TÜRKİYE CUMHURİYETİ
TİCARET BAKANLIĞI

AB SİBER DAYANIKLILIK TÜZÜĞÜ (CRA)

Ürün Güvenliği ve Denetimi Genel Müdürlüğü

AVRUPA BİRLİĞİ TEKNİK MEVZUAT UYUMU

- Miktar kısıtlamaları ve her türlü eş etkili önlem **yasaklanmıştır**.
- Türkiye AB'den gelen ve AB teknik mevzuatına uygun ürünlerin Türk piyasasına girmesine **izin verecektir**.
- Ticaret ancak **meşru gerekçeler** ile kısıtlanabilir.
- **Türkiye AB teknik mevzuatı iç hukukuna dâhil edecektir**.

GÜMRÜK BİRLİĞİ KARARI

AB Teknik Mevzuat Uyumu → Güvenli ve Kaliteli Üretim → PGD ve İthalat Denetimleri → **İHRACAT**

Malların Serbest Dolaşımı:

- Türkiye, AB mevzuatını uyumlaştırdığında, TR-AB arasındaki ticarette **AB üyeleri ile denktir.**
- Ürünlerin **belgelendirme**si ülkemizde yapılmaktadır. (OK ataması)

TİCARET BAKANLIĞI'NIN ROLÜ

97/9196 sayılı BAKANLAR KURULU KARARI

YATAY KURALLARIN HAZIRLANMASI

- 7223 sayılı Kanun
- 7223 sayılı Kanun Uygulama Yönetmelikleri

TEKNİK MEVZUAT UYUMU KOORDİNASYONU

- AB teknik mevzuatını uyumlaştıracak kurumların tespiti
- Taslak mevzuatın Avrupa Komisyonuna iletilmesi ve müzakerelerin yürütülmesi

TİCARET BAKANLIĞI'NIN ROLÜ

❖ **Cumhurbaşkanlığı 12. Kalkınma Planı ve Orta Vadeli Program (OVP) kapsamında,**

Avrupa Birliği (AB) Dijital Ekonomi Düzenlemelerinin ülkemiz ticaretine etkisine ilişkin çalışmalar neticesinde AB ile koordinasyonu sağlamak amacıyla Bakanlığımız uhdesinde "AB Komisyonu ile Dijital Diyalog Çalışma Grubu" oluşturulmuş ve 2024, 2025 yılları içerisinde CRA'nın da dahil olduğu gündem çerçevesinde toplantılar yapılmıştır.

❖ **Ayrıca, Bakanlığımızca başvurulan ve AB tarafından kabul edilen "CRA'nın Türkiye Tarafından Uyumlaştırılmasına Yönelik Rehber" başlıklı bir Teknik İş Birliği ve Bilgi Değişimi (TAIEX) Çalıştayı, hazırlıkların tamamlanması ile 13-14 Kasım 2025 tarihinde ilgili kamu kurumları ve kuruluşları katılımıyla AB'den gelen uzmanlar Eşliğinde Ankara'da gerçekleştirilmiştir.**

AB Siber Güvenlik Mevzuatı

NIS I
NIS II
Directives

- 2024 itibariyle uygulamada
- Zorunlu uygulama
- Kritik altyapı ve kamu güvenliğini ilgilendiren hizmet sağlayıcılar ve tedarikçiler için siber güvenlik gereklilikleri belirler
- Ulusal yetkili otorite, olay müdahale ekibi oluşturulur

Cybersecurity Act (CSA)

- 2021 itibariyle uygulamada
- Gönüllü uygulama
- ENISA yetkileri artırılır, hukuki kişiliği haiz olur
- ENISA'nın ICT ürünler için sertifikasyon şeması (EUCC) oluşturulmasına imkan tanır

Cyber Resilience Act (CRA)

- Aralık 2027 itibariyle tam uygulamada (raporlama ve OK bildirimi 2026 yılında)
- Zorunlu uygulama
- Pazara giriş şartı
- ENISA tarafından belirlenen standartlara atıf

Siber Dayanıklılık Yasası Nedir?

Siber Dayanıklılık Yasası (CRA), AB yasa koyucuları tarafından belirtilen iki temel problemi çözmeyi amaçlamaktadır:

- **Birçok ürünün doğasında bulunan yetersiz siber güvenlik seviyesi veya bu tür ürün ve yazılımlara yönelik yetersiz güvenlik güncellemeleri,**
- **Tüketicilerin hangi ürünlerin siber güvenlikli olduğunu ya da bu ürünlerin korunacak şekilde nasıl ayarlanacağını bilmemesi,**

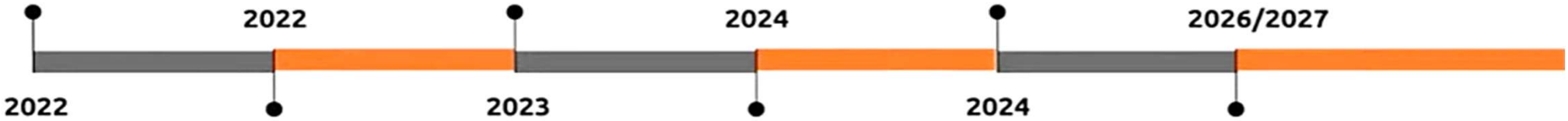
CRA, dijital unsur içeren ürünleri satın alan veya kullanan tüketicilerin ve işletmelerin korunmasına, siber güvenlik gerekliliklerinin yerine getirilmesine yardımcı olacaktır.

AB Siber Dayanıklılık Tüzüğü Yol Haritası

Yasa Üzerinde Anlaşma
Mart 2022'de, Üye Devletler yeni bir yasa oluşturulması konusunda anlaştı.

AB Siyasi Uzlaşısı
Kasım 2023'te AB siyasi uzlaşısı sağlandı ve teklif için son aşamaya gelindi.

Yayım
Tüzük, 20 Kasım 2024 tarihli AB Resmi Gazetesi'nde yayımlandı. 10 Aralık 2024 tarihi itibariyle yürürlüğe girdi.



Taslak Teklifi
Eylül 2022'de, Taslak AB Resmi Gazetesi'nde duyuruldu.

Avrupa Parlamentosu Onayı
Mart 2024'te teklif Avrupa Parlamentosunda onaylandı.

Uygulama
Uygunluk değerlendirme kuruluşlarının bildirimi (Haziran 2026)

Üreticilerin Raporlama yükümlülüğü (Eylül 2026)

Tüzüğün tam olarak uygulamaya konulması, 36 aylık geçiş süreci (11 Aralık 2027)

Dijital Unsur İçeren Ürün Nedir?

Ürünün veri alışverişi için başka bir cihaza veya ağa bağlı olması

- doğrudan/dolaylı bağlantı
- fiziksel, kablosuz/radyo veya sanal bağlantılar
- uzaktan veri işleme bağlantısı

Ürünün AB pazarında kullanıma sunulması

- nerede bulunduğunuzdan bağımsız olarak
- nerede geliştirildiğine/üretildiğine bakılmaksızın

AB pazarındaki ticari maksatlı olmayan özel amaçlı kullanım için çözümler dijital unsur içeren ürün olarak değerlendirilmez, CRA kapsamında değildirler.

Tüzük Kimleri İlgilendiriyor?

Üreticiler

Avrupa pazarında dijital unsurlar içeren ürünleri üreten ve tüketicilere ulaştıran kuruluşlar

Sağlayıcılar

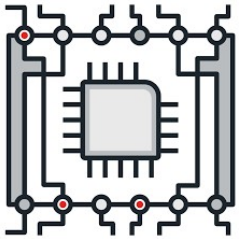
Üreticiler tarafından kullanılan bileşenleri veya yazılımları sağlayan kuruluşlar

İthalatçılar ve Dağıtıcılar

Dijital unsurlar içeren ürünleri Avrupa pazarına ithal eden veya dağıtan kuruluşlar

Tüzüğün Kapsamı

Standart Ürünler



- Ürünlerin %90'ı
- Sabit Diskler
- Akıllı Hoparlörler

Önemli Ürünler Sınıf I

- Virüs programları
- Pasaport Yönetim Uygulamaları
- Uzaktan Erişim Yazılımları
- Giyilebilir cihazlar

Önemli Ürünler Sınıf II

- Sunucular, masaüstü bilgisayarlar ve mobil cihazlar için işletim sistemleri
- Endüstriyel kullanıma yönelik güvenlik duvarları, izinsiz giriş tespit ve/veya önleme sistemleri

Kritik Ürünler

- Akıllı kartlar, akıllı kart sistemleri
- Akıllı sayaç sistemleri geçitleri

- Ürünlerin hangi kategoride değerlendirildikleri Tüzüğün 3 ve 4 üncü ekinde belirtilmektedir.

Önemli ve Kritik Ürünlerin Tarifi (2025/2392/EU)

Önemli Ürünler (Sınıf I — Sınıf II)

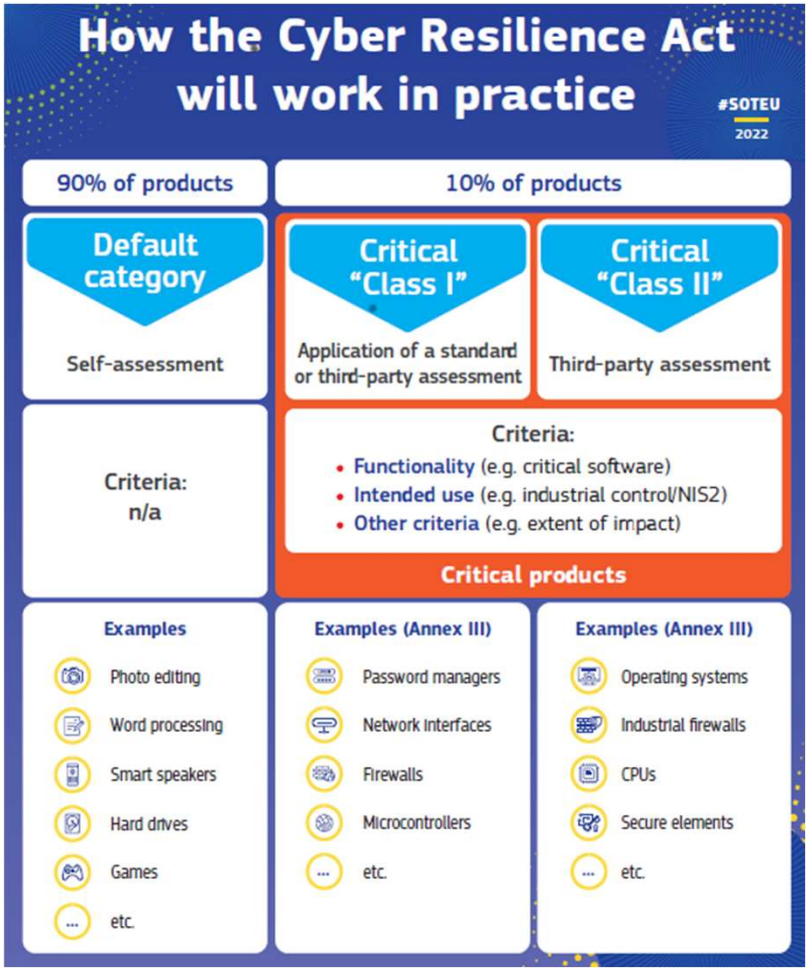
- Kimlik doğrulama ve yönetimi sistemleri ile yazılım ve donanımları
- Bağımsız ve gömülü tarayıcılar
- Şifre yöneticileri
- Zararlı yazılımları arayan, kaldıran veya karantinaya alan yazılım
- Ağ yönetim ve VPN sistemleri
- Açık anahtar altyapısı ve dijital sertifika verme yazılımı
- İşletim sistemleri, modemler

Kritik Ürünler

- Güvenlik Kutulu Donanım Cihazları
- Akıllı ölçüm sistemleri içindeki akıllı sayaç ağ geçitleri
- Güvenli unsurlar da dahil olmak üzere akıllı kartlar veya benzeri cihazlar

*https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202502392

Tüzüğün Kapsamı



- **Siber güvenlik, ürünün planlama, tasarım, geliştirme, üretim, teslimat ve bakım dahil olmak üzere tüm aşamalarında dikkate alınmalıdır.**
- **Ürünün yaşam döngüsü (end of life) veya beş yıllık bir süre boyunca (hangisi daha kısa ise) güvenli olmasının sağlanması gerekmektedir.**
- **Ürünlerin doğuştan güvenli olarak üretilmesi ve piyasaya sunulması sağlanmalıdır.**

CRA Temel Gereklilikler

1 Risk Değerlendirme

Üreticiler;
- Bilinen veri zafiyeti bulunmayan, istismar edilme ihtimali en aza indirgenmiş ve veri işleme miktarı azaltılmış **ürünleri piyasaya sunmakla yükümlüdür. (secure by design)**

2 Belgeleme

Üreticiler;
- Ürün tasarımı, teslimatı ve güvenlik açığı yönetimi, risk değerlendirmesi ve uygunluk beyanı, yazılım malzeme listesi (SBOM) **belgelendirmesini yapmak ve ilgililerine sunmakla yükümlüdür.**

3 Uygunluk Değerlendirme

Üreticiler;
- İç denetim veya bağımsız üçüncü taraf denetçiler tarafından sağlanan **uygunluk beyanı sunmakla yükümlüdür.**

4 Güvenlik Açığı Raporlama

Üreticiler;
- Mevcut güvenlik açıklarını, ürün güvenliğini etkileyecek güvenlik açıklarını ve farkına varılan tüm güvenlik açıklarını 24 saat içinde ENISA'ya bildirmelidir.

Teknik Dokümantasyon

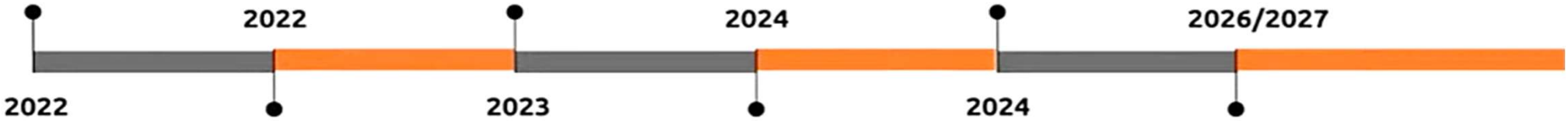
- **Dijital öğeler içeren ürünün genel açıklaması** (kullanım amacı, güvenliğe ilişkin yazılım sürümleri, CRA Ek-2'de belirtilen kullanıcı bilgileri ve talimatları)
- **Ürünün tasarımı, geliştirilmesi ve üretimi hakkında bir açıklama** (sistem mimarisinin tanımı, yazılım malzeme listesi, güvenlik açıklarının bildirilmesi için iletişim adresi, üretim ve izleme süreçlerine ilişkin gerekli bilgiler)
- **Siber güvenlik risklerinin değerlendirilmesi ve temel siber güvenlik gerekliliklerinin nasıl sağlandığını gösterir açıklama**
- **Ürünün güvenlik açığı yönetimine ilişkin açıklama** (CRA Ek-1 2. kısımda düzenlenmiştir)
- **Ürünün uygunluğunu gösteren harmonize standartların veya AB sertifikasyon şemasının bilgisi**
- **CRA Ek-1'de düzenlenen temel gerekliliklere ilişkin yapılan test raporları**
- **AB uygunluk beyanının bir kopyası**
- **PGD otoritesinin istemesi halinde ürünün temel gereklilikleri sağladığını kontrol edebilmesi için yazılım malzeme listesi (Software Bill of Materials)**

AB Siber Dayanıklılık Tüzüğü Yol Haritası

Yasa Üzerinde Anlaşma
Mart 2022'de, Üye Devletler yeni bir yasa oluşturulması konusunda anlaştı.

AB Siyasi Uzlaşısı
Kasım 2023'te AB siyasi uzlaşısı sağlandı ve teklif için son aşamaya gelindi.

Yayım
Tüzük, 20 Kasım 2024 tarihli AB Resmi Gazetesi'nde yayımlandı. 10 Aralık 2024 tarihi itibariyle yürürlüğe girdi.



Taslak Teklifi
Eylül 2022'de, Taslak AB Resmi Gazetesi'nde duyuruldu.

Avrupa Parlamentosu Onayı
Mart 2024'te teklif Avrupa Parlamentosunda onaylandı.

Uygulama
Uygunluk değerlendirme kuruluşlarının bildirimi (Haziran 2026)

Üreticilerin Raporlama yükümlülüğü (Eylül 2026)

Tüzüğün tam olarak uygulamaya konulması, 36 aylık geçiş süreci (11 Aralık 2027)

ENISA (Avrupa Birliği Siber Güvenlik Ajansı)

Üreticilerin Raporlama yükümlülüğü (Eylül 2026)

- **Bildirim yükümlülüğü**
  -Üründeki mevcut olan ve istismar edilen güvenlik zafiyeti
  -Ağır bir güvenlik olayına sebep olan zafiyet

Aşamalar	Yapılacaklar	Süre	Amaç
1. Erken Uyarı	Üye devletlerin uyarılarak alarma geçirilmesi	**24 saat içinde**	Hızlı farkındalık
2. Tam Bildirim	Detaylı teknik bilgilendirme, ilk değerlendirme, önerilen önlem ve hassasiyet derecesi.	**72 saat içinde**	Detaylı takip ve planlama
3. Nihai Rapor	Zafiyetin şiddetini gösterir detaylı açıklama, tehdidin türü ve asıl nedenine ilişkin sebebi, halihazırda alınan önlemi ve ilerideki önlemlere ilişkin detayların paylaşılması	**14 gün içinde** (zafiyetler için) **1 ay içinde** (ciddi siber güvenlik olayları için)	Olayın çözümü ve kapatılması

Uygunluk değerlendirmesi

Ürün Kategorisi	Modül A	Modül B+C	Modül H	AB sertifikasyon şeması
Standart Ürünler	✓	✓	✓	✓
Önemli Ürünler Sınıf I	✓ 1	✓	✓	✓
Önemli Ürünler Sınıf II		✓	✓	✓
Kritik Ürünler		✓ 2		✓

- Bir ürünün teknik gereklilikleri sağladığını ve uygunluğunu gösterir uygunluk değerlenmesi için CE işareti kullanılır.

1- Yalnızca uyumlaştırılmış (harmonized) standartlar kullanılması halinde mümkündür.
2- İlgili ürüne ilişkin bir sertifikasyon şeması olmaması halinde mümkündür.

Onaylanmış Kuruluşlar

- CRA'da belirli ürün kategorilerinde Onaylanmış Kuruluşlarla çalışma şartı
  - Onaylanmış Kuruluş: Üçüncü taraf bağımsız test veya belgelendirme hizmeti gerektiren CE işaretli ürünlerde piyasaya arz öncesi bu hizmeti sağlayan uygunluk değerlendirmesi kuruluşları
  - Hangi mevzuat kapsamında görevlendirildiğine bağlı olarak ilgili yetkili kuruluş tarafından görevlendirilmesi uygun görülen aday OK'lara dair bildirimler (ülkemizde Ticaret Bakanlığı aracılığıyla) NANDO sistemi üzerinden yapılır, bir itiraz sürecine tabi olarak OK atanır.
  - Ülkemiz açısından bu süreç önce ilgili mevzuatın Komisyona iletilip uyum teyidi almasına bağlıdır.

- CRA Dibacesinde OK atama süreci:
  - Dibace 100. Paragraf: 2022/30 sayılı Telsiz Ekipmanları Yönetmeliği Uygulama Mevzuatı (RED Delegated Act) kapsamında veya 2019/881/AB sayılı Siber Güvenlik Tüzüğü kapsamında oluşturulan Siber Güvenlik Sertifika Şemaları kapsamında atanan OK'lar yeniden değerlendirilip bildirilmelidir.
  - Madde 8 (Kritik Ürünlerle İlgili) : EUCC kapsamında esaslı seviyede sibergüvenlik sertifikası alan ürünlerin CRA altında ilave uygunluk değerlendirmesine tabi tutulmasına gerek olmamasına yönelik düzenlemelerin Komisyon tarafından yapılabileceği

Cezalar

- Üreticinin temel siber güvenlik gerekliliklerini sağlamaması, üretim ve raporlama yükümlülüklerini yerine getirmemesi halinde **15 milyon Euro tutarında ceza veya önceki yılki cirosunun %2.5 kadarı ceza** riski.

- Tüzük'ün onaylanmış kuruluşlara, yetkili temsilcilere, iktisadi işletmecilerin yükümlülüklerine, AB uygunluk beyanına, CE işareti iliştirilmesine, teknik dokümantasyon oluşturulmasına, ürünün uygunluk değerlendirmesi prosedürüne ve talep edilmesi halinde PGD otoriteleriyle veri paylaşımına ilişkin hükümlerine uyumsuzluk halinde **10 milyon Euro tutarında ceza veya önceki yılki cirosunun %2 kadarı ceza** riski.

- Bildirimde bulunulan kurumlara ve piyasa gözetim makamlarına yapılan taleplere yanıt olarak yanlış, eksik veya yanıltıcı bilgi verilmesi halinde **5 milyon Euro tutarında ceza veya önceki yılki cirosunun %1 kadarı ceza** riski.

- **İSTİSNA:** Mikro ve küçük işletmeler — Açık kaynak yazılım yöneticilerinin ihlali

Bakanlığımızca Müzakere Edilen Önemli Hususlar- OK Atanması Süreci

- OK Atanmasının Önemi
- OK Ataması için Gerekenler
  - Mevzuat Uyumu – Uyum Teyidi
  - Mevzuat Uyum Çalışmaları – Çalışma Grubu
- Süreci Kolaylaştırabilecek Unsurlar
  - RED Delegated Act için Uyum Teyidi ve OK Ataması
  - EUCC kapsamında TSE'nin sertifika üreticisi konumunda olması
- AB ile Gerçekleştirilen Toplantılar
  - Aralık 2024: CRA'nın GB ile bağlantısı – AB'den rehberlik/çözüm beklentimiz

Bakanlığımızca Müzakere Edilen Önemli Hususlar- Raporlama

- **CRA'da Raporlama:**
- Üretici (AB'de yerleşik İktisadi İşletmeci) – (SRP üzerinden) CSIRT – ENISA – diğer CSIRT'ler'e
- ENISA düzeltilen güvenlik açıklarını Avrupa Veritabanına (European Vulnerability Database) iletir

- **Türkiye'nin bu sistemde özel durumu: Uyum ve AB 27 ile eşit muamele hakkı**
- Hangi CSIRT'e raporlama yapılacak?
- EU CyCLONe'a erişim?
- ENISA'ya raporlama?
- Tek taraflı bilgi akışı? Veritabanına Ulaşım
- Tek Raporlama Platformuna Erişim?

- **ENISA'nın /AB'nin Üçüncü Ülkelerle İşbirliği Yapması**
- NIS II Madde 17: *The Union may, where appropriate, conclude international agreements with third countries or international organisations, allowing and organising their participation in particular activities of the Cooperation Group, the CSIRTs network and EU-CyCLONe. Such agreements shall comply with Union data protection law.*
- CSA Madde 12 (ENISA uluslararası işbirliği) / Madde 42 (üçüncü ülkelerle ve uluslararası kuruluşlarla işbirliği) / CRA Dibace 123 (üçüncü ülkelerle MRA)

- **AB ile Gerçekleştirilen Toplantılar**
  - Aralık 2025: Beklentilerimizin – Sorularımızın yinelenmesi

TÜRKİYE CUMHURİYETİ
TİCARET BAKANLIĞI

TEŞEKKÜRLER.

ÜRÜN GÜVENLİĞİ VE DENETİMİ GENEL MÜDÜRLÜĞÜ