CI|cert

06.08.2026/R01

ISO/IEC 27701:2025 REVİZYONU YAYIMLANDI

TEMEL DEĞİŞİKLİKLER

Alan	ISO/IEC 27701:2019	ISO/IEC 27701:2025
Standardın niteliği	ISO/IEC 27001 ve ISO/IEC 27002'nin bir uzantısı	Bağımsız bir yönetim sistem standardıdır
Ön koşul	ISO/IEC 27001 ile beraber belgelendirmesi zorunludur.	Artık ISO/IEC 27001'den bağımsız olarak uygulanabilir ve belgelendirme yapılabilir
Yapı ve esneklik	ISO/IEC 27001:2013'e uyumlu eklenti	Diğer ISO standartlarıyla daha kolay entegrasyon sağlayan yapı (Maddeler 4–10)
Madde 4 – Kuruluşun Bağlamı	ISO/IEC 27001'den türetilmiştir	KVYS kapsamı ve kuruluşun bağlamına ilişkin açık gereklilikler içermektedir
Madde 5 – Liderlik	Gizlilik rolleri BGYS içerisinde ele alınır	Gizlilik için özel liderlik sorumluluğu tanımlanmış ve üst yönetimin gizlilik konusundaki hesap verebilirliği arttırılmıştır
Madde 6 – Planlama	Gizlilik riski, BGYS risk yönetimi ile ilişkilidir	Gizlilik risklerinin yönetişimi daha açık ve sistematik hale gelmiştir
Madde 7 – Destek	ISO/IEC 27002 kontrollerine atıfta bulunur	KVYS için kaynaklar, yetkinlik ve dokümantasyon gereklilikleri tanımlanmıştır
Madde 8 – Operasyon	Gizlilik kontrolleri ekler aracılığıyla entegre edilmiştir	Uygulama beklentileri daha açık hale gelmiş ve operasyonel gizlilik süreçleri tanımlanmıştır
Madde 9 – Performans Değerlendirme	Gizliliğe yönelik ayrı bir performans maddesi bulunmamaktadır	Açık şekilde tanımlanmış gizlilik metrikleri, iç tetkikler ve yönetimin gözden geçirmesi gereklilikleri
Madde 10 – İyileştirme	Bağımsız sürekli iyileştirme yaklaşımı sınırlıdır	KVYS için sürekli iyileştirme süreci tanımlanmış ve düzeltici ve önleyici yaklaşım güçlendirilmiştir.
Ek (Annex) Yapısı	Veri Sorumluları (PII Controllers) ve Veri İşleyenler (PII Processors) için ayrı ekler bulunur; ISO/IEC 27002 ile güçlü bağlantıya sahiptir.	Ekler yeniden yapılandırılmış; kontroller birleştirilmiş, rehberlik sadeleştirilmiş ve geçiş eşleştirmeleri eklenmiştir.

ISO/IEC 27701:2025, ile standardın yapısı köklü biçimde değişmiştir. Bu yapısal değişikliklerin doğru anlaşılması, geçiş sürecinin etkin şekilde planlanmasının temelini oluşturur.

ISO/IEC 27701:2025
KONTROL YAPISI VE EKLER

ISO/IEC 27701:2025'te kontroller kaldırılmamış, yeniden yapılandırılmıştır. Bu yapılandırma özellikle Dokümantasyonunuzu ve Uygulanabilirlik Bildirgesi (Statement of Applicability – SoA) dokümanınızı en fazla etkileyecek değişikliklerden biridir.

- **Kontrol yapısı** önemli ölçüde **sadeleşti.**
- Kontroller, "Maddeler"den **"Ekler"**e taşındı.
- **"neyin uygulanacağı" (Ek A)** ile **"nasıl uygulanacağı" (Ek B)** birbirinden ayrıldı.
- Kişisel Veri (PII) Yönetimi açısından ilave **uygulama rehberliği** gerektiren kontrollere odaklandı.

KONTROL YAPISI

2019 VERSİYONU	2025 VERSİYONU	AÇIKLAMA
Madde 6 (90'dan fazla alt maddeye atıf)	→ **Ek A/Tablo A.3** (29 kontrol)	Kişisel Veri (PII) için ortak bilgi güvenliği kontrolleri
Madde 7	→ **Ek A/Tablo A.1** (31 kontrol)	Veri Sorumlusu (PII Controller) kontrolleri
Madde 8	→ **Ek A/Tablo A.2** (18 kontrol)	Veri İşleyen (PII Processor) kontrolleri
Madde 6–8 içerisine yerleştirilmiş rehberlik	→ **Ek B**	Uygulama rehberliği (Ek A'nın yapısını yansıtır)

Ek F içerisinde yer alan **eşleştirme (correspondence) tablosu,** 2019 sürümündeki her bir kontrolü 2025 sürümündeki eşdeğeri ile eşleştirmektedir.
Böylece **boşluk analizi ve geçiş planlaması** çok daha sistematik ve uygulanabilir hale gelmektedir.

Geçiş süresi 3 yıldır. Mevcut 2019 versiyonlu sertifikaların Ekim 2028'den önce yeni versiyona geçirilmesi gerekmektedir.

Cicert, mevcut müşterileri için geçiş tetkikini, 3 yıllık geçiş döneminde herhangi bir programlı tetkik (gözetim, belge yenileme vb.) sırasında gerçekleştirmeyi öngörmektedir.

İlave geçiş tetkiklerinin gerçekleştirilip gerçekleştirilmeyeceği, Cicert'in yeni versiyona geçiş tetkiklerini yapmaya ve yeni versiyonda başvuruları almaya ne zaman başlayacağı akreditasyon düzenlemelerinin yayımlanmasının ardından ayrıca duyurulacaktır.

GEÇİŞ TAKVİMİ

Ekim 2025 Geçiş Dönemi Başlangıcı
14.10.2025 Standartın yayımlanması

Ekim 2025-Ekim 2028 Geçiş Dönemi
Kuruluşların yönetim sistemini güncellemesi, 3. taraf tetkiklerin tamamlanması

Ekim 2028 2019 Geçiş Dönemi Sonu
2019 revizyonlu sertifikaların geçerliliğini yitirmesi

ISO/IEC 27701:2025 GEÇİŞİ ÖNERİLEN ADIMLAR

1 Yeni standardı anlayın.
Yeni standardın içeriğini ve gerekliliklerini anlamak için standardı edinin. Revize edilmiş standardın getirdiği değişikliklere odaklanın.

2 Personel eğitimlerini gerçekleştirin.
İlgili personel eğitimlerini gerçekleştirerek gereklilikleri ve önemli değişiklikleri anladığından emin olun.

3 Eksiklikleri belirleyin ve plan oluşturun.
Yeni gereksinimleri karşılamak için ele alınması gereken eksiklikleri belirleyin ve bir uygulama planı oluşturun.

4 Uygulama ve güncelleme yapın.
Yeni gereksinimleri karşılamak için gerekli adımları uygulayın ve yönetim sisteminizi güncelleyin.

CIcert

GEÇİŞ İÇİN DİKKAT EDİLECEK KİLİT FAALİYETLER

1 Mevcut Kontrollerin 2025 Yapısıyla Eşleştirilmesi

Özellikle Ek F içerisinde "N/A" olarak işaretlenen kontrollere dikkat edilmelidir. Bunlar, 2019 versiyonunda yer almasına rağmen 2025 versiyonunda doğrudan bir karşılığı bulunmayan kontrolidir. Bu durumda ilgili kontrolün amacının başka bir 2025 kontrolü kapsamında karşılanıp karşılanmadığı değerlendirilmeli veya ilgili dokümantasyonun KVYS kapsamından güvenle çıkarılıp çıkarılamayacağı belirlenmelidir.

2 Yeni Gerekliliklerin Belirlenmesi

Mevcut KVYS dokümantasyonunuzu, ISO/IEC 27701:2025'in Yönetim Sistemi Gereklilikleri (Maddeler 4–10) ile karşılaştırarak gözden geçirin.

Özellikle aşağıdaki maddeler değerlendirilmelidir:

- **Madde 4.1 ve Madde 4.2** – İklim değişikliği artık kuruluşun bağlamı ve ilgili tarafların ihtiyaç ve beklentilerinin değerlendirilmesinde dikkate alınması gereken bir hususdur.
- **Madde 5.2** – Gizlilik Politikası (Privacy Policy) artık (BGYS politikasının bir uzantısı değil, bağımsız bir politika olarak oluşturulmalıdır.
- **Madde 6.1.2 ve Madde 6.1.3** – Gizlilik Risk Değerlendirmesi (Privacy Risk Assessment) ve Gizlilik Risk İşleme (Privacy Risk Treatment) gereklilikleri bağımsız olarak tanımlanmıştır.
- **Madde 6.3** – Değişikliklerin Planlanması açık bir gereklilik olarak standarda eklenmiştir.

3 Uygulanabilirlik Bildiriminin (SoA) Yeniden Oluşturulması

- Mevcut Uygulanabilirlik Bildirimi (SoA), 2019 sürümünde Madde 6, Madde 7 ve Madde 8 kapsamındaki kontrollere dayanmaktadır.
- ISO/IEC 27701:2025 ile birlikte SoA, Ek A (Annex A) içerisinde yer alan 78 kontrol esas alınarak yeniden hazırlanmalıdır.
- Ayrıca uygulanmayan kontroller için gerekçelerin Madde 6.1.3 e) kapsamında açık şekilde belirtilmesi gerekmektedir.

4 Dokümantasyonun Güncellenmesi

Geçiş sürecinde en az aşağıdaki dokümanların güncellenmesi gerekmektedir:

- **KVYS Kapsamı** (Artık BGYS kapsamına atıf yapmayan bağımsız bir kapsam dokümanı.)
- **Gizlilik Politikası** (Madde 5.2 gerekliliklerine uygun olarak.)
- **Gizlilik Risk Değerlendirme Metodolojisi** (Madde 6.1.2 gerekliliklerine uygun olarak.)
- **Uygulanabilirlik Bildirimi (SoA)** (Ek A'nın yeni kontrol yapısına göre.)
- **İç Tetkik Programı** (Maddeler 4–10 ile uygulanabilir Ek A kontrollerini kapsayacak şekilde.)
- **Yönetimin Gözden Geçirmesi Girdileri ve Çıktıları** (Madde 9.3 gerekliliklerine uygun olarak.)

5 ISO/IEC 27701:2025'e Göre İç Tetkikin Gerçekleştirilmesi

Geçiş tetkikinden önce, kuruluşunuzun ISO/IEC 27701:2025 gerekliliklerine uygunluğunu doğrulamak amacıyla kapsamlı bir İç Tetkik gerçekleştirin.

Bu tetkik;

- gerçekleştirilen boşluk analizini (Gap) doğrular,
- güncellenen dokümantasyonun etkinliğini değerlendirir,
- Yönetimin Gözden Geçirmesi için geçiş sürecinin hazır olma durumuna ilişkin anlamlı girdiler sağlar,
- Belgelendirme geçiş tetkiki öncesinde eksikliklerin giderilmesine imkân tanır.

✓ Geçiş Eğitimi
✓ Boşluk Analizi
✓ Geçiş Tetkikleri
için bizimle iletişime geçebilirsiniz

Cicert Belgelendirme Hizmetleri Ltd. Şti.
Soğanlık Yeni Mah. Fuatpaşa Sok.
Kartal İstofis No: 12 Daire: 10 Kartal
İstanbul, 34880

+(90) 0 216 546 05 26
cicert@cicert.com.tr
www.cicert.com.tr