraf firmaların oluşturduğu teknoloji ve siber güvenlik kaynaklı risklerin etkin bir şekilde ele alınabilmesi için, organizasyonların üçüncü taraf firma risk yönetimi yetkinliklerini sağlam bir şekilde yapılandırması ve Tasarım Aşamasında Güven (Trust by Design) prensibini benimsemesi önerilmektedir.

Aşağıdaki şekilde görüldüğü üzere, organizasyonların üçüncü taraf organizasyon risk yönetimi yetkinliklerini etkin ve tutarlı bir biçimde tasarlayıp uygulamasına olanak sağlayan 10 temel bileşen bulunmaktadır. Raporumuzun önceki bölümlerinde irdelendiği üzere, tutarlı ve kapsamlı bir üçüncü taraf firma risk yönetim çerçevesi olmaması durumunda, itibar kaybı, üçüncü taraf firmaların etkin olarak izlenememesi ve finansal kayıp gibi riskler ortaya çıkabilir.

Üçüncü taraf firma risk yönetimi, ilgili firmaların kontrollerine, performansına ve aktivitelerine ilişkin göstergelerin takibini sağlayarak bu firmalar ile ilişkilerin daha iyi anlaşılabilmesini sağlar. Etkin yönetim ile risklerin üçüncü taraf firmalar ile iş yapış maliyetini aşıp aşmadığı organizasyonlar tarafından tutarlı bir şekilde değerlendirilebilecektir[23].



23 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

Üçüncü taraf firma risk yönetişimi ve gözetiminin sağlanması

Üçüncü taraf risk yönetiminin etkin bir şekilde işletilebilmesi için organizasyonların doğru yönetişim ve gözetim uygulamalarının benimsemesi gerekmektedir. Üçüncü taraf organizasyonların yönetilmesine ilişkin işletim modelinin; organizasyon seviyesinde resmi olarak kabul görmüş organizasyonel yapıları, belirgin rol ve sorumlulukları kapsaması ve üçüncü taraf organizasyon risk yönetim aktivitelerinin diğer risk yönetim fonksiyonlarıyla entegrasyonu sağlanmalıdır.

Organizasyonel yapının oluşturulmasında organizasyonlar merkezi, dağıtık ya da karma bir yapı izleyebilecek olmakla birlikte, yapılacak olan seçim organizasyonun kültürü, işletim modeli ve üçüncü taraf firma risk yönetimi fonksiyonlarının olgunluğuna göre değişim gösterecektir. Üçüncü taraf firma risk yönetim kapasitesine özgü[24] ve tam zamanlı[25] kaynak sayısının ise büyüklüğe göre değişim gösterdiği gözlemlenmektedir.

İyi uygulama örneklerine bakıldığında, ek olarak bir de gözetim komitesi oluşturulduğu ve bu komitenin çalışma ve çıktılarını kurul seviyesinde raporladığı görülmektedir[26].

Trendler[26]

Üçüncü taraf firma riskleri Yönetim Kurulu (YK) seviyesinde dikkat toplayacaktır.
Organizasyonlar üçüncü taraf firma risklerini genel itibarda üst yönetim seviyesinde raporlamaktadır ve bu raporlamalardan bazıları YK seviyesine eskale edilmektedir. Üçüncü taraf firma risk yönetimine ilişkin başarıda YK katılımının önemli bir faktör olduğunun farkına varılmasıyla birlikte, bu konu YK gündeminde yerini sağlamlaştıracaktır.

24 Gartner, 2019. 2019-2020 Annual Edition: Top Insights for the C-Suite, s.l.: Gartner.

25 Babin, R., 2020. Governing Vendors for Transformation: Getting the Most from Third-Party Relationships, s.l.: IDC.

26 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

Üçüncü taraf firma envanterinin oluşturulması ve güncelliğinin sağlanması

Organizasyonların üçüncü taraf firma risklerinin yönetimi faaliyetlerine başlamadan önce öncelikle tüm üçüncü taraf firmaları ve bunlardan sorumlu olan çalışanları belirleyerek bir envanter hazırlaması ve organizasyonun önceliklerine göre belirlenmiş kriterlere göre bu üçüncü taraf firmaları sınıflandırması gerekmektedir. Henüz bir üçüncü taraf firma envanteri bulunmayan organizasyonlar, bu envanteri oluşturmak için fatura veya ödeme verileri, sözleşme yönetim veri tabanları ya da kurumsal kaynak planlaması (ERP) sistemlerinden faydalanabilir. Envanterin oluşturulmasını takiben üçüncü taraf firmaların sınıflandırılması, hem harcanan eforların önceliklendirilmesine katkı sağlar hem de üçüncü taraf firmaların risk bakış açısıyla yönetilmesine imkân verir. Bu sınıflandırmaya en basit düzeyde yeni - eski üçüncü taraf firmalar olarak, ardından kritiklik, servis tipi ve ücret, üçüncü taraf firma servislerini alan iş birimleri gibi detaylar eklenebilecektir.

Bankacılık sektörüne bakıldığında, üçüncü taraf firma sınıflandırma kriterleri **Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik** kapsamında oluşturulan kontrol listeleri aracılığıyla takip edilmektedir. Diğer sektörlerde faaliyet gösteren organizasyonların da bu gibi iyi uygulama örneklerini benimsemeleri önerilmektedir. Yapılacak değerlendirmeler sonrasında üçüncü taraf firmaların ayrıca risk seviyesine göre de sınıflandırması önerilmektedir.

Bahse konu envanter içeriği sürekli olarak değişebileceği için (örneğin; üçüncü taraf firmaların veya alınan hizmetlerin artıp azalması durumlarında) güncel bir şekilde sürdürülmesi kritik önem taşımakta olup, tutarlı ve tam bir üçüncü taraf firma envanterinin oluşturulması, risk yönetim sürecinin otomatize edilmesine de temel oluşturacaktır. Bu sebeple belirli periyotlar tanımlanarak envanterin düzenli olarak gözden geçirilmesi ve güncelliğinin sorumlu birimlerce sağlanması tavsiye edilmektedir[27].

Trendler[27]

Organizasyonlar, satın alma ve tedarik zinciri fonksiyonlarının daha etkin kararlar alabilmesi için üçüncü taraf firma risk verisi, öngörücü modelleme, istatistik ve görselleştirmeye başvurmaktadır. İş zekası çözümleri, operasyonel değişimi desteklemekte ve karar alma süreçlerini iyileştirmektedir.

27 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

Risk çerçevesinin kurgulanması

Organizasyonların **risk iştahlarını** baz alarak kullanılacak risk modelini belirlemesi ve üçüncü taraf firma yönetimi ile ilişkili riskleri tespit etmesi gerekmektedir. Tespit edilen bu risklerin ise organizasyonun risk belirleme stratejileri ve **kurumsal risk yönetim süreci** ile hizalanmış olması sağlanmalıdır.

Organizasyonların konsolide bir envanter aracılığıyla üçüncü taraf firmalar hakkında net bir görüş elde edebilmesini takiben, üçüncü taraf firmaları teşkil ettikleri risk bazında ayırt edebilmeleri ve riskten korunmaya yönelik ne gibi aksiyonların gerektiğini anlamaları önem kazanacaktır. Söz konusu risk yönetimi süreçlerinde tecrübeli organizasyonların, üçüncü taraf firmalar ile olan ilişkilerini değerlendirmek için hangi risklerin kullanılacağını belirleyebilmek adına bir **risk evreni** oluşturduğu ve **kabul edilebilir risk seviyesi**ni belirlediği gözlemlenmektedir. Bu organizasyonlar, üçüncü taraf firmalardan toparlanan risk bilgisini risk modelleriyle beslemek suretiyle niteliksel ve niceliksel değerlendirmeler yapabilmekte ve eforlarını daha yüksek seviye üçüncü taraf firma risklerinin izlenmesi ve yönetilmesine yönlendirebilmektedir. Risk modelleri, organizasyonlara ayrıca üçüncü taraf firmaları önden tanımlı risk seviyelerine göre sınıflandırma imkânı da sağlamaktadır.

Bu doğrultuda, organizasyonlar üçüncü taraf firmaları risk seviyelerine göre kategorize etmelidir. Böylelikle organizasyon tarafından gerçekleştirilecek izleme faaliyetleri, söz konusu risk değerlendirme sonuçlarına göre şekillenmiş ve tetiklenmiş olacaktır[28].

Trendler[28]

Gün geçtikçe dijitalleşen teknoloji odaklı günümüz dünyasında, organizasyonların bilgi güvenliği ve kişisel veri mahremiyeti risklerini anlayarak karşılık verebilmesi hayati önem taşımaktadır. Nitekim üçüncü taraf firma riskleri evrimleşmeye devam ettikçe, organizasyonların odak noktalarını bilgi güvenliği ve kişisel veri mahremiyetinin ötesine taşıyarak daha geniş kapsamda risk faktörlerini değerlendirmeye alması gerekmektedir. Organizasyonların risk hususunda daha bütüncül bir bakış açısı benimseyebilmeleri için kurumsal risk yönetimi, üçüncü taraf firma risk yönetimi, siber güvenlik ve diğer risk tabanlı fonksiyonlarını birbirine hizalamaları gerekmektedir.

28 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

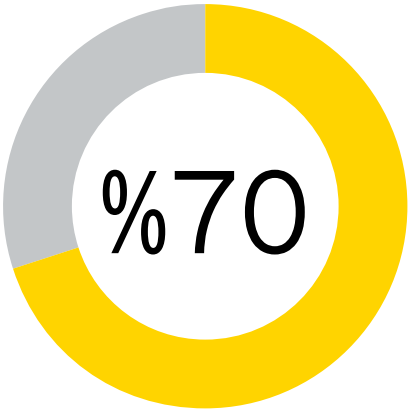
Politika ve standartların oluşturulması

Politika ve standartlar, üçüncü taraf firma risk yönetimi kapsamında olan tüm paydaşlara ilişkin rol, sorumluluk ve beklentilerin netleştirilmesinde[29] kılavuzluk etmektedir. Politika ve standartların etkin bir şekilde oluşturulması ve işletilebilmesi için yönetici kadronun desteğinin alınması gerekmektedir. Yönetici kadro, politika ve standartlarda bulunan gereksinimleri uygulatabilmeli ve böylelikle anahtar paydaşlar üzerinde sorumluluk oluşturabilmelidir.

İç paydaşların üçüncü taraf firma etkileşime geçme, dış bir organizasyon ile iş yapmaya ilişkin riskler ve organizasyon politika ve standartlarına uyum göstermemenin sonuçlarına ilişkim sorumluluklarının ve yükümlülüklerinin bilincinde olmaları, etkin bir üçüncü taraf firma risk yönetimine ulaşma yolunda kritik konumdadır.

Üçüncü taraf firma risk yönetimi politika ve standartları açık bir şekilde üçüncü taraf firma risk yönetiminin amacını ve yaklaşımını belirtmeli, ilişkili tanımları ve terimleri sağlamalı, üçüncü taraf firma risk yönetimi çerçevesini özetlemeli, üçüncü taraf firma risk yönetimi yaşam döngüsünün fazlarını açıklamalı, üçüncü taraf firma yönetmekte kullanılan sistemleri dokümante etmeli ve uyum göstermeyen paydaşlar ya da üçüncü taraf firma sorunları için işletilecek eskalasyon protokollerini detaylandırmalıdır.

Politika ve standartların yönetici kadro tarafından minimum yılda bir kere gözden geçirilerek onaylanması sağlanmalıdır[30].



Üçüncü taraf firma risk yönetimi alanında yapılan global anketlerde[30], katılımcıların %70'inin politika, prosedür ve kılavuzları tesis etmede ve bunlara sürekli uyum yaşamada güçlük çektiği gözlemlenmektedir.

Üçüncü taraf firma risk yönetim sürecinin kurgulanarak uygulanması

Organizasyonların üçüncü taraf firma risk yönetimi alanında yaşadığı güçlükler, risklerin tanımlanması ve izlenmesinde tekrarlı bir yaklaşım izlemenin önemini ortaya çıkarmaktadır. Bu yaklaşım, sözleşmenin imzalanması öncesinde üçüncü taraf firmalara ilişkin detaylı bilgi edinimi gerektirir. Ayrıca üçüncü taraf firmalarla olan ilişki boyunca **sürekli öğrenmeye** daha fazla önem verilmelidir.

Üçüncü taraf firma ilişkileri yönetimi; ilerleyen bölümlerde inceleme çalışmaları, sürekli izleme ve sertifika yenileme olarak 3 faza ayrılmış şekilde[31] işlenmekte ve önerilen risk giderici önlemler ise faz bazında belirtilmektedir.

i. İnceleme çalışmalarının kritik risklere odaklanacak şekilde konumlandırılması

Üçüncü taraf firma risk yönetimi inceleme çalışmalarında kullanılan anketlere ilişkin sektördeki örneklere bakıldığında, zaman içerisinde bu anketlerdeki soru sayılarının giderek arttığı ve böylelikle hem organizasyon tarafında hem de üçüncü taraf firma tarafında inceleme çalışmalarına ayırılan eforun gitgide fazlalaştığı gözlemlenmektedir. Bu durum organizasyon tarafında ek kaynak ihtiyaçlarına sebep olabilmekte, üçüncü taraf firma tarafında da eforun organizasyonun korunmasından ziyade anketlerin tamamlanmasında yoğunlaşmasına sebep olabilmektedir[32].

Sektördeki iyi uygulamalar incelendiğinde ise, önceki dönemlerde yaşanan üçüncü taraf firma kaynaklı olaylar, sektör verileri ve ilgili acil yardım hatları (hotline) aracılığıyla veriye dayalı bir yaklaşım benimsendiği ve böylelikle daha etkin risk göstergelerini adresleyen anket sorularına odaklanıldığı gözlenmektedir.

Sağlık sektöründe faaliyet gösteren bir organizasyon öncelikle üçüncü taraf firma risk değerlendirme anketindeki sorulardan hangilerinin ilgili kanun ve düzenlemeler uyarınca tayin edildiğini ve hangilerinin ise organizasyonu (ya da sektördeki diğer organizasyonları) etkileyen geçmiş riskleri adreslediğini belirleyip, ardından veri kaynaklarını (iç denetimden gelen geçmiş dönem risk raporları, sektör birlikleri tarafından üretilen risk raporları, acil yardım hattı (hotline) raporları gibi) gözden geçirerek geçmiş, mevcut ya da potansiyel üçüncü taraf firma olaylarına göre kritik önemde olan sorulara ilişkin tamamen anket üzerinden filtreleme yaptığını belirtmiştir.

İnceleme çalışmalarının kritik risklere odaklanacak şekilde konumlandırılması için bir sonraki sayfada bulunan özet şemadan faydalanılabilir.

29 Gartner, 2019. 2019-2020 Annual Edition: Top Insights for the C-Suite, s.l.: Gartner.

30 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

31 Audet, C. (2019). Stay Ahead of Growing Third-Party Risk. Gartner.

32 Budge, J. et al., 2019. Executive Spotlight: Top Priorities for Security and Risk Leaders In 2019, s.l.: Forrester.

1. Adım: Kritik soruların belirlenmesi

Geçmişte organizasyonu etkileyen riskler baz alınarak, üçüncü taraf firma ile etkileşime geçmeden önce hangi bilgileri öğrenmek kritik konumdadır?

2. Adım: Veri kaynaklarının gözden geçirilmesi

İç denetimden gelen geçmiş dönem risk raporları	Sektör birlikleri tarafından üretilen risk raporları

Acil yardım hattı (hotline) raporları[33]

ii. Üçüncü taraf firma ilişkilerindeki değişikliklerin izlenmesi için alarmların tesis edilmesi

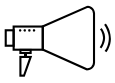
Üçüncü taraf firma risk yönetimi süreçlerinin iş süreçleri ile hizalanmış olmaması, iş süreçlerine ilişkin risk toleransı ile uyumsuzluğa ve gelişen risklere ilişkin gerçek zamanlı iç görü elde edilememesine sebep olmaktadır. Bu sebeple üçüncü taraf firma riski oluşturabilecek faaliyetleri belirlemek adına işletme genelindeki operasyonların kapsamlı bir şekilde gözden geçirilmesi gerekmektedir.

Alarm bazlı izleme kontrollerinin kurgulanması için aşağıdaki özet şekilden faydalanılabilir.

Alarm bazlı izleme[33]

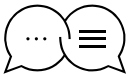
Risk izlemede metriklerin kullanılması

Metrikler aracılığıyla iş ortaklarınızın performanslarını ve risklerini öğrenin.



Metriklerin üzerine alarmların kurulması

Metriklerinizi alarm otomasyonları ile takip edin.



Raporlama aracılığıyla gerçek zamanlı içgörü

Alarmlar tetiklendiğinde otomatik raporlama üreten bir altyapı kurgulayın

Üçüncü taraf firma ilişkilerindeki değişikliklerde tetiklenecek[34] bir alarm mekanizmasının, işletme süreçleri boyunca üçüncü taraf firma ağında konumlandırılması bu konuda etkin bir yaklaşım sergilenmesini sağlayabilecektir. Bunun gerçekleştirilebilmesi için de fonksiyonlar arası belirlenecek iş metrikleri aracılığıyla üçüncü taraf firma performansı ve risklerinin öğrenilmesi, bu metriklere ve yüksek risk oluşturan alanlara ilişkin alarmların oluşturulması ve alarmların aşıldığı durumlarda otomatik raporlamaların yapılacağı bir altyapının kurgulanması önerilmektedir.

Finansal sektörde faaliyet gösteren bir organizasyon, üçüncü taraf firma performansı ve risklerine ilişkin metrikleri tanımlayarak bu metriklerin aşıldığı durumlarda tetiklenen bir alarm kurgusu ile otomatik raporların üretildiğini ve gerçek zamanlı kavrayış sağlayan bu raporların da uyum fonksiyonu tarafından gözden geçirildiğini belirtmiştir[35].

iii. Üçüncü taraf organizasyon ilişkilerindeki değişikliklerin izlenmesi için kontrol ve teşviklerin oluşturulması

Yüksek riskli üçüncü taraf firmalara ilişkin kontrol ve teşviklerin tanımlanıp risklerin sürekli olarak izlenmesi ve takibinin sağlanması gerekmektedir.

Üçüncü taraf firma risk yönetimi alanında yapılan global araştırmalarda, telekomünikasyon sektöründe faaliyet gösteren bir organizasyonun bu konuda iki temel güçlükle karşılaştığı öğrenilmiştir. Birincisi, hizmet veren tedarikçilerin kendi tedarikçileri (alt yüklenicileri) tarafında ortaya çıkan itibar risklerini nasıl ele alacağı belirli ve yapılandırılmış bir yaklaşıma sahip olmadığıdır. İkinci olarak, üçüncü taraf firma ağının genişliği de göz önüne alındığında, geleneksel risk denetimleri esnasında toplanan bilgilerin yeterliliğini değerlendirmenin kolay olmadığı ifade edilmiştir.

Bu güçlüklerin üstesinden gelebilmek için organizasyonun öncelikle stratejik tedarikçilere kendi tedarik ağları boyunca itibar riski yönetimini sahiplendirmesi gerekmektedir. İş birlikçi bir risk yönetimi bakış açısı oluşturmak için yerinde ziyaretler, mülakatlar ve tedarikçiler ile birlikte çalıştaylar düzenlenmesi faydalı olabilecektir.

Ek olarak, tedarikçi ağına tutarlı bir risk değerlendirilmesi uygulayabilmek adına tedarikçilere gerekli çerçeve ve araçların sağlanması gerekmektedir. Manuel olarak değerlendirilen risk anketleri yerine çoklu kaynaktan edinilen bilgilerin çapraz kontrolüne imkân tanıyan ve böylelikle daha güvenilir sonuçlar üreten teknolojik araçlar hem organizasyonun üçüncü taraf firma risk yönetim sürecini daha etkin bir şekilde yönetmesini sağlayacak, hem de tutarlılığı artırarak daha güvenilir sonuçlar elde edilmesini sağlayabilecektir[33].

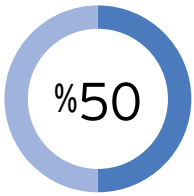
33 Audet, C. (2019). Stay Ahead of Growing Third-Party Risk. Gartner.

34 Budge, J. et al., 2019. Executive Spotlight: Top Priorities for Security and Risk Leaders In 2019, s.l.: Forrester.

35 Gartner, 2019. 2019-2020 Annual Edition: Top Insights for the C-Suite, s.l.: Gartner.

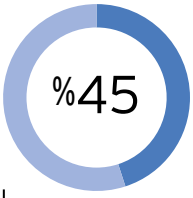
2019 yılında 246 global organizasyonla yapılan EY Global Üçüncü Taraf Firma Risk Yönetim Anketi[36]'ne ilişkin sonuçlar aşağıdaki gibidir:

İşletim modeli



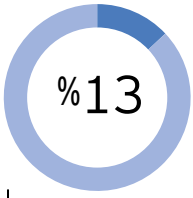
katılımcı, üçüncü taraf firma risk yönetimini merkezi olarak yürütmektedir.

Uygulama



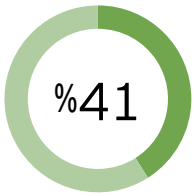
katılımcı, üçüncü taraf firma risk yönetimi alanında 2 ila 3 sene içinde daha çok yönetilen servis kullanacaktır.

Kaynak modeli



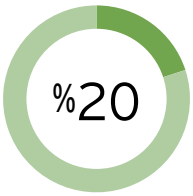
oranında ortalama kaynak, üçüncü taraf firma risk yönetimini desteklemek için kullanılmaktadır.

Araçlar ve teknoloji



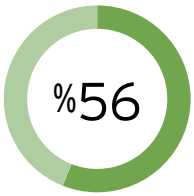
katılımcı, üçüncü taraf firma risk yönetimine özel bir teknoloji platformu kullanmaktadır.

İnovasyon



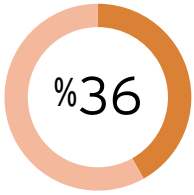
katılımcı, üçüncü taraf firma risk yönetimi kapsamında ileri analitik kullanmaktadır.

Üçüncü taraf firmalar



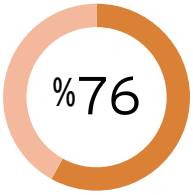
katılımcı, üçüncü taraf firmaların alt yüklenicileri için sözleşmelere veya değerlendirmelere bel bağlamaktadır.

Siber güvenlik



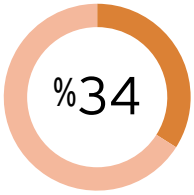
katılımcı, geçtiğimiz 2 sene içerisinde üçüncü taraf firma kaynaklı veri ihlali yaşamıştır.

Değerlendirmeler



katılımcı, kritik üçüncü taraf firmalarını senelik olarak değerlendirmektedir.

Doğal risk



katılımcı, doğal risk profillerini üçüncü taraf firmalarının skoruna göre yenilemektedir.

36 EY, 2019. Building Trust With Your Third Parties in a Technology-Driven and Disruptive World, s.l.: EY.

Sertifika gereksinimlerinin değerlendirilmesi

Sertifikasyon, dijital tedarik zincirinde güvence sağlamak amacıyla alınan temel aksiyonlardandır. Sertifikasyonların bir çoğu üçüncü taraf firma güvenliğini desteklemeyi amaçlamakta ve iç paydaşlara asgari güvenlik seviyesinin uygulanması yönünde ek fayda sağlamaktadır.

Sertifikasyon, organizasyonlarda güvenlik seviyesinin yükselmesine aracı olacak ve deneyimli dış denetçiler tarafından uygunluğun gözden geçirilmesini de beraberinde getirecektir. Böylelikle, sertifika sahibi organizasyonların düzenli olarak güvenlik faaliyetlerine ilişkin yatırım ve geliştirme yapması, ayrıca potansiyel alıcıların dikkatine gelecektir.

Üçüncü taraf firma yönetiminde ilgili asgari standartların karşılanması, sertifikasyon standartları aracılığıyla güvence altına alınabilecektir. Bu standartlar arasında en yaygın olanları aşağıda listelenmektedir:

- **International Standard on Assurance Engagements (ISAE) 3402:** Organizasyonların yeterli iç kontrol altyapısının bulunduğuna dair müşterilerine ve servis kullanıcılarına güvence veren raporlamadır.
- **AICPA Service Organization Control (SOC) 2 Reporting:** Organizasyonların güvenlik, erişilebilirlik, bütünlük, gizlilik ve kişisel veri mahremiyeti kontrollerine ilişkin güvence sağlayan raporlamadır.
- **International Organization for Standardization (ISO) 27001:** Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulumuna ilişkin standarttır.
- **Payment Card Industry (PCI) Data Security Standard (DSS):** Kredi kartı bilgilerinin korumasında yardımcı olacak kontrolleri içeren standarttır.
- **NIST Cybersecurity Framework (NIST CSF):** Siber güvenlik ve temel altyapı sistemlerini korumak için yaklaşım geliştirmeyi hedefleyen bir çerçevedir.
- **Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR):** Bulut bilişim alanında iyi uygulamaların kullanımına yönlendiren ve bu alanda güvence sağlayan bir programdır.
- **International Organization for Standardization (ISO) 27701:** Mahremiyet Bilgi Yönetim Sistemi kurulumuna ilişkin standarttır.

İyi uygulamalara bakıldığında, sertifikasyona ilişkin 3 temel kullanım modeli göze çarpmaktadır:

- Müşterilerine üçüncü taraf firma yönetimi, güvenlik, gizlilik gibi alanlarda güvence sağlamak amacıyla sertifika alan organizasyonlar
- Servis sağlayıcıları veya iş ortaklarının değerini anlamayı talep eden organizasyonlar
- İç veya dış paydaşlarına güvenli uygulamalarını sergilemek isteyen organizasyonlar[37].

Teknoloji desteğinin sağlanarak risk iyileştirme sonuçlarının geliştirilmesi

Teknoloji odaklı günümüz dünyasında, üçüncü taraf firma risk yönetimi süreçlerinin otomatize edilebilmesi ve üçüncü taraf firma risk yönetimi aktivitelerinin ürettiği verilerin etkin bir şekilde analiz edilebilmesi için teknoloji desteği gerekmektedir.

Birçok organizasyon üçüncü taraf firma envanterlerini ve süreçlerini halen Excel tabloları ve manuel süreçler aracılığıyla sürdürmekte ve raporlamaktadır. Diğer organizasyonlar ise yerinde veya hizmet olarak yazılım modellerinin adreslediği çözümleri kullanmakta ve bu iki model arasından yazılım modelinin daha çok tercih edildiği gözlemlenmektedir. Genel olarak maliyet uygunluğu ve ölçeklenebilirlik kriterlerinin üçüncü taraf firma risk yönetimi teknolojisi tercihlerinde etkin olduğu görülmektedir. Ayrıca üçüncü taraf firma risk yönetimi araçlarının organizasyondaki diğer mevcut sistemlerle entegre edilebilirliğini de mutlaka göz önünde bulundurması gerekmektedir.

Robotik süreç otomasyonu, üçüncü taraf firma risk yönetimi endüstrisine yüksek etkili yenilikler katmakta ve böylelikle işlem süresini kayda değer ölçüde düşürerek değerlendirme ve inceleme faaliyetlerine ilişkin hacmi artırabilmektedir. Ayrıca manuel görevler, tekrarlı işler ve süreç tıkanıklıkları robotik süreç otomasyonunun sağladığı otomasyon desteğiyle ortadan kaldırılabilmektedir. Bu durum da organizasyonların eforlarını her tip riski içerecek şekilde üçüncü taraf firma risk envanterlerine yönlendirmesini sağlayacaktır[38].

Trendler[38]

Teknoloji alanındaki dönüşüm trendleri, üçüncü taraf firma risk yönetimi fonksiyonlarının manuelden otomatiğe geçmesine aracılık edecektir. Üçüncü taraf firma risk yönetimi, yerinde teknolojiden bulut tabanlı ve SaaS platformlara doğru ilerleyen bir dijital dalgayı takip ettikçe, manuel süreçler ve Excel çalışmaları yerini otomasyonlara ve analitiğe bırakacaktır. Otomasyon ve gerçek zamanlı analitik kullanımı ise organizasyonlara düşük maliyet, verimlilik artışı, yüksek erişilebilirlik ve güvenilirlik sağlayacaktır.

37 Predovich, B., Thielemann, K. & Olyaei, S., 2020. Market Guide for Organization Security Certification Services, s.l.: Gartner.

38 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

Teknik kontroller ve güvenlik değerlendirmelerinin sağlanması

Güvenlik kontrollerinin etkinliğinin değerlendirilmesi ve test edilmesi hususunda sızma ve açıklık testlerinin rolü büyük öneme sahiptir[39]. Bu ve bunun gibi güvenlik testleri, üçüncü taraf firmaların güvenlik olgunluğunun anlaşılmasında kullanılabileceği gibi, uygulama güvenliği değerlendirmesi, zafiyet testleri vb. uygulamalara ilişkin dokümante sonuçlar organizasyonlar tarafından üçüncü taraf firmalardan talep edilebilecek ve güvenlik kriterine dair daha ölçülebilir sonuçlarla ilerlenebilecektir.

Üçüncü taraf firma risk yönetimi alanında yönetilen servisler modelinin değerlendirilmesi

Profesyonel risk danışmanlığı ve denetimi alanında faaliyet gösteren organizasyonların sağladığı hizmetlere bakıldığında, Servis Olarak Risk Yönetimi (Risk Management as a Service) hizmeti göze çarpmaktadır. Bu hizmetler, deneyimli risk uzmanları tarafından önden tanımlı ve çokça pratik edilme imkânı olmuş metotlar çerçevesinde uygulanmakta olup, organizasyonların stratejik hedeflerine öngörülebilir maliyetler ile ulaşmasını sağlamaktadır. Buna ilaveten, yönetilen servisler modeli aracılığıyla yapay zekâ fonksiyonu organizasyonların iş stratejisine hizalanabilecek ve böylelikle hızla değişen bir risk ortamında organizasyonlara teknoloji ve yenilik tabanlı günümüz çağında yeni ve güncel çözümler sunulmasını sağlayabilecektir. Yönetilen Siber Güvenlik Hizmetleri (Cybersecurity Managed Services) kapsamında ise zafiyetlerin tespiti ve yönetilmesi, tehdit yönetimi ve uygulama güvenliği alanlarında organizasyonlara zamanında aksiyon alma, siber güvenlik tehditlerini etkisiz hale getirme ve dijital ürün ve servislerin güvenli şekilde tasarlayabilme desteği sağlanacaktır[40].

Üçüncü taraf firma denetimi

Üçüncü taraf firma risk yönetimi çerçevesinin etkin bir şekilde işletilebilmesi için üçlü savunma hattı etrafında yapılandırma önerilmektedir. Bu durumda birinci savunma hattıyla sorumlu ekip üçüncü taraf firma iş ilişkilerini sahiplenerek operasyonel (örnek olarak günlük) gözetim yapacak, ikinci savunma hattıyla sorumlu ekip üçüncü taraf firma risk yönetim çerçevesini tasarlayacak ve sahiplenecek, üçüncü savunma hattıyla sorumlu ekip de bağımsız olarak bu çerçeveye bağlılığı ve sürecin tasarlandığı şekilde işletilip işletilmediğini değerlendirecektir[41]. Bununla birlikte, üçüncü taraf firma denetimi konusunda organizasyonlar dış destek alternatifi ile de ilerleyebilecektir. Söz konusu hizmet, profesyonel risk danışmanlığı ve denetimi alanında faaliyet gösteren ve dış kontrol rolünde bağımsız görüş sunabilecek organizasyonlar aracılığıyla sağlanabilmektedir.

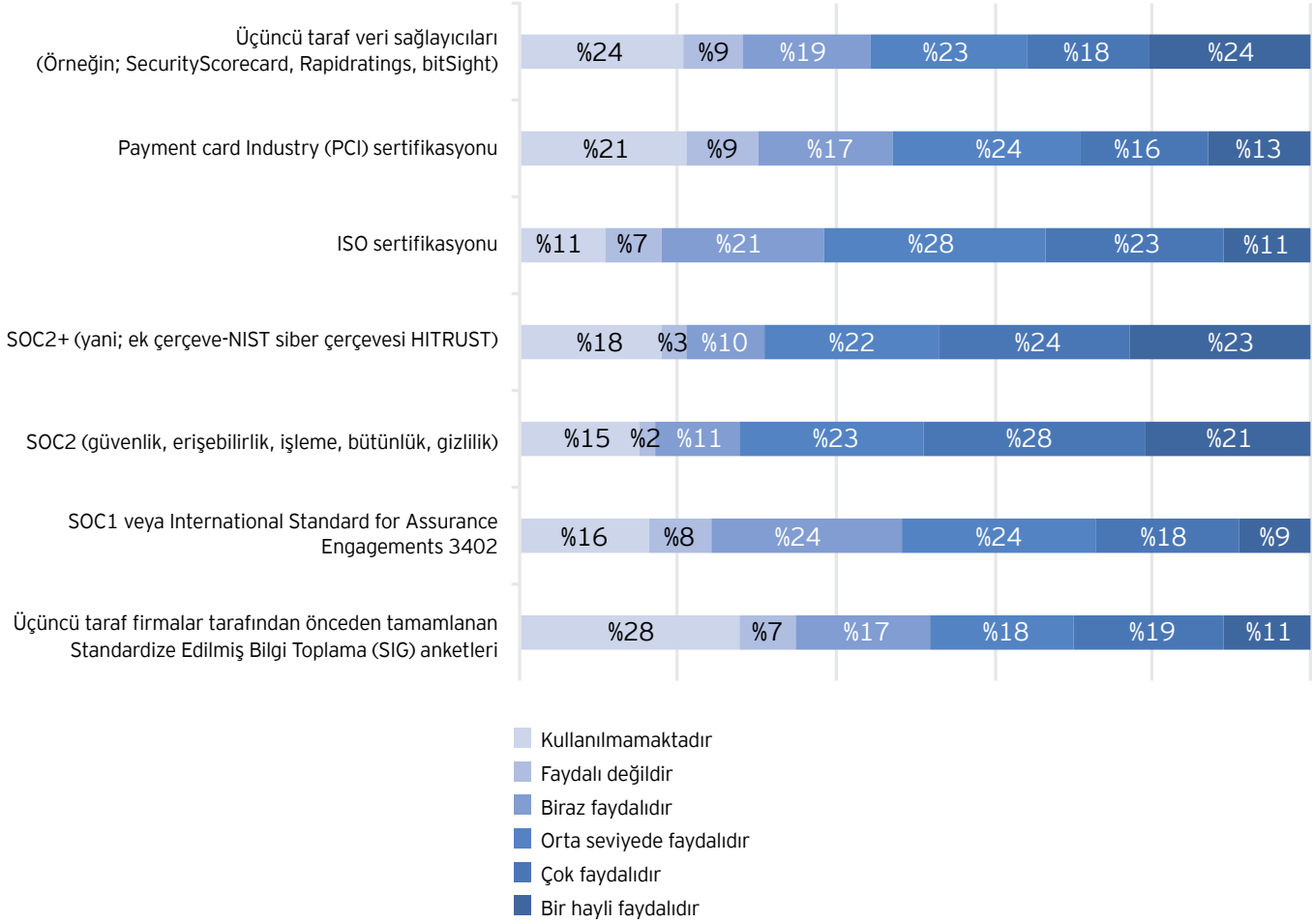
39 Barros, A., 2020. Using Penetration Testing and Red Teams to Assess and Improve Security, s.l.: Gartner.

40 Stengel, B. & Little, G., 2019. IDC MarketScape: Worldwide Risk Consulting Services 2019 Vendor Assessment, s.l.: IDC.

41 EY, 2018. Can You Transform Your Third Parties' Risk into a Competitive Advantage?, s.l.: EY.

2019 EY Global Üçüncü Taraf Firma Risk Yönetim Anketi'nde risk/kontrol değerlendirmeleri, güvence yöntemi ve güvenlik sertifikasyonları alanında göze çarpan hususlar aşağıdaki gibidir:

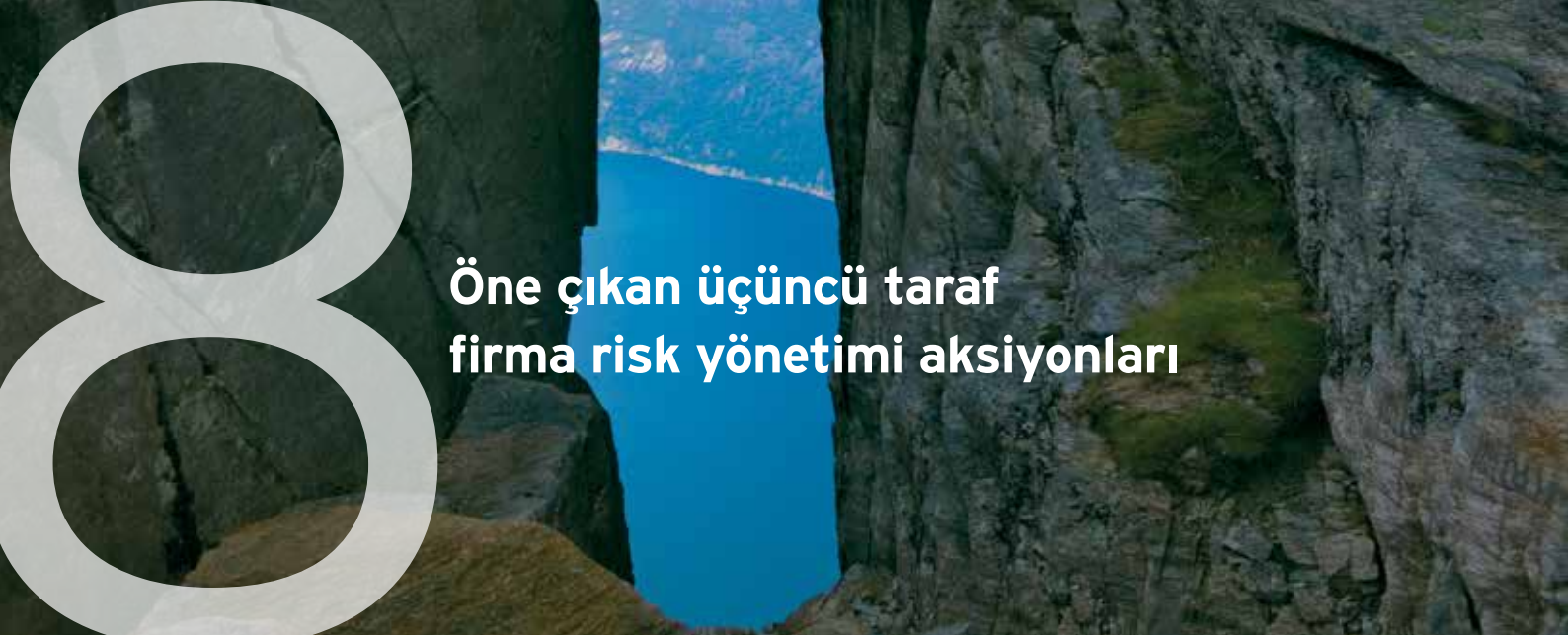
Üçüncü taraf firma risklerinin azaltılması amacıyla risk/kontrol değerlendirmesi gerçekleştirme gereksinimini ortadan kaldırabileceği öngörülen kanallar/çerçeveler ve bunların organizasyonlar nezdinde bu amaca ilişkin faydalılık oranları[42].



Anket sonuçları incelendiğinde, katılımcıların yarısının System and Organization Controls (SOC) 2 veya SOC 2+'yi yararlı olacak ek bir çerçeve olarak değerlendirdiği göze çarpmaktadır. Diğer çerçevelerin (ISO, PCI, vb.) ise orta seviyede ve SOC 2 ve SOC 2+'a nazaran daha az yararlı olarak belirtildiği gözlemlenmektedir.

Ayrıca, anket sonuçlarının da gösterdiği üzere, organizasyonlar halen bir risk/kontrol değerlendirmesi yapma ihtiyacını azaltmada tamamen başarılı olan bir çerçeve/güvence yöntemi bulamamıştır.

42 EY, 2019. Building Trust With Your Third Parties in a Technology-Driven and Disruptive World, s.l.: EY.



8 Öne çıkan üçüncü taraf firma risk yönetimi aksiyonları

1. Yönetişim ve gözetim yapısının kurgulanması

Çalışılan üçüncü taraf firmalara ilişkin risklerin yönetimi ve gözetimiyle sorumlu bir yapının tasarlanması ve rol/sorumlulukların tesis edilmesi önerilmektedir. Ayrıca ilgili yönetişim yapısı için komite seviyesinde temsil yapısı kurgulanabilir.

2. Envanterlerin oluşturulması ve güncelliğinin sağlanması

Çalışılan tüm üçüncü taraf firmaları kapsayan konsolide bir envanterin oluşturulması sağlanmalıdır. Bu envanter aracılığı ile üçüncü taraf firmaların kritiklik ve risk seviyelerini içerecek şekilde sınıflandırılması ve envanterin güncel tutulmasına adına süreçlerin tesis edilmesi önemlidir.

3. Risk çerçevesinin kurgulanması

Üçüncü taraf firma risklerine ilişkin risk iştahının ve risk yönetim modelinin belirlenmesi sağlanmalıdır. Tespit edilen risklerin, kurumsal risk yönetimi çerçevesi ile hizalandırıldığından emin olunmalıdır.

4. Üçüncü taraf firma ilişki yönetimi süreçlerinin tasarlanması ve işletilmesi

Üçüncü taraf firma ilişkilerinin yönetimine ilişkin resmi bir süreç kurgulanmalıdır. Bu sürecin risk analizi çalışmaları, performans takibi, sürekli izleme ve yeterlilik sertifika yenileme adımlarını içerdiğinden emin olunmalıdır.

5. Resmi politika ve standartların oluşturulması

Üçüncü taraf firma risk yönetimine ilişkin rol, sorumluluk ve beklentileri içeren ve üst yönetim tarafından onaylanmış resmi politika ve standartların oluşturulması sağlanmalıdır. Bu dokümanların amaç, yaklaşım, ilişkili tanım ve terimler, üçüncü taraf firma risk yönetimi çerçevesi, bu kapsamda kullanılacak sistemler ve disiplin süreci konularını kapsadığından emin olunmalıdır.

6. Teknoloji desteği

Üçüncü taraf risk yönetim süreçlerini etkin bir şekilde yönetebilmek için, teknoloji desteğinin (araç kurulumu, entegrasyon danışmalığı, yönetilen servisler vb.) alınarak, süreçlerin otomatize edilmesi oldukça fayda sağlayacaktır.

7. Teknik kontrollerin belirlenmesi ve düzenli güvenlik değerlendirmelerinin yapılması

Çalışılan üçüncü taraf firmaların sızma testi, açıklık testi, zafiyet testi vb. güvenlik testlerini düzenli olarak yaptığından veya yaptırdığından emin olunması ve söz konusu değerlendirme sonuçlarının alınacak hizmet kapsamındaki güvenlik kriterlerinin anlaşılması açısından düzenli olarak incelenmesi tavsiye edilmektedir.

8. KVKK ve GDPR uyumu değerlendirmesi

KVKK ve GDPR kişisel veri mahremiyeti düzenlemelerine uyumlu bir şekilde faaliyet gösterdiğinden emin olunması adına düzenli kontroller yapılmalı veya yaptırılmalıdır.

Kişisel veri haritalama çalışmaları gerçekleştirilerek verilerin nerede olduğu, hangi üçüncü taraf firmaların erişebileceği, organizasyonda hangi veri kategorilerinin bulunduğu ve bu verilerle ne yapıldığı anlaşılmalıdır. Hassas verilere erişim sadece yetkisi olan taraflarla kısıtlanmalı ve erişimler düzenli gözden geçirilmelidir. Sözleşme tarafları üçüncü taraf veri işleyenler veya veri sorumluları olarak sınıflandırılmalı ve KVKK ve GDPR ile uyumluluk açısından gözden geçirilmelidir. Veri toplama faaliyetlerinde kullanım veya transfer için onay ve rıza istenmelidir. Tüm veri işleme faaliyetlerinin denetim izlerini tutulmalı ve bu denetim izleri düzenli olarak incelenmelidir. Kişisel verilere erişen ve bunları işleyen tüm üçüncü taraf firmalarla Mahremiyet Etkisi Değerlendirme çalışması gerçekleştirilmelidir.

9. Organizasyonlar için yönetilen servisler modelinin değerlendirilmesi

Çalışılan organizasyon ve üçüncü taraf firmalarının risk seviyelerinin değerlendirilmesi adına, deneyimli risk uzmanları tarafından önden tanımlı ve çokça pratik edilme imkânı olmuş metotlar çerçevesinde uygulanan Yönetilen Risk Yönetimi Servisi (Risk Management as a Service) hizmetinin alımı değerlendirilmelidir.

10. Düzenli denetim faaliyetleri

Üçüncü taraf firma risk yönetim çerçevesinin, üçlü savunma hattı etrafında yapılandırılması ya da profesyonel risk süreç danışmanlığı ve denetimi alanında faaliyet gösteren ve dış kontrolcü rolünde bağımsız görüş sunabilecek organizasyonlar aracılığıyla üçüncü taraf firmaların düzenli denetimler tabii tutulması önerilmektedir.

EY konu uzmanları

Raporumuza veya hizmetlerimize ilişkin sorularınız için bizlere ulaşabilirsiniz.

EY konu uzmanları

Ümit Yalçın Şen
EY Türkiye Danışmanlık Hizmetleri Şirket Ortağı
Siber Güvenlik Hizmetleri Lideri
+90 212 315 30 00
umit.sen@tr.ey.com

Özlem Çetin
EY Türkiye Danışmanlık Hizmetleri Müdürü
Siber Güvenlik Hizmetleri
+90 212 315 30 00
ozlem.cetin@tr.ey.com

Aylin Türker
EY Türkiye Danışmanlık Hizmetleri Müdürü
Risk Hizmetleri
+90 212 315 30 00
aylin.turker@tr.ey.com

Araştırma ekibi

Bu rapor ve raporda sunulan içerikler EY Türkiye'nin yaptığı araştırma çalışmasının bir sonucudur. Rapor, herhangi bir yoruma dayanmadan, objektif veriler temel alınarak hazırlanmıştır. Sadece genel bilgi verme amacıyla sunulan bu yayın profesyonel hizmetler alanında geçerli bir kaynak olarak kullanılması amacıyla hazırlanmamıştır. Bu yayında geçen üçüncü taraf görüşleri hiçbir şekilde EY'ın resmi görüşlerini yansıtmamaktadır. Konuya ilişkin detaylı bilgiler için ilgili araştırma ekibine başvurulmalıdır.

Merve Eroğlu
Kıdemli Danışman
Siber Güvenlik Hizmetleri
+90 212 315 30 00
merve.eroglu@tr.ey.com

Sema Erkan
Kıdemli Danışman
Siber Güvenlik Hizmetleri
+90 212 315 30 00
sema.erkan@tr.ey.com

EY | Assurance | Tax | Strategy and Transactions | Consulting

EY Hakkında
EY bağımsız denetim, vergi, strateji, kurumsal finansman ve danışmanlık hizmetlerinde bir dünya lideridir. Anlayışımız ve kaliteli hizmetlerimiz dünya ekonomisi ve sermaye piyasalarında güvenin oluşmasına katkıda bulunmaktadır. EY, güçlü yönetim ekibiyle tüm paydaş gruplarına verdiği sözleri yerine getirmekte ve bu şekilde çalışanları, müşterileri ve içinde yer aldığı diğer çevreler için daha iyi bir çalışma hayatı oluşturulmasında önemli bir rol üstlenmektedir.

EY adı küresel organizasyonu temsil eder ve Ernst & Young Global Limited'in her biri ayrı birer tüzel kişiliğe sahip olan, bir veya daha çok, üye firmasını temsil edebilir. Sınırlı sorumlu bir Birleşik Krallık şirketi olan Ernst & Young Global Limited müşteri hizmeti sunmamaktadır. Kişisel Verileri Koruma Kanunu (KVKK) kapsamında; EY'ın kişisel verileri nasıl topladığı, kullandığı ve bireylerin sahip olduğu haklara dair bilgilere ey.com/tr_tr/privacy-statement adresinden ulaşabilirsiniz. Daha fazla bilgi için lütfen ey.com adresini ziyaret edin.

ey.com/tr
vergidegundem.com
facebook.com/ErnstYoungTurkiye
instagram.com/eyturkiye
twitter.com/EY_Turkiye