MÜŞTERİ GEÇİŞ PLANI REHBERİ

1 Amaç ve kapsam

Bu rehber, ISO/IEC 27701:2019 kapsamında belgelendirilmiş müşterilerin yeni sürüme hazırlanması, geçiş tetkikinin planlanması ve belgelendirme kararının tamamlanması için uygulanacak yöntemi açıklar. KVYS, gizlilik bilgileri yönetim sistemini; SoA, Uygulanabilirlik Bildirgesini ifade eder. Rehber, TÜRKAK akreditasyonu kapsamındaki geçişe yöneliktir.

ISO/IEC 27701:2025 müşterinin belgelendirileceği yönetim sistemi standardıdır. ISO/IEC 27706:2025 ise Sigmacert'in tetkik ve belgelendirme faaliyetlerine ilişkin şartları düzenler; müşteriye yönelik ayrı bir yönetim sistemi belgesi değildir.

2 Geçiş takvimi

Aşama veya tarih	Uygulama
Hazırlık dönemi	Kuruluş fark analizini yapar; sistemi, kontrol referanslarını ve uygulama kayıtlarını günceller; iç tetkik ve yönetimin gözden geçirmesi çalışmalarını geçiş değişikliklerini kapsayacak şekilde yürütür.
Sigmacert ile teyit edilen tarih	Geçiş tetkiki, müşteri hazırlığı ve belgelendirme çevrimi dikkate alınarak planlanır.
31.12.2027	TÜRKAK duyurusuna göre mevcut belgelendirme kuruluşlarının akreditasyon geçişini tamamlaması için son tarihtir.
31.10.2028	Sertifikalı müşterilerin geçişini tamamlaması için son tarihtir. Tetkik, gerekli kapamalar ve olumlu belgelendirme kararı bu tarihe kadar sonuçlandırılır.

Mevcut sertifikanın daha ileri bir bitiş tarihi taşıması geçiş son tarihini uzatmaz. Yeni sürümde TÜRKAK akreditasyonu kapsamında sertifika, Sigmacert'in ilgili akreditasyon geçişi ve müşteri belgelendirme kararı tamamlandıktan sonra düzenlenir.

3 Yeni sürümün temel değişiklikleri

Konu	Müşteri açısından gereklilik
Bağımsız yönetim sistemi	ISO/IEC 27001 belgesi ön koşul değildir. KVYS kapsamı, süreçleri, sorumlulukları ve bilgi güvenliği programı kendi içinde gösterilir.
Yönetim sistemi yapısı	Bağlam, liderlik, planlama, destek, operasyon, performans değerlendirme ve iyileştirme Madde 4–10 altında ele alınır. İklim değişikliğinin ilgisi değerlendirilir.
Gizlilik risk yönetimi	Risk kriterleri, risk sahipleri, ilgili kişiler üzerindeki etkiler, risk işleme planı ve kalan risk kabulü gözden geçirilir.
Bilgi güvenliği programı	Kişisel verilerin güvenliğini sağlayan program, risk temelli gerekli kontroller ve etkinlik kanıtları dokümante edilir.
Kontroller ve rehber	Normatif Ek A; veri sorumlusu, veri işleyen ve ortak güvenlik kontrollerini kapsar. Normatif Ek B, bu kontrollerin uygulanmasına ilişkin rehberi içerir.
SoA ve izlenebilirlik	Gerekli kontroller, dahil edilme gerekçeleri, uygulama durumu ve Ek A kontrollerinin hariç tutulma gerekçeleri güncellenir. Eski/yeni kontrol eşleştirmesinde Ek F'den yararlanılabilir.

4 Müşterinin hazırlayacağı doküman ve kayıtlar

Doküman veya kayıt	Beklenen içerik
Geçiş fark analizi ve planı	Yeni şartların mevcut sisteme etkisi, sorumlular, terminler ve kapanış kayıtları.
Kapsam ve roller	Faaliyetler, ürün/hizmetler, lokasyonlar, uzaktan yürütülen işler ve işleme faaliyeti bazında veri sorumlusu/veri işleyen rolleri.
Kişisel veri işleme bilgileri	İlgili kişi grupları, veri kategorileri, işleme amaçları, işleme envanteri, aktarımlar ve alt işleyenler.
Politika hedef ve sorumluluklar	Gizlilik politikası, ölçülebilir hedefler, kaynaklar, görev ve yetkiler.
Gizlilik risk kayıtları	Risk değerlendirmesi, işleme planı, risk sahibi onayları ve kalan risk kabulleri.
Bilgi güvenliği programı	Kişisel verileri koruyan güvenlik süreçleri, kontroller ve uygulama/etkinlik kayıtları.
Uygulanabilirlik Bildirgesi	Yeni Ek A ile karşılaştırılmış ve güncellenmiş SoA.
Operasyon kayıtları	İlgili kişi talepleri, işleyen talimatları, tedarikçi/alt işleyen yönetimi, aktarım, olay ve saklama/silme kayıtları.
Eğitim ve farkındalık	İlgili personelin eğitim, farkındalık ve görev bazlı yeterlilik kanıtları.
İç tetkik ve yönetimin gözden geçirmesi	Yeni sürüm ve rol bazlı kontrolleri kapsayan değerlendirmeler ile kararlar.
Düzeltici faaliyetler	Tespit edilen uygunsuzluklara ilişkin düzeltme, neden analizi, faaliyet ve etkinlik kayıtları.

5 Başvuru ve tetkik öncesi bilgi paylaşımı

Geçiş talebinde güncel kapsam, faaliyet bazlı roller, lokasyonlar, kişisel veri işleme faaliyetlerine ilişkin personel sayısı, veri kategorileri, ilgili kişi grupları, aktarılan ülkeler/yargı alanları, bilgi sistemleri ve bulut/dış kaynak hizmetleri bildirilir. Güncel SoA, mevcut sertifika bilgileri, önemli değişiklikler ve tercih edilen tetkik dönemi paylaşılır.

Gizlilik veya hassasiyet nedeniyle erişime kapalı olacak kayıtlar tetkik öncesinde açıklanır. Sigmacert, yeterli kanıt elde edilip edilemeyeceğini değerlendirir. Yeterli tetkik mümkün değilse gerekli erişim düzenlemeleri tamamlanmadan tetkik yürütülmez.

6 Geçiş tetkikinin yöntemi ve süresi

Geçiş tetkiki; uygun olması hâlinde gözetim veya yeniden belgelendirme tetkikiyle birlikte ya da ayrı bir tetkik olarak planlanır. Yöntem, değişikliklerin kapsamı, hazırlık düzeyi, belgelendirme çevrimi ve Sigmacert'in akreditasyon geçiş durumu dikkate alınarak belirlenir.

Süre, ISO/IEC 27706:2025 Madde 9.1.4 ve normatif Ek A esas alınarak belirlenir. Rol, efektif personel, işleme karmaşıklığı, risk, veri kategorileri, teknolojik altyapı, lokasyonlar ve dış kaynak süreçleri değerlendirilir. Müşteriye teklif ve tetkik planında bildirilir. TÜRKAK'ın akreditasyon geçişi için belirttiği 2 adam/gün ilave süre, müşteri tetkiklerine otomatik olarak uygulanmaz.

Uzaktan yöntem kullanımı, yeterli kanıta erişim ve tetkik etkinliği bakımından değerlendirilir. Çoklu sahalı kuruluşlarda merkez fonksiyon, ortak süreçler, sahaların faaliyet ve riskleri incelenir; süre dağılımı ve varsa örnekleme gerekçelendirilir. Kapsam genişletme talebi bulunması hâlinde bu talebin değerlendirmesi geçiş planına ayrıca dahil edilir.

7 Tetkik kapama ve belgelendirme kararı

Tetkikte Madde 4–10, uygulanabilir rol kontrolleri, bilgi güvenliği programı, SoA, risk yönetimi, iç tetkik, yönetimin gözden geçirmesi ve uygulama etkinliği değerlendirilir. Kuruluş, ilgili personeli ve kayıtları erişilebilir kılar. Bulgular kapanış toplantısında bildirilir ve raporlanır.

Uygunsuzluklar için düzeltme, kök neden analizi ve düzeltici faaliyet kanıtları bildirilen süre içinde sunulur. Gerektiğinde ilave inceleme veya takip tetkiki gerçekleştirilir. Geçiş, tetkik dosyasının gözden geçirilmesi, gerekli kapamaların kabulü ve olumlu belgelendirme kararıyla tamamlanır.

8 Sertifika ve mevcut belgenin durumu

Yeni sertifikada ISO/IEC 27701:2025 referansı, KVYS ifadesi, kapsam içindeki faaliyet/ürün/hizmet bazlı roller, ilgili kişi grupları ve SoA sürümü gösterilir. Kapsamdaki hiçbir faaliyet tanımlı fiziksel lokasyonda yürütülmüyorsa tüm faaliyetlerin uzaktan yürütüldüğü belirtilir.

Geçiş otomatik olarak yeni bir üç yıllık belgelendirme çevrimi başlatmaz. Sertifika tarihleri, tetkik türü ve belgelendirme kararı doğrultusunda belirlenir. Geçiş süresi mevcut belgenin geçerliliğini uzatmaz; gözetim ve diğer sözleşmesel yükümlülükler devam eder. 31.10.2028'e kadar geçişi tamamlanmayan 2019 belgeleri bu tarihten sonra geçerli akredite belge olarak kullanılamaz.

9 Değişiklik bildirimi ve takip

Kuruluş; kapsam, lokasyon, personel, roller, işleme faaliyetleri, bilgi sistemleri, bulut hizmetleri, alt işleyenler ve dış kaynak düzenlemelerindeki önemli değişiklikleri Sigmacert'e bildirir. Geçiş takvimi, tetkik süresi ve ekip ihtiyacı bu bilgilere göre yeniden değerlendirilebilir. Müşteri bazında hazırlık, tetkik, bulgu, kapama, karar ve sertifika durumu takip edilir.

10 Müşteri hazırlık kontrol listesi

Kontrol	Durum veya kayıt referansı
Geçiş sorumlusu ve hedef tetkik tarihi belirlendi.	
Fark analizi ve geçiş planı hazırlandı.	
Kapsam, roller ve işleme bilgileri güncellendi.	
Risk değerlendirmesi, işleme planı ve SoA güncellendi.	
Bilgi güvenliği programı ve kontroller gözden geçirildi.	
Dokümanlar yeni madde ve kontrol referanslarıyla güncellendi.	
İlgili personel eğitildi ve uygulama kayıtları oluşturuldu.	
İç tetkik ve yönetimin gözden geçirmesi geçişi kapsayacak şekilde tamamlandı.	
Tespit edilen eksiklikler ve düzeltici faaliyetler ele alındı.	
Tetkik kapsamı, tarih ve erişim düzenlemeleri Sigmacert ile teyit edildi.	

11 Sık sorulan sorular

ISO/IEC 27001 belgesi zorunlu mu?

Hayır. Bununla birlikte, kişisel verilerin güvenliğini destekleyen yeterli bir bilgi güvenliği programı ve gerekli kontroller uygulanmış olmalıdır.

ISO/IEC 27706 için ayrıca müşteri sertifikası düzenlenecek mi?

Hayır. Bu standart belgelendirme kuruluşunun faaliyetlerine ilişkindir. Müşterinin yönetim sistemi belgesi ISO/IEC 27701:2025'e göre düzenlenir.

Belgemin bitişi 2028 sonrasındaysa geçişi erteleyebilir miyim?

Hayır. Belgenin üzerinde yazan tarih, 31.10.2028 geçiş son tarihini uzatmaz.

Tetkikte uygunsuzluk çıkarsa belge hemen iptal edilir mi?

Bulgular, önem derecesi ve belgelendirme prosedürü kapsamında ele alınır. Gerekli kapamalar ve olumlu karar geçiş son tarihine kadar tamamlanmalıdır.

Sertifika numarası değişecek mi?

Numara ve çevrim bilgileri, tetkik türü ve Sigmacert'in sertifika yönetim kuralları doğrultusunda değerlendirilir.

12 İletişim ve dayanaklar

Geçiş kapsamı, hazırlık, yöntem, süre ve kayıtlar için Sigmacert Belgelendirme ve Operasyon Birimiyle mevcut müşteri iletişim kanallarınız üzerinden iletişime geçebilirsiniz.

Dayanaklar: ISO/IEC 27701:2025, ISO/IEC 27706:2025 ve TÜRKAK Standart Geçiş Duyurusu.
https://www.turkak.org.tr/duyurular/1189