TÜRKİYE BANKALAR BİRLİĞİ

BANKACILAR

SAYI 135 ARALIK 2025

SAYI 135 ARALIK 2025

BANKACILAR

BANKACILAR
Yıl/Volume : 36
Sayı/Issue : 135 – Aralık 2025
Yayın Türü /Type of Publication:
Yerel Süreli Hakemli Yayın/ Refereed
Yayın Aralığı / Frequency: 3 Aylık / Quarterly
(Mart / Haziran/ Eylül/ Aralık)
(March/ June/ September/ December)

ISSN 1300-0217
e- ISSN 1307-8631
www.tbb.org.tr
Sertifika No/ Certificated Number 17188

Türkiye Bankalar Birliği adına İmtiyaz Sahibi
Nurullah Bakır

Sorumlu Yazı İşleri Müdürü
Ümit Ünsal

Yayın Sorumlusu: Özkan Sezer-Umut Dağ

İdare Merkezi
Kültür Mahallesi, Nisbetiye Caddesi, Akmerkez No:56 İç Kapı No:24 Beşiktaş / İSTANBUL

Tel : 212-282 09 73
Faks : 212-282 09 46
E-posta: tbb@tbb.org.tr

Yayınlanma Tarihi: Aralık 2025

Para ile satılmaz.

Bankacılar Dergisi Hakkında

Bankacılar dergisi, ekonomi, finans, bankacılık konularında ve bu konularla ilgili alanlarda bilimsel özgün makalelere yer veren hakemli bir dergidir.

Bankacılar, akademisyenler, araştırmacılar, uygulamada yer alan profesyoneller ve politika yapıcıları arasındaki bilgi paylaşımının artırılmasına, bankacılık mesleğinin geliştirilmesine ve literatüre katkıda bulunmayı amaçlar.

Yılda dört kez sadece elektronik ortamda yayımlanır. Üç ana bölümden oluşur. Birinci bölümde, hakemler tarafından değerlendirilen, yayımlanması uygun görülen makalelere, ikinci bölümde konferans bildirisi ve konuşma metinlerine, üçüncü bölümde ise bankacılık uygulamalarına ilişkin özel araştırma yazılarına ve çevirilere yer verilir.

Yayımlanmak üzere gönderilecek makalelerin, daha önce herhangi bir yerde yayımlanmamış olması ve değerlendirme süreci içerisinde başka bir yerde yayınlama girişiminde bulunulmaması gerekir.

Bankacılar dergisi, kabul edeceği makalelerde, kapsadığı konularla ilgili olma ve Türk Dil Kurumu ve dergi yazım kurallarına uygun olarak hazırlanma şartlarını arar Makaleler, “anonim yazar/anonim hakem” sistemine göre değerlendirilir. Uygun bulunan makaleler konu ile ilgili iki hakeme gönderilir. Hakem raporlarına göre makalelerin yayınlanıp yayımlanmayacağına karar verilir. Daha detaylı bilgi makale değerlendirme sürecinde yer almaktadır. Yayımlanacak makalelerde yazım kurallarına ve biçime ilişkin değişiklikler yapılabilir veya bunların yapılması yazardan istenebilir.

Bankacılar dergisinde yayımlanan yazılar, Türkiye Bankalar Birliği’nin resmi görüşlerini yansıtmaz; yazar ve görüş sahiplerini bağlar. Yazılardan kaynak göstererek alıntı yapılabilir. Dergiye başvurular ücretsizdir. Yayımlanması kabul edilen makalelerin elektronik tüm yayın hakları, süresiz olmak üzere Türkiye Bankalar Birliği’ne aittir. Makaleler için yazarlara telif ücreti ödenir.

Dergiye gönderilen makalelerde, COPE (Committee on Publication Ethics – Yayın Etiği Komitesi)’un hakemler, yazarlar ve editörler için uluslararası standartları dikkate alınmakta ve makalelerin araştırma ve yayın etiğine uygunluğuna dikkat edilmektedir

Dergide yayımlanması talep edilen makaleler, Birlik idare adresine, posta veya e-posta (tbb@tbb.org.tr) olarak gönderilebilir.

TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi Müdürlüğü’nden Birliğimize iletilen karar uyarınca Bankacılar Dergisi 2022 yılından itibaren dizinlenmemektedir. Ancak ULAKBİM TR Dizin tarafından Derginin daha sonra yayımlanarak iletilecek sayıları hakkında ayrıca değerlendirme yapılacağı belirtilmiştir.

Saygılarımızla,

Türkiye Bankalar Birliği

İçindekiler

Araştırma Makaleleri

Contents

Research Articles

Araştırma Makalesi/Research Article
Cilt / Volume: 36, Sayı / Issue: 135, Yıl / Year: 2025

Dijital Operasyonel Dayanıklılık Mevzuatı (DORA) ile Dijital Güven Mimarisi: Türkiye Finans Sektörüne Yansımalar

Yağızcan Yücel Çendik[1]

Öz

Özellikle son 25 yılda hızlanan ve her geçen gün daha da karmaşıklaşan teknolojik gelişmeler, getirdiği faydaların yanında aynı zamanda belirsiz bir siber risk ortamı oluşmasına da sebep olmaktadır. Ortaya çıkan ve hem doğası hem kapsamı farklılaşabilen bu yeni siber risklerin yönetimi de bireyler, kurumlar ve devletler için başa çıkılması gereken bir sorun olarak ortada durmaktadır. Sürekli gelişen ve farklılaşan saldırı çeşitleri karşısında, bireylerin ve tekil olarak kurumların mücadele edebilme ihtimali oldukça düşüktür. Bunun bir sebebi bireysel veya kurumsal olarak risklerin ortaya çıkış hızına yetişmenin imkansız olmasıdır. Bir diğer sebebi ise bireysel ve kurumsal mücadelelerin çok yüksek maliyetleri beraberinde getirmesidir. Son olarak kurumların karmaşık tedarik zincirleriyle birbirine bağlı olması bu risklerin de topyekün yönetilmesini zorunlu kılmaktadır. Çünkü "*bir zincir en zayıf halkası kadar güçlüdür.*"

İşte bu zorluklarla mücadele etmek için çoğunlukla devletler önderliğinde siber güvenlik çerçeveleri oluşturulmaya çalışılmaktadır. Bu makalede global ölçekte son dönemlerde hayata geçirilmiş iki temel düzenleme karşılaştırılacak ve bunların Türkiye'ye muhtemel yansımaları irdelenecektir. Özellikle Avrupa Birliği tarafından yayımlanan ve 17 Ocak 2025 tarihinde tam olarak uygulamaya başlanmış olan "Dijital Operasyonel Dayanıklılık Yasası (Digital Operational Resilience Act)", beş ana sütunuyla detaylıca incelenecektir. Bununla birlikte DORA'nın ortaya koyduğu Tehtit Odaklı Sızma Testi yaklaşımı, üst yönetimin hesap verebilirliğini artırması ve kritik tedarikçiler üzerindeki doğrudan denetimi gibi hükümleriyle "Ağ ve Bilgi Sistemleri Direktifi (Network and Information Security Directive)" gibi diğer çerçevelerden nasıl ayrıştığı vurgulanacaktır. Türkiye'de AB ile olan güçlü bağlantıları nedeniyle bu regülasyonlara dolaylı olarak uyum sağlama zorunluluğu bulunan ülkelerden bir tanesidir. Özellikle bu düzenlemeye uyumun rekabet avantajı olarak nasıl kullanılabileceğini ortaya koyulmaya çalışılacaktır.

Anahtar Kelimeler: DORA, Operasyonel Dayanıklılık, Regülasyon, Sistemik Siber Risk, NIS2
JEL Sınıflandırması: G28, K24

[1] Türkiye Bankalar Birliği Risk Merkezi, İç Denetim ve İç Kontrol Direktörü, yagizcancendik@gmail.com, https://orcid.org/0000-0003-2562-3987

Makale Başvuru Tarihi: 04/11/2025 Kabul Tarihi: 17/12/2025

Atıf: Çentik, Y.Y. (2025). Dijital Operasyonel Dayanıklılık Mevzuatı (DORA) ile Dijital Güven Mimarisi: Türkiye Finans Sektörüne Yansımalar. *Bankacılar Dergisi*, 35(135), 1-11.

Digital Trust Architecture through the Digital Operational Resilience Act (DORA): Implications for the Turkish Financial Sector

Abstract

Especially over the past 25 years, technological developments that have accelerated and become increasingly complex day by day have, alongside their benefits, also led to the emergence of an uncertain cyber risk environment. The management of these new cyber risks, which vary in nature and scope, has thus become a major challenge for individuals, organizations, and governments alike. Against constantly evolving and diversifying attack vectors, it is virtually impossible for individuals or organizations to cope on their own. One reason is that it is impossible to keep up with the pace at which risks emerge. Another reason is that individual or organizational efforts to combat these risks entail extremely high costs. Finally, the fact that organizations are interconnected through complex supply chains makes it necessary to manage these risks collectively, because *"a chain is only as strong as its weakest link."*

To address these challenges, cybersecurity frameworks are increasingly being developed, often under the leadership of governments. This article compares two major global regulatory initiatives introduced in recent years and discusses their implications for Turkey. In particular, it provides an in-depth examination of the Digital Operational Resilience Act (DORA), a regulation issued by the European Union and fully implemented as of 17 January 2025, through its five main pillars. Moreover, it highlights how DORA differentiates itself from other frameworks such as "Network and Information Security Directive (NIS2)", especially through its provisions that enhance the accountability of senior management and enable direct supervision over "critical" third-party providers. Given its strong ties with the European Union, Turkey is among the countries that must ensure indirect compliance with these regulations. This paper also seeks to demonstrate how alignment with such frameworks can be leveraged as a competitive advantage.

Keywords: DORA, Operational Resilience, Regulation, Systemic Cyber Risk, NIS2
JEL Classification: G28, K24

1. Giriş

Global ekonominin dijitalleşme hızı, özellikle yapay zeka teknolojilerinin entegrasyonu ile birlikte, karşı karşıya kalınan siber risk düzeyini benzeri görülmemiş bir şekilde genişletmiştir. Üstelik kuantum teknolojileri gibi nispeten yeni gelişen teknolojiler de, risk yönetimi bakış açısıyla, belirsizlik ortamını artırmaktadır. Bunun yanında kurumların operasyonları da günümüzde ulusal boyutların çok ötesine geçmiştir. OECD tarafından yayımlanan "Kurumların Bilgi ve İletişim Teknolojileri Erişimi ve Kullanımı (ICT Access and Usage by Businesses)" istatistiklerine göre 10 ve daha fazla çalışanı bulunan işletmelerde 2024 yılında Kurumsal Kaynak Planlaması (Enterprise Resource Planning) yazılımı kullanan firma oranı Avrupa Birliği üyesi ülkelerde %40.28 iken, Türkiye'de bu oran %28.68'dir. Yine aynı istatistiklere göre 2024 yılında Müşteri İlişkileri Yönetimi (Customer Relationship Management) yazılımı kullanan firma oranı Avrupa Birliği üyesi ülkelerde %25.75 iken bu oran Türkiye'de %12.13'dür. Bu istatistiklerden de anlaşılacağı gibi, günümüzde karmaşık bilgi ve iletişim teknolojilerinin kullanımı son derece yaygındır. Hızlı teknolojik gelişmeler ve karmaşıklaşan tedarik zincirleri sebebiyle kurumların artan bağımlılığı, bir sistem veya kurumdaki zaafiyetin, domino etkisiyle tüm ulusal ve hatta global istikrarı tehlikeye atma potansiyelini de beraberinde getirmektedir.

Bu karmaşık risk ortamına karşı ülkeler ve uluslararası kuruluşlar bir karşı yanıt arayışına girmiştir. Avrupa Birliği (AB) de, Dijital Operasyonel Dayanıklılık Yasası (DORA) düzenlemesiyle birlikte siber riskleri yönetmeye ve dijital operasyonel dayanıklılığı artırmaya çalışmaktadır. DORA, AB finansal hizmetler sektöründeki kuruluşların bilgi sistemlerinde ortaya çıkabilecek siber saldırılar, operasyonal aksaklıklar ve kesintilere dayanıklılıkları artırma ve bunlara karşı koyma kabiliyetlerini geliştirmeyi hedefleyen bir düzenlemedir. DORA, 16 Ocak 2023 tarihinde yürürlüğe girmiş olmasına rağmen, bir çok yeni yasal düzenleme getirmesi sebebiyle tam olarak uygulanmaya başlandığı tarih 17 Ocak 2025'tir. Bu tarih, AB pazarında faaliyet gösteren ve AB pazarına girmek isteyen her işletme için bir milat teşkil etmektedir.

DORA'dan daha önce, 2016 yılında yayımlanan NIS Direktifi, Avrupa Birliği'nin ilk siber güvenlik yasası olma niteliğini taşımaktadır. Daha sonra güncellenmiş ve güçlendirilmiş bir versiyon olan Ağ ve Bilgi Sistemleri Direktifi (NIS2) yayımlanmıştır. Bu direktif, Avrupa Birliği üyesi ülkelerde siber güvenlik seviyesini yükseltmeyi ve siber olayların ortaya çıkaracağı olumsuz sonuçlara karşı dayanıklılığı artırmayı hedeflemektedir. NIS2, kritik hizmet ve altyapı sağlayıcılarına yönelik hazırlanan bir düzenlemedir. DORA ise, özellikle finansal hizmetler sektörüne yoğunlaşmasıyla "Ağ ve Bilgi Sistemleri Direktifi" gibi düzenlemelerden farklılaşmaktadır. Bunun yanı sıra klasik bilgi güvenliği çerçevelerinde yer alan gizlilik, bütünlük ve erişilebilirlik yaklaşımının ötesinde "operasyonel dayanıklılık" vurgusu yapması da DORA'nın farklılaşan unsurlarından bir tanesidir. Burada kullanılan "dayanıklılık" terimi, siber saldırılara karşı önlem alınmasının ötesinde bir anlam ifade etmektedir. Dayanıklılık, aynı zamanda bir olay (incident) yaşandığında kritik işlevleri sürdürme ve mümkün olan en kısa sürede toparlanma kabiliyetini de zorunlu kılmaktadır.

Türkiye'de henüz yeterince üzerinde durulmamakla birlikte, DORA'nın getirdiği bu yeni düzenlemeler, AB pazarıyla iş yapmak isteyen tüm kurumların ve bu kurumlara hizmet sağlayan üçüncü tarafların dolaylı olarak uyması gereken kuralları içermektedir. Bu anlamda AB pazarında rekabet avantajı elde etmek isteyen kurumların DORA'ya uyumlu olması son derece önemlidir. Bunun ötesinde DORA'ya uyum, global çapta bir güven inşa edilmesine sebep olacağı için AB ile doğrudan ilişkisi olmayan kurumlar için bile siber dayanıklılık stratejileri oluşturmada en önemli yol göstericilerden bir tanesi olacaktır.

Bu makale, söz konusu yasal düzenlemeyi, mevcut yasal düzenlemelerle karşılaştırmalı olarak inceleyecek, Türkiye'de yürürlükte olan benzer düzenlemelerle benzeştikleri ve

ayrıştıkları noktaları ortaya koyacaktır. Aynı zamanda DORA'nın Türkiye finans sektörü için ne anlam ifade ettiği de tartışılacak ve öneriler getirilecektir.

2. DORA'nın Kapsamı ve Yapısı: Kimleri Kapsıyor ve Hangi Alanları Dönüştürüyor?

DORA, Avrupa Birliği'nin finansal hizmetler sektöründeki en kapsamlı dijital düzenlemesidir. Düzenlemenin diğer düzenlemelerden farklılaştığı en temel noktası ve bizce en büyük gücü, yalnızca finansal kuruluşları değil, aynı zamanda bu finansal kuruluşlara hizmet sağlayan üçüncü tarafların da bu düzenlemelerin kapsamına dahil edilmesinden kaynaklanmaktadır. Bu açıdan DORA hemen hemen tüm sektörlere temas eder. Bunlar arasında bankalar, kredi kuruluşları, yatırım firmaları, sigorta ve reasürans şirketleri, ödeme ve e-para kuruluşları, kripto varlık hizmet sağlayıcıları gibi finansal kurumlar ve buna ilave olarak bu kurumlara hizmet sağlayan bulut sağlayıcıları gibi üçüncü taraflar da DORA'nın kapsamında yer almaktadır. Kapsamın bu kadar geniş tutulmasının ana nedeni, finansal sektörün ulusal ve global ekonomilerde çok önemli bir yer tutmasıdır. Özellikle büyük ölçekli finansal kurumlarda meydana gelen bozulmaların, global olarak sistemik risk yarattığı onlarca defa tecrübe edilmiştir.

Sistemik risk, tek bir kurumun başarısızlığı gibi tetikleyici bir olayın, ekonomik sonuçları itibariyle bir zincir halinde geniş çevrelere yayılmasını ve sonuç olarak finansal kurumların veya piyasanın çöküşüne sebep olmasını ifade eder. Finansal kurumların iflas etmesi, geri kalan tüm kurumların da sermaye ve finansman olanaklarından mahrum kalması ve sermaye maliyetinin artması anlamına gelecektir. Çünkü finansal kurumlar, sermayenin en önemli kaynaklarıdır. Bu açıdan sermaye maliyetindeki artış veya sermaye erişimindeki azalma, sistemik bir çöküşün en ciddi sonuçları arasında yer almaktadır (Schwarcz, 2008).

Siber saldırılar ise, devletleri, bireyleri ve işletmeleri global ölçekte etkileyebilen saldırılardır. Nitekim son yıllarda Amerika Birleşik Devletleri'nde gerek seçim sistemlerine yönelik gerçekleştirilmeye çalışılan siber saldırılar, gerekse de dünyanın en büyük şirketlerini hedef alan siber saldırılar, bu saldırıların sonuçlarının yıkıcılık seviyesini de ortaya koymaktadır. Sistemik siber risk de en basit haliyle, yukarıda yapılan sistemik risk tanımının siber ortamda gerçekleşen haline verilen addır. Dünya Ekonomik Forumu'na göre sistemik siber risk, "tek bir kritik altyapı bileşeninde meydana gelen siber olayın, önemli kesintilere ve kayıplara neden olması ve bunun etkilerinin geniş bir çevreye zincirleme biçimde yayılması" riskidir (World Economic Forum, 2016). Bu anlamda siber sistemik riskler, geniş bir çevreye etki etmeleri ve yıkıcı sonuçlar doğurmaları sebebiyle günümüzde üzerlerinde ciddi olarak durulması gereken risklerin başında gelmektedir.

DORA'nın bu kadar geniş bir çevreyi kapsamasının bir diğer önemli sebebi de finansal ekosistemde görülen bulaşma (contagion) riskidir. Sistemik risk ile doğrudan bağlantılı olan bulaşma, bir kurumda meydana gelen olayın, diğer kurum veya sektörlere yayılmasını ifade etmektedir. Finansal kurumlar da bulaşma etkisinin en yüksek olduğu sektörlerden bir tanesidir. Hatta finansal kurumlar içerisinde de bu yayılma etkisinin şiddeti açısından sıralama yapmak mümkündür. Örneğin finansal krizlerin yayılmasında bankalar, sigorta şirketleri ve diğer aracı kurumlara nispetle daha büyük bir rol oynamaktadır (Billo, Getmansky, Lo ve Pelizzon, 2012).

Avrupa Sistemik Risk Kurulu (ESRB), sistemik siber risklere ilişkin 2020 tarihinde yayımladığı raporda, siber olayların meydana gelme sıklığına vurgu yapmış ve siber saldırıların sonuçlarının giderek daha maliyetli ve yıkıcı olacağına dikkat çekmiştir. Buna göre finansal sektörde meydana gelen siber olaylar çok hızlı ve geniş bir çevreye kolaylıkla yayılabilmektedir. Finansal hizmetler sektörü de, giderek yaygınlaşan yeni teknolojik çözümler ve bunun getirdiği bilgi ve iletişim teknolojilerinin birbirine bağımlılığı sebebiyle potansiyel yıkıcı

etkinin en önemli hedeflerinden bir tanesidir. Buna ek olarak bulut bilişim gibi bazı yeni teknolojilerde ortaya çıkan yeni bağımlılıklar da kurumlar için dayanıklılığı artırmakla birlikte yeni risklerin de ortaya çıkmasına sebep olmaktadır (ESRB, 2020). Bu eğilimin önümüzdeki dönemde de hızlanarak devam edeceğine ise şüphe yoktur. Çünkü eskiden ulaşılması son derece güç olan gelişmiş araçlar ve yöntemler, artık herkes tarafından erişilebilir bir hale gelmiştir.

DORA da bu anlamda finans sektöründe meydana gelen kırılganlıkların finansal aktarım kanalları aracılığıyla yayılacağını ve genel bir güven kaybı yaratacağını vurgulamaktadır. 2008 finansal krizinin ardından yayımlanan düzenlemeler her ne kadar finansal dayanıklılığı güçlendirse de operasyonel dayanıklılığın bir parçası olan dijital dayanıklılığa yeteri kadar önem verilmemiştir (Avrupa Birliği, 2022). İşte sayılan bu sebeplerle DORA ile birlikte üçüncü taraflar dahil meydana gelebilecek siber olayların, birden fazla finansal kuruluşu aynı anda etkileme riskine karşı sistemik bir dayanıklılık oluşturulması hedeflenmektedir.

3. Kritik Üçüncü Taraf Bilgi ve İletişim Teknolojileri Hizmet Sağlayıcıları

Bulaşma etkisi ile bir kurumda meydana gelen bir olayın sistemik risk yaratma ihtimali üzerinde durmuştuk. Bulaşma etkisini minimuma indirmek ve siber sistemik riski güvenle yönetmek için ise sistemin en zayıf halkası olan dayanıklılığı düşük kurumları ve bunun yanında kritik öneme sahip kurumları belirlemek ve bunlara yönelik önlemler almak son derece önemlidir. Genellikle, operasyonel dayanıklılığı en düşük olan kuruluşlara yönelik politikalar tasarlamak beklenen faydayı sağlamayabilir. Yapılan bilimsel araştırmalar bu politikaları en zayıf kurumlara yönlendirmek yerine yüksek tehdit altında bulunan kurumlara yönlendirmenin daha başarılı sonuçlar doğuracağını ortaya koymaktadır (Summer, 2013).

Finansal kuruluşların fiziksel dayanıklılığı ile dijital dayanıklılığı arasındaki güçlü bağlantılar sebebiyle kritik kuruluşların belirlenmesi son derece önemlidir. DORA'ya göre kritik kurumlar, finansal kuruluşlara hizmet veren ve yaşanabilecek herhangi bir olumsuzlukta tüm finansal sistemi çökertme potansiyeli taşıyan teknoloji şirketleridir. Bunların belirlenmesinde Avrupa Denetleme Otoriteleri (ESAs) önemli bir rol oynar. Kritiklik değerlendirmesi yapılırken göz önünde bulundurulan temel kriterler şunlardır[2]:

- **Sistemik etki:** Hizmet sağlayıcının kaç firmaya hizmet verdiği ve bu hizmet alan kuruluşların finansal sistemdeki ağırlığı ile doğru orantılıdır. Eğer bir hizmet sağlayıcıda meydana gelen bir olumsuzluk piyasa istikrarını etkileyecek boyuttaysa kritik olarak değerlendirilir.

- **Kritik fonksiyon desteği:** Temin edilen hizmetin finansal kuruluşların önemli işlevlerini yerine getirmesini destekleyip desteklemediği kritiklik değerlendirmesinde önemlidir. Bu kriter, aşağıda bahsedeceğimiz ikame edilebilirlik kriteriyle birlikte değerlendirilebilir.

- **İkame edilebilirlik:** Hizmet veren firmaların tekel olup olmadığı da kritiklik değerlendirilmesinde önemlidir. Eğer temin edilen hizmet finansal kurumlar için olmazsa olmaz bir hizmetse ve piyasada bu hizmeti sağlayacak başka bir kurum yoksa hizmet sağlayıcı kritik olarak değerlendirilir.

[2] European Parliament and the Council of the European Union, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act – DORA). Official Journal of the European Union, L 333, 1–93. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554

- **Sınır ötesi bağımlılık:** Hizmet sağlayıcının farklı Avrupa Birliği üyesi devletlerdeki finansal kurumlara hizmet verip vermediği de kritikliğin belirlenmesinde bir diğer kriterdir. Eğer bir hizmet sağlayıcı, birden çok ülkede hizmet veriyorsa kritik olarak değerlendirilebilir.

DORA'ya tabi olan finansal kuruluşlar, önemli fonksiyonlar için kullandıkları tüm bilgi ve iletişim teknolojileri hizmet sağlayıcılarını yetkili mercilere bildirmek zorundadır. Ulusal makamlar aracılığıyla Avrupa Denetleme Otoriteleri'ne iletilen bu raporlar üzerinden hizmet sağlayıcılarının kritik olup olmadığı değerlendirilir. Kritik olarak değerlendirilen firmalar DORA'nın "Gözetim Çerçevesi (Oversight Framework)"ne dahil olur. Bu çerçeve uyarınca kritik olarak değerlendirilen kurumlarda denetim faaliyeti yürütmek üzere bir baş denetçi (Lead Overseer) atanır. Baş denetçiler, bu kritik kurumların bilgi ve iletişim teknolojileri risklerini yönetmek amacıyla kapsamlı ve etkili politika ve prosedürlere sahip olup olmadığını değerlendirir ve raporlar.

DORA, dijital operasyonel dayanıklılığın sağlanması için kurumların uygulaması gereken gereksinimleri beş ana başlık altında toplamaktadır:

1. **Bilgi ve İletişim Teknolojileri Risk Yönetimi:** DORA'nın ikinci bölümünü oluşturan bilgi ve iletişim teknolojileri risk yönetimi, yasanın temelini oluşturur ve DORA'ya tabi kuruluşların siber riskleri nasıl yönetmesi gerektiğini genel hatlarıyla düzenler. Buna göre kuruluşlar, kritik işlevlerini destekleyen tüm bilgi ve iletişim teknolojileri sistemlerini ve süreçlerini proaktif bir şekilde yönetmelidir. Finansal kuruluşlar, yüksek düzeyde dijital operasyonel dayanıklılık sağlamak amacıyla bir yönetişim ve kontrol çerçevesine sahip olmalıdır. Bu çerçevenin hazırlanması ve güncel tutulması ilgili kuruluşun yönetim organının sorumluluğundadır.
2. **Bilgi ve İletişim Teknolojileriyle İlişkili Olayların Yönetimi, Sınıflandırılması ve Raporlanması:** Bu bölüm, kurumların bilgi ve iletişim teknolojileri olaylarını nasıl yöneteceğini düzenlemektedir. Özellikle, önemli olaylarının tanımlanması, sınıflandırılması ve standartlaştırılmış şablonlar kullanılarak yetkili ulusal makamlara raporlanması zorunludur. Burada olayların raporlanmasında standart şablonlar kullanılması ve katı bir zaman çizelgesi ortaya konulmuş olması önemlidir.
3. **Dijital Operasyonel Dayanıklılık Testi:** Düzenlemenin dördüncü bölümü olan dijital operasyonel dayanıklılık testi bölümü, ortaya konulan en kritik yeniliklerden biridir. Bu düzenleme, kurumların kritik sistemleri ve uygulamaları üzerinde periyodik olarak dayanıklılık testleri yapmalarını zorunlu kılar. Kuruluşlar, yıllık düzenli olarak yapacakları güvenlik testlerinin yanı sıra, kritik üçüncü tarafların da dahil edildiği ve en az üç yılda bir yapılacak Tehdit Odaklı Sızma Testi (Threat Led Penetration Testing) de yaptırmak zorundadır.
4. **Üçüncü Taraf Bilgi ve İletişim Teknolojileri Riskinin Yönetimi:** DORA, finansal kuruluşların bilgi ve iletişim teknolojileri hizmet sağlayıcılarıyla olan tüm sözleşmelerini izlemesini ve yönetmesini zorunlu kılar. Bu bölümde, sözleşmede yer alması gereken zorunlu unsurlar belirlenmiştir. Bunun yanı sıra kritik üçüncü taraf hizmet sağlayıcıları için Avrupa Denetleme Otoriteleri tarafından gerçekleştirilecek doğrudan denetim de bu bölümde düzenlenmektedir. Bu denetim ile finansal ekosistemin güvenliğinin sağlanması amaçlanmaktadır.
5. **Bilgi Paylaşımı:** Bu bölüm, siber tehditler ve zafiyetler hakkındaki bilgilerin finansal kuruluşlar arasında gönüllülük esasına dayalı olarak paylaşılmasını düzenlemektedir. Bahsi geçen bilgi paylaşımı sayesinde sektörün kolektif olarak dayanıklılığı artacaktır.

4. Genel Amaçlı Çerçeveler ve DORA: Amaçtaki Birliktelik, Uygulamadaki Farklar

DORA ve "Ağ ve Bilgi Sistemleri Güvenliği Direktifi (NIS/NIS2)", Avrupa Birliği'nin siber güvenlik ve operasyonel dayanıklılık stratejisinin iki temel ayağını oluşturmaktadır. Her iki düzenleme de dijital güveni sağlamayı ortak hedef olarak benimserken, kapsam, odak ve spesifik gereklilikler açısından farklılaşmaktadır. İki düzenlemenin benzeşen ve farklılaşan noktalarını anlamak, finansal hizmetler sektörü başta olmak üzere bu iki düzenlemeye de tabi olan kuruluşlar için son derece önemlidir.

Temel olarak DORA ve NIS2'nin benzeştiği noktalar risk yönetimi, yönetişim, hesap verilebilirlik, tedarik zinciri güvenliği ve raporlama yükümlülükleridir. Bu düzenlemelerde yönetim kurulları ve üst yönetimden sorumlu olanlar, bilgi ve iletişim teknolojilerinden doğan riskler başta olmak üzere, risklerini kurumsal stratejilere entegre etmekle ve bunlara uyum için sorumluluk almakla mükelleftir. Böylece en üst seviyede katılım ve hesap verebilirlik sağlanmış olacaktır. Ayrıca siber güvenlik yalnızca teknik bir sorumluluk olmaktan çıkmakta ve kurumsal bir öncelik haline gelmektedir. Bir diğer benzeştikleri nokta da proaktif bir risk yönetimi sürecini zorunlu tutmalarıdır. Kuruluşlar proaktif bir şekilde risklerini yönetmeli, bunun için bir risk yönetimi çerçevesi oluşturmalı, bu risk yönetimi çerçevesi doğrultusunda risklerini belirlemeli, belirledikleri bu riskleri sürekli olarak izlemeli ve nihayet bunlara karşı kurumsal risk cevaplarını oluşturmalıdır.

Ayrıca her iki düzenlemede de üçüncü taraf riski üzerinde çokça durulmaktadır. Bu düzenlemelere tabi kuruluşlar, üçüncü taraf risk yönetimi ve tedarik zinciri güvenliğini sağlayacak önlemler almakla yükümlüdür. Son olarak kuruluşların raporlama yükümlülükleri de benzeşen bir diğer hususdur. Her iki düzenleme de önemli olayların ilgili otoritelere zamanında raporlanmasını zorunlu tutar. Her ikisinin de raporlama süreci son derece benzerdir. Buna göre olaydan sonra ilk rapor 24 saat içinde yetkililere iletilmeli, NIS2'de detaylı rapor 72 saat içinde hazırlanmalı ve nihai rapor her ikisi için de bir ay içerisinde raporlanmalıdır.

Benzerliklerine rağmen, DORA ve NIS2 arasında bir çok konuda farklılıklar da bulunmaktadır. Bunlardan ilki yasal nitelikleridir. DORA, tüm Avrupa Birliği üye devletlerinde doğrudan uygulanması gereken yasal bir düzenleme iken; NIS2, Avrupa Birliği üyelerinin belirli bir süre içerisinde ulusal yasalarına aktarması gereken bir direktiftir. Bu boyutuyla DORA uluslararası bir düzenleme iken NIS2 her üye devletin kendi hukuk sistemine entegre edeceği bir düzenlemedir. Hatta DORA'nın NIS2'ye karşı normlar hiyerarşisinde regülatif önceliği bulunmaktadır. Yani finansal hizmetler sektörü özelinde düzenlemeler arası bir çelişki olması durumunda, DORA hükümleri özel kanun (lex specialis) olarak NIS2 hükümlerine göre önceliklidir.

Bunun yanı sıra DORA ile NIS2 arasındaki temel farklılık odaklandıkları sektörlerdir. DORA, münhasıran finansal hizmetler sektörüne ve bunların kritik hizmet sağlayıcılarına odaklanırken; NIS2, enerji, sağlık, ulaşım ve dijital hizmetler gibi geniş bir yelpazedeki kritik altyapı sektörlerine odaklanmaktadır. DORA ayrıca kritik hizmet sağlayıcıların doğrudan Avrupa Birliği organları tarafından denetlenmesini sağlayan bir gözetim modeli getirir. NIS2 ise kritik üçüncü taraf hizmet sağlayıcılarına yönelik bir gözetim mekanizması önerir, ancak doğrudan denetim yetkisi vermez.

Son olarak DORA'nın hem NIS2 hem de diğer risk yönetimi çerçevelerinden farkı, getirmiş olduğu yeni test yükümlülüğüdür. DORA'da Tehtit Odaklı Sızma Testi, "gerçek bir siber tehdit oluşturduğu değerlendirilen tehdit aktörlerinin taktik, teknik ve prosedürlerini taklit eden; finansal kuruluşun kritik, canlı üretim sistemleri üzerinde kontrollü, özel olarak tasarlanmış ve istihbarat odaklı test gerçekleştiren bir çerçeveyi" ifade eder. Aşağıdaki tablo, DORA ve NIS2'nin temel benzerliklerini ve farklarını özetlemektedir:

	DORA	NIS2
Yasal Nitelik	Tüzük niteliğindedir ve tüm AB'de doğrudan uygulanır	Direktif niteliğindedir ve ulusal hukuka uyarlanır
Sektörel Odak	Finansal hizmetler ve kritik hizmet sağlayıcıları	Geniş kritik altyapı hizmetleri (Enerji, Sağlık, Ulaşım, Dijital Hizmetler vb.)
Temel Odak	Kesintilere karşı koyma ve kurtarma	Bilgi sistemlerinin güvenliğini sağlama
Test Zorunluluğu	Kritik kurumlar için Tehdit Odaklı Sızma Testi zorunludur (en az 3 yılda 1)	Genel sızma ve güvenlik testleri önerilir
Üçüncü Taraf Denetimi	Kritik sağlayıcılara AB yetkililerince doğrudan denetim yetkisi vardır	Risk yönetimi zorunludur ancak hizmet sağlayıcılar üzerinde doğrudan denetim yetkisi yoktur

DORA ve NIS2 gibi yasal düzenlemeler, temel bir bilgi güvenliği çerçevesi sunmakta ve operasyonel dayanıklılığı artırarak kurumlara değer katmaktadır. Ancak bu düzenlemelere uymamak da kurumlar için ciddi sonuçlar doğurabilmektedir. Bu sonuçlar operasyonel aksaklıklar ve itibar kaybı gibi zararların yanı sıra ciddi boyutlardaki idari para cezalarını da kapsamaktadır. NIS2, kurumların yıllık cirolarına göre bir para cezası öngörmektedir. DORA ise düzenlemede belirtilen yetkili makamlara düzeltici tedbirler ve cezai yaptırımlar uygulama yetkisi vermektedir.

5. Türkiye Perspektifi ve Stratejik Çıkarımlar: DORA'dan Çıkarılan Dersler

DORA tüzük niteliğinde olması nedeniyle Avrupa Birliği üyesi ülkelerde faaliyet gösteren kuruluşlar için bir zorunluluk teşkil etmektedir. Türkiye'de faaliyet gösteren kuruluşlar ise doğrudan DORA'nın kapsamı içerisinde bulunmamaktadır. Ancak Avrupa Birliği üyelerinde faaliyet gösteren veya bu ülkelerde faaliyet gösteren kuruluşlara hizmet sağlayan Türk firmalarının bu düzenleye uymaları zorunludur.

Türkiye'nin ticari ve finansal ilişkilerinin büyük bir kısmı Avrupa Birliği üyesi ülkeler ile gerçekleştirdiği göz önüne alındığında, DORA'nın etkileri Avrupa Birliği'ndeki finansal kuruluşlara hizmet ihraç eden Türk şirketlerini de kapsamaktadır. DORA'ya uyum, bu firmalar için Avrupa Birliği pazarına erişimin temel bir zorunluluğu ve uluslararası rekabet gücünü koruma aracı haline gelecektir. Özellikle Avrupa Birliği üyesi ülkelerde şubeleri veya iştirakleri bulunan Türk finansal hizmet kuruluşları ve Avruoa Birliği'ne doğrudan hizmet veren bilgi ve iletişim teknolojileri firmaları DORA'ya uymak zorundadır. Bunun yanı sıra DORA'nın getirdiği tehdit odaklı testler ve kapsamlı olay yönetimi gibi avantajlar, dijital güvenin inşasında önemli bir temel sağlamaktadır.

Türkiye'nin siber güvenlik çerçevesi, Avrupa Birliği'nin iki temel mevzuatı olan NIS2 Direktifi ve Dijital Operasyonel Dayanıklılık Yasası ile paralellik göstermektedir. NIS2 Direktifi, hedeflediği sektörler bakımından 2025 yılında yayımlanan "Siber Güvenlik Kanunu" ve bu

kapsamda kurulan Siber Güvenlik Başkanlığı ile önemli ölçüde örtüşmektedir. NIS2, finans sektörünün yanı sıra ulaştırma, enerji, sağlık, dijital altyapı ve kamu hizmetleri gibi kritik hizmet sağlayıcılarına yönelik bir siber güvenlik standardı getirmeyi amaçlamaktadır. Siber Güvenlik Kanunu'nu da benzer şekilde ulusal kritik altyapıları ve temel hizmetleri düzenlemektedir. Bu anlamda Siber Güvenlik Kanunu, NIS2'nin Türkiye'deki eşdeğeri olarak değerlendirilebilir.

DORA'nın kapsamı ise finansal hizmetler sektörü ve onun kritik tedarikçilerinden ibarettir. Türkiye'de bu yapı farklı bir şekilde kurgulanmıştır. Buna göre Türkiye'de finansal sektörün düzenlenmesi farklı otoriteler tarafından gerçekleştirilmektedir. Bankalar başta olmak üzere finansal kiralama, faktoring, finansman ve varlık yönetim şirketlerinin bilgi sistemleri Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından; ödeme ve elektronik para şirketlerinin bilgi sistemleri Türkiye Cumhuriyet Merkez Bankası (TCMB) tarafından ve son olarak sigorta şirketleri Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu (SEDDK) tarafından düzenlenmektedir. Özellikle BDDK tarafından yayımlanan 3 temel düzenleme, finansal sektörün siber güvenlik ve bilgi sistemleri yönetimi altyapısını sağlam bir temele oturtmaktadır.

Buna göre "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik", COBIT benzeri bir yapıyla bankaların tüm bilgi sistemleri yönetişimi ve altyapısına ilişkin düzenlemeler getirmektedir. Yönetmelik'de Bilgi Sistemleri Strateji Komitesi ve Yönlendirme Komitesi gibi kurumsal yapılar tanımlanmıştır. Yönetim Kurulu ile üst yönetimin sorumlulukları ortaya konulmuştur. Bilgi varlıklarının envanteri, sınıflandırılması ile gizlilik, bütünlük ve erişilebilirlik gereksinimleri düzenlenmiştir. Ayrıca bankaların dış hizmet alımına ilişkin hükümler bulunmaktadır. Finansal kiralama, faktoring, finansman ve varlık yönetim şirketleri için de benzer yönetmelikler yayımlanmış ve benzer düzenlemeler getirilmiştir.

Bununla birlikte 3 temel düzenleme olarak belirttiğimiz düzenlemelerden ikincisi "Bilgi Sistemlerine İlişkin Sızma Testleri Hakkında Genelge"dir. Bu genelgede güvenlik açıklarını tespit etmek amacıyla, icrai görevi bulunmayan bağımsız ekipler tarafından yılda en az bir kez sızma testi yaptırılması zorunlu tutulmuştur. Son olarak "Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik" ile de BDDK denetimi altındaki kuruluşların bilgi sistemleri ve iş süreçlerinin bağımsız denetim kuruluşları tarafından denetlenmesi düzenlenmiştir.

Bankacılık ve finansal hizmetler sektörüne yönelik bu düzenlemelerin haricinde, 2018 yılında kurulan Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (DDO) de bir bilgi ve iletişim rehberi yayımlamıştır. Bu rehberde, DORA ve NIS2'yle paralel şekilde kritik altyapı niteliğinde hizmet veren kuruluşlar tanımlanmış ve bunlar ile birlikte kamu kurum ve kuruluşları için asgari bilgi sistemleri güvenlik tedbirleri belirlenmiştir. Siber olay yönetimi süreci, rehberde tanımlanan Siber Olaylara Müdahale Ekipleri (SOME) ve Siber Olaylara Müdahale Merkezi (USOM) sayesinde operasyonel işbirliğini içerecek şekilde düzenlenmiştir. Ayrıca Rehber, varlık gruplarının kritiklik derecesinin ve bunlara uygulanacak tedbirlerin belirlenmesini önermektedir. Kritik varlık grupları için ise, DORA'da tanımlanan Tehdit Odaklı Sızma Testi yaklaşımına benzer şekilde, "Kırmızı Takım Tatbikatı" yapılmasını zorunlu tutulmuştur.

Türkiye'de finansal hizmet sektörüne yönelik çıkarılan düzenlemeler ile siber risk yönetimi ve dijital operasyonel dayanıklılık önemli bir seviyeye getirilmiştir. Bununla birlikte Dijital Dönüşüm Ofisi Bilgi ve İletişim Rehberi ile de sektör ayrımına gidilmeden, yatay bir düzlemde kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren kuruluşların bilgi sistemleri düzenlenmiştir. Son olarak Siber Güvenlik Yasası ile bu alanda bütünleşik bir çerçeve ortaya konulmuştur. Bu anlamda Türkiye'de, Avrupa Birliği'nde uygulanan DORA ve NIS2 ile benzer bir yapı mevcuttur. Bu sebeple DORA'yı BDDK, SEDDK ve TCMB düzenlemeleri ile; DDO'yu ve Siber Güvenlik Yasası'nı ise NIS2 düzenlemeleriyle kıyaslamak uygun olacaktır.

BDDK düzenlemeleri DORA ile benzer şekilde sadece finansal hizmetler sektörüne ilişkin hükümler içermektedir. Her iki düzenleme de yönetim kurullarına belirli seviyelerde sorumluluklar atamakta ve belirli bir bilgi sistemleri yönetişimi yapısı oluşturulmasını zorunlu tutmaktadır. Bu düzenlemelerde siber risk yönetimi için kontroller ortaya konmaktadır. Siber olay yönetimi ve bunların raporlanması da benzer şekilde düzenlenmiştir. Buna göre her iki düzenlemede de siber olaylar 24 saat içerisinde bildirilecektir. DORA'da 1 ay içinde detaylı rapor talep edilirken, BDDK düzenlemesinde belirli bir süre verilmemiş ve makul bir süre içerisinde detay rapor istenmiştir.

Türkiye'de finansal hizmetler sektörüne ilişkin düzenlemeler ile Avrupa Birliği'nde DORA düzenlemeleri arasında önemli farklar da mevcuttur. Örneğin iş sürekliliği ve olağanüstü durum testleri konusunda BDDK düzenlemeleri bankalar için her yıl en az bir kez yaptırılacak genel sızma testini zorunlu tutar. Ancak DORA, sızma testinin yanı sıra dijital operasyonel dirençlilik testlerini zorunlu tutmakta ve Tehdit Odaklı Sızma Testi yapısı ile daha geniş bir yaklaşım sunmaktadır. Bir diğer önemli fark da üçüncü taraf hizmet sağlayıcılarına ilişkindir. BDDK düzenlemelerinde dış hizmet tanımı ve bu hizmetlerden doğabilecek riskleri yönetmek üzere belirli bir risk yönetimi gereksinimleri tanımlanmıştır. Ancak bu daha çok sözleşmeler üzerinden ve sınırlı bir kapsamda düzenlenmiştir. DORA'da ise kritik üçüncü taraf hizmet sağlayıcıları tanımlanmış, düzenleyicilerin bunlar üzerinde doğrudan denetim yetkisi düzenlenmiştir.

6. Sonuç ve Öneriler

Teknolojik gelişmelerin ve dijitalleşmenin ivme kazandığı, yapay zeka ve kuantum hesaplama gibi yeni teknolojilerin hızla artan, henüz olgunlaşmamış riskler yarattığı ve her geçen gün daha da karmaşıklaşan siber risklerin bulunduğu bir dönemde Dijital Operasyonel Dayanıklılık Yasası (DORA)'nın, 17 Ocak 2025'te tam olarak uygulamaya alınması, özellikle Avrupa Birliği finansal hizmetler sektörü için bir milat olmuştur. Bu makale, bu miladın ne ifade ettiğini ve Türkiye'ye ilişkin ne gibi yansımaları olabileceğini ortaya koymayı ve Türkiye'deki mevcut yasal düzenlemelere ilişkin öneriler getirmeyi hedeflemektedir. Türkiye'de finansal hizmetler sektörüne ilişkin yayımlanan yasal çerçeve sağlam bir temel sunsa da, Avrupa Birliği düzenlemelerine uyum Türk firmaları için son derece önemlidir. Çünkü bu uyumun getireceği rekabet avantajı dahil bir çok avantaj bulunmaktadır.

Avrupa Birliği'nde DORA ile finansal dayanıklılık ve NIS2 ile genel kritik altyapı güvenliği net bir şekilde ayrılırken ve her ikisi de tek tip standartlar hedeflerken, Türkiye'de finansal dayanıklılık standartları, farklı düzenleyici kurumların mevzuatları arasında farklılaşabilmektedir. Örneğin Türkiye'de faaliyet gösteren bir banka ile bir faktoring firmasının hangi aralıklarla sızma testi yaptıracağı farklı yönetmeliklerde farklı şekilde düzenlenmiştir. Bu durum, Türkiye'nin AB pazarına hizmet ihraç eden finansal kuruluşları için uyum sürecini de karmaşıklaştırabilecektir. Bunun da ötesinde BDDK'nın bankalar için yılda en az bir kez yaptırılmasını zorunlu kıldığı sızma testi yapısını, gerçek siber tehdit aktörlerini simüle eden Tehdit Odaklı Sızma Testi yaklaşımı ile güçlendirmek, ulusal düzenlemeler vasıtasıyla DORA'ya uygun bir yapı tasarlanmasını sağlayacaktır. Bu, uyumun getireceği faydaların yanında, daha kapsamlı bir test gerçekleştirilmesi yoluyla kuruluşların operasyonel dayanıklılığını ve güvenliğini de artıracaktır.

Bir diğer önemli nokta da AB düzenlemelerinde yer alan üçüncü taraf hizmet sağlayıcılara yönelik yaklaşımdır. Türkiye'de BDDK düzenlemelerinde dış hizmet ve destek hizmeti tanımlanmıştır. Ancak DORA düzenlemelerine benzer şekilde kritik hizmet sağlayıcıların tanımlanması, bunlara ilişkin doğrudan bir gözetim ve denetim yapısının oluşturulması sistemik riskin yönetilmesine katkı sağlayacaktır. Bu sayede, Türkiye'deki finansal hizmet sektörü bütünsel olarak siber olaylara ve olası kesintilere karşı daha dirençli hale gelecektir.

Sonuncusu ve belki de en önemlisi, Türkiye'de de düzenlemelerin bütüncül bir yaklaşımla ve tüm finansal hizmetler sektörünü kapsayacak şekilde yapılması son derece önemlidir. Yani BDDK, SEDDK, Türkiye Cumhuriyet Merkez Bankası, Siber Güvenlik Başkanlığı ve Dijital Dönüşüm Ofisi düzenlemelerinin tek bir çerçeve düzenleme ile bütüncül bir çatıda toplanması yararlı olacaktır. Türkiye'deki finansal sektör regülasyonunun parçalı yapısı, dirençlilik ve siber güvenlik konusunda sektör genelinde yeknesaklığı ve sistemik risk yönetimini zorlaştıran bir yapı teşkil edebilir.

Siber Güvenlik Başkanlığının kurulmasıyla birlikte, Türkiye'de bu parçalı yapıyı bütünleştirme ve uluslararası standartlara uyumu hızlandırma yolunda önemli bir adım atılmıştır. NIS2'nin kapsamına giren sektörlerde yeknesaklığın sağlanması için Siber Güvenlik Başkanlığı merkezi rol oynarken, DORA'nın finansal hizmetler sektöründeki zorunlulukları için BDDK, SEDKK ve TCMB tarafından ortak bir operasyonel dayanıklılık mevzuatı oluşturması faydalı olacaktır. Bu stratejik uyum, Türk finans sektörünün küresel pazarda rekabet gücünü korumasının ve AB ile olan ticari bağlarını sürdürmesini de kolaylaştıracaktır.

Finansal hizmetler sektörünün bilgi sistemleri yönetişimi, risk yönetimi ve operasyonel dayanıklılığını düzenleyen bütüncül bir çerçeve yaklaşımının da bazı riskleri vardır. Çünkü finansal kurumlar arasında gerek operasyonel gerekse de kaynak olarak büyük farklar bulunabilmektedir. Örneğin bir banka ile bir varlık yönetim şirketinin sermayesi, işlem hacmi ve insan kaynağı eşit değildir. Dolayısıyla yayımlanacak düzenlemelerin bu farklılıkları da gözetmesi gerekecektir. Bu da farklı çalışmalarda detaylıca ele alınması gereken bir konu olarak önümüzde durmaktadır.

Kaynakça

Avrupa Parlamentosu ve Avrupa Konseyi. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act – DORA). Official Journal of the European Union, L 333, 1–93. 10.09.2025 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 adresinden erişildi.

Avrupa Parlamentosu ve Avrupa Konseyi. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). Official Journal of the European Union, L 333/80. 08.09.2025 tarihinde https://eur-lex.europa.eu/eli/dir/2022/2555/oj adresinden erişildi.

Bankacılık Düzenleme ve Denetleme Kurumu. (2019). Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ. T.C. Resmî Gazete (Sayı: 30737, Tarih: 06.04.2019)

Billo, M., Getmansky, M., Lo, A., & Pelizzon, L. (2012). Econometric measure of connectedness and systemic risk in the finance and insurance sector. Journal of Financial Economics, 104(3), 535–559.

European Systemic Risk Board. (2020). Systemic cyber risk. European Systemic Risk Board. 10.09.2025 tarihinde https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf adresinden erişilebilmiştir.

OECD. Key ICT Indicators. 09.09.2025 tarihinde http://www.oecd.org/sti/broadband/oecdkeyictindicators.html adresinden erişildi.

Schwarcz, S. L. (2008). Systemic risk. Duke Law School Legal Studies Research Paper Series, 163.

Summer, M. (2013). Financial contagion and network analysis. Annual Review of Financial Economics, 5(1), 277–297.

Türkiye Büyük Millet Meclisi. (2025). Siber Güvenlik Kanunu (Kanun No. 7545). T.C. Resmî Gazete (Sayı: 32846, Tarih: 19.03.2025)

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020). "Bilgi ve İletişim Güvenliği Rehberi." 08.09.2025 tarihinde https://cbddo.gov.tr/SharedFolderServer/Genel/File/bg_rehber.pdf adresinden erişildi.

World Economic Forum. (2016). Understanding Systemic Cyber Risk. Global Agenda Council on Risk & Resilience, White Paper.

Yazım Kuralları

1. Bankacılar dergisinde yayımlanmak üzere gönderilecek makaleler, word formatında arial yazı karakterinde, 11 punto ile tek aralıklı ve paragraflar arasında bir satır boşluk bırakılmak üzere Türkçe yazılmalıdır.
2. Kapak sayfasında, yazının başlığı, yazar(lar)ın bağlı bulundukları kuruluşlar ve ünvanları, iletişim kurulacak yazarın adı ve iletişim bilgileri bulunmalıdır.
3. Makalenin ilk sayfasında makalenin adı, öz/ abstract (en fazla 250 kelime), en az üç tane anahtar kelime Türkçe ve İngilizce olarak yazılmalı ve makaleye uygun JEL sınıflama numaraları verilmelidir. (http://www.aeaweb.org/journal/jel_class_system.php)
4. Yazı içinde kullanılan birinci düzey, ikinci ve üçüncü düzey başlıklar koyu harflerle yazılmalıdır. Başlıklar ile izleyen metin arasında bir satır boşluk verilmelidir. Başlıklardan sonra paragraf başı yapılmalıdır.
5. Yazı içinde yer alan tablo ve şekiller arial yazı karakterinde 10 punto ile hazırlanmalı, başlık ve sıra numarası verilmeli, kaynakları ise alta yazılmalıdır. Denklemlere sıra numarası verilmelidir.
6. Dipnotlar atlama yapılmadan numaralandırılmalı ve ayrı bir sayfada "Dipnotlar" başlığı altında toplanmalıdır.
7. Kaynaklara göndermeler dipnotlarla değil, metin içinde açılacak ayraçlarla yapılmalıdır.
8. Metinde gönderme yapılan veya yapılmayan tüm kaynaklar, kaynakçada yer almalıdır. Kaynaklar ayrı bir sayfada alfabetik sırayla yazılmalıdır.
9. Metin içi gönderme, dipnotlar ve kaynakça belirtilen kurallar çerçevesinde ve American Psychological Association (APA) (http://www.apastyle.org/learn/tutorials/basics-tutorial.aspx) sistemine göre yapılmalıdır.

Kaynakça ve Gönderme Örnekleri

Bir ve Birden Fazla Yazarlı Kitaplar

Arıcan, E., Yücememiş, B.T, Karabay, M.E. ve Işıl, Gökhan (2011). *Türk Bankacılık Sektöründe Ölçek Ekonomileri ve Rekabet Gücü Maliyet Etkinliği ve Ölçek Ekonomilerine İlişkin Bir Uygulama.* İstanbul: Türkiye Bankalar Birliği.

İlk Gönderme (Arıcan, Yücememiş, Karabay ve Işıl, 2011, s. 78)

İkinci ve Sonraki Göndermeler (Arıcan ve diğerleri, 2011, s.80)

Tüzel Kuruluş Tarafından Yayınlananlar

Türkiye İstatistik Kurumu. (2009). *Türkiye istatistik yıllığı*. Ankara: Türkiye İstatistik Kurumu.

İlk Gönderme (Türkiye İstatistik Kurumu [TÜİK], 2009, s.27)

İkinci ve Sonraki Göndermeler (TÜİK, 2009, s.38)

Çeviri Kitaplar

Sicilia, D.B ve Cruikshank, J.L. (2000). Greenspan Etkisi: Dünya Piyasalarını Harekete Geçiren Sözler (E. Salman, Çev.). İstanbul: Literatür Yayıncılık (Orijinali 2000 yılında yayımlanmıştır).

Gönderme (Sicilia ve Cruikshank, 2000, s.78)

Kitaptan Bir Bölüm

Esen, H. (2009) Kart Çıkaran Kuruluşların Yükümlülükleri. T.Ö. Kiraz (Yay. Haz.). *5464 Sayılı Banka Kartları ve Kredi Kartları Kanununun Değerlendirilmesi ve Uygulamadan Doğan Sorunlar* içinde (ss.21-47). İstanbul: Akademi.

Makaleler

Birgili, E., Tuna, G. ve Tuna V.E. (2011). Portföy Seçiminde Riski Sevmeyen Yatırımcılar İçin Hisse Senedinin Ait Olduğu Sektör ve İlgili Firmanın Kuruluş Tarihi Önemli midir? . *Finans Politik ve Ekonomik Yorumlar Dergisi*, 48(558), 23-35.

Internet adresleri

Tuna, K. (2005), "Bankacılık Kanununda Kurumsal Yönetim", 20 Mayıs 2006 tarihinde http://bsy.marmara.edu.tr/TR/konferanslar/2005/2005tebligleri/9.doc adresinden erişildi.

Bankacılık Düzenleme ve Denetleme Kurumu (2011) "İnteraktif Aylık Bülten Ağustos 2011" 20 Ekim 2011 tarihinde http://ebulten.bddk.org.tr/AylikBulten/Basit.aspx adresinden erişildi.

Kültür Mahallesi, Nisbetiye Caddesi,
Akmerkez No: 56 İç Kapı No: 24
Beşiktaş / İstanbul
Tel: 0212 282 09 73 Faks: 0212 282 09 46
tbb@tbb.org.tr www.tbb.org.tr