

## A. AMAÇ

Bu doküman Vericert ISO 27001:2022 Bilgi Güvenli Yönetim Sistemi standardından belgeli olan kuruluşların ISO 27001:2022 versiyonuna geçişlerinin eksiksiz bir şekilde yapılması amaçlanmaktadır.

## B. KAPSAM

Vericert ISO 27001:2022 Bilgi Güvenli Yönetim Sisteminin versiyon geçişini ve denetim süreçlerini kapsamaktadır.

## D. UYGULAMA

ISO 27001:2022 Bilgi Güvenli Yönetim Sistemi standardı geniş kapsamlı bir revizyona uğramıştır. Bu rehberde gerçekleşen revizyon bağlamında Vericert tarafından belgelendirilecek ve mevcut 2013 versiyonunda 2022 versiyonuna geçiş yapacak kuruluşların yapmaları gerekenler hakkında bilgilendirme yapılmaktadır. Bu bilgilendirme ile Vericert kendi müşterileri için versiyon geçişle ilgili hem bilgilendirme hem de kuruluşların yapacaklarını tarif etmektedir.

### D.1. ISO 27001:2022 Standardı

Ekim 2022'de yayınlanan standartta önemli değişiklikler olmuştur. ISO 27001:2022 Standardı; Standard ISO direktifi Ek SL'ye göre hazırlanmıştır. Oluşturulan Yüksek Seviyeli bu yapı doğrultusunda alt madde başlıkları, temel konular, ortak terimlerle yönetim sistem standartları arasında uyumluluk sağlanmış ve tüm yönetim sistemleri için ortak olacak olan 10 maddelik sisteme geçilmiştir.

Revize edilen ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardındaki temel değişiklikler şunlardır;

1. 4.4 Maddesi düzenlenerek BGYS'nin uygulanması ve sürdürülmesi için Prosesler ve Etkileşimlerinin tanımlanması
2. '6.3 Değişikliklerin Planlanması' maddesi eklendi
3. Bilgi güvenliği amaçları izlenmesi istendi
4. 8.1 Maddesinde Operasyonel proseslerin ve proseslerin kontrolünün uygulanması için kriterler belirlenmesi
5. İç tetkik ve YGG diğer maddelerle uyumlu hale geldi
6. EK A kontrolleri tamamen değiştirildi ve ISO/IEC 27002 ile uyumlu hale getirildi.
7. EK A kontrolleri 4 başlık altında 93 kontrole dönüştürüldü

### D.2. ISO 27001:2022 Sertifikalarının Geçerliliği ve Geçiş Süreci

ISO 27001:2013 sertifikası yeni standardın yayınlanmasından sonra 3 yıl içinde geçerliliğini kaybedecektir. ISO 27001:2013'e sahip belgeli olan kuruluşların en geç Eylül 2025'e kadar geçişlerini tamamlamaları gerekmektedir.

Yeni ISO 27001:2022 BGYS geçişinizi ilk belgelendirme denetiminde yapılabileceğiniz gibi gözetim ve yeniden belgelendirme tetkikinizde de bu geçişi sağlayabilirsiniz.

Vericert olarak siz firmalarımızdan beklentimiz etkin bir geçiş planı hazırlamanız ve yapacağınız plan sonrasında en uygun sürede geçiş çalışmalarınızı tamamlamanızdır.

Vericert bu sürecin her aşamasında ISO 27001:2022 kapsamında yeni standart TSE tarafından yayınlanmıştır. İlgili standart için TSE standart satış kısmından temin edebilirsiniz.

### D.3. Vericert'in Müşteri Kuruluşlarından Bekledikleri

Vericert hali hazırda ISO 27001:2013 BGYS belgesi bulunan kuruluşlarından ISO 27001:2022'e geçiş ile ilgili bazı hazırlıklar yapmasını beklemektedir. Bu geçiş süreci içinde firmalarının kesintisiz ve eksiksiz olarak belgelerini güncelleyip devam ettirmeleri için bazı düzenlemelerin yapılması etkili ve iyi bir uygulama olacaktır.

Bunun için belgeli kuruluşların ISO 27001:2022'e bir geçiş planı ile geçişlerini planlamaları gerekmektedir. Bu geçiş planında şu adımları belirtmeleri tavsiye edilmektedir;

1. Yeni şartların karşılanması için kuruluş içindeki farklılıkların belirlenmesi
2. Uygulama planının geliştirilmesi
3. Kuruluşun etkililiği için ilgili tarafların tümünün bilinçlendirilmesi ve eğitim çalışmalarının tamamlanması
4. Revize edilen şartların karşılanması için Bilgi Güvenliği Yönetim Sisteminin güncellenmesi ve etkililiğinin doğrulanması
5. Geçiş ile ilgili çalışmalarınızı Vericert ile paylaşmanızdır.

### D.4. ISO 27001:2022 Versiyonu Geçişi İle İlgili İzlenecek Prosedür

Vericert olarak ISO 27001:2022 BGYS versiyon geçişi ile ilgili olarak yapmanız gerekenleri aşağıda maddeler olarak belirtmiştir. Olası her türlü sonuca karşı en geniş kapsamda hazırlanan bu kısa kılavuz siz Vericert ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi Belgeli firmalarımız için tüm belirsizlikleri ortadan kaldıracak düzeyde hazırlanmıştır.

#### ISO 27001:2022 Geçiş Başvuru ve Süreç Aşamaları;

1. ISO 27001:2022 Geçiş Planının siz müşterilerimiz tarafından planlanması ve Vericert ile net olarak paylaşılması (Geçiş sürecinin gözetim veya yeniden belgelendirme denetimi ile birlikte mi olacağı yada ekstra bir versiyon geçiş denetimini talep edildiği) ,
2. Vericert tarafından hazırlanan **Form.48 - ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi Versiyon Geçiş Planının** doldurulup Vericert Planlama Sorumluları ile paylaşılması
3. Vericert Planlama Sorumlusu ile görüşülerek geçişin tamamlanmasının istendiği tarihin belirlenmesi,
4. Geçiş planındaki adımların uygulanması geçiş çalışmalarının tamamlanması,
5. Geçiş, Gözetim tetkiki veya Yeniden Belgelendirme tetkikinin önceden belirlenen tarihte gerçekleştirilmesi.
6. Uygunlukları kapatma için size verilen 6 ay (Maksimum) süre içinde uygunlukların kapatılması
7. Vericert tarafından olumlu sonuçlanan geçiş sonucu sertifikanızın tarafınıza ulaştırılmasıdır.

Firmanızın talebi ile geçiş tetkikinin gözetim tetkiki ve/veya yeniden belgelendirme tetkiki ile aynı anda yapılması durumunda firmanız ISO 27001:2022 geçişi için yeter seviyede uygunluk gösterememişse bir sonraki gözetim ve/veya yeniden Belgelendirme tetkiki esnasında geçişini yapabilir. Eğer bir sonraki gözetim veya yeniden belgelendirme denetim tarihinin Eylül 2025'den sonra olması durumunda; firmanızın ilgili denetiminin Eylül 2025 tarihinden önce sonuçlanacak şekilde yapılması planlanacaktır. Kuruluş Eylül'den önce bu tetkikin yapılmasını kabul etmezse Eylül 2025 tarihinde ISO 27001:2013 BGYS standardı yürürlükten kalkacağı için kuruluşun ISO 27001:2013 belgesi otomatik olarak iptal edilecektir.

Bu durum geçiş denetiminin ekstra bir denetimle planlanması durumunda da geçerlidir. Geçiş denetiminin Eylül 2025 tarihinden önce sonuçlanmış olması gerekmektedir. Gerek gözetim tetkiki ve/veya yeniden belgelendirme tetkiki ile gerekse ekstra bir denetimle geçişini yapacak müşterilerimiz. Eylül 2025 tarihine kadar ilgili geçişi yapmazlar ise; müşterilerimize ilk belgelendirme süreci uygulanacaktır.

## VERİCERT ISO 27001:2022 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ MÜŞTERİ VERSİYON GEÇİŞ REHBERİ

Versiyon geiş denetimlerinde; uygulanacak denetim süreleri tarafınızdan gönderilecek **Form.48 - ISO 27001:2022 Bilgi Güvenliđi Yönetim Sistemi Versiyon Geiş Planının** Vericert Belgelendirme Hizmet sorumlularınızın göndermiş olduğunuz geiş planı ve ilgili dokümanlarınız incelenmesi sonucu firmanıza bildirilecektir.

ISO 27001:2022 Bilgi Güvenliđi Yönetim Sistemine sahip kuruluşlarımızın belgelerinin devamı ve bu tür istenmeyen durumlarla karşılaşmamaları için gerekli çalışmalarını yapmaya başlamalarını önemle tavsiye ederiz.

Saygılarımızla...

VERİCERT YÖNETİMİ

REVİZYON TAKİP TABLOSU		
REVİZYON İÇERİĞİ	REVİZYON NO	REVİZYON TARİHİ
İlk yayın	00	20.10.2022