



ISO 27001:2022 Geçiş Duyurusu_Rev.02 25.05.2023

DSR Uluslararası Gözetim ve Belgelendirme Hiz. Ltd. Şti.

Yeşilbağlar mah. Helis Beyaz Ofis A Blok K:2 D:207 Pendik/İSTANBUL

info@dsrbelgelendirme.com.tr, 0(216) 606 06 35

Ocak 2023

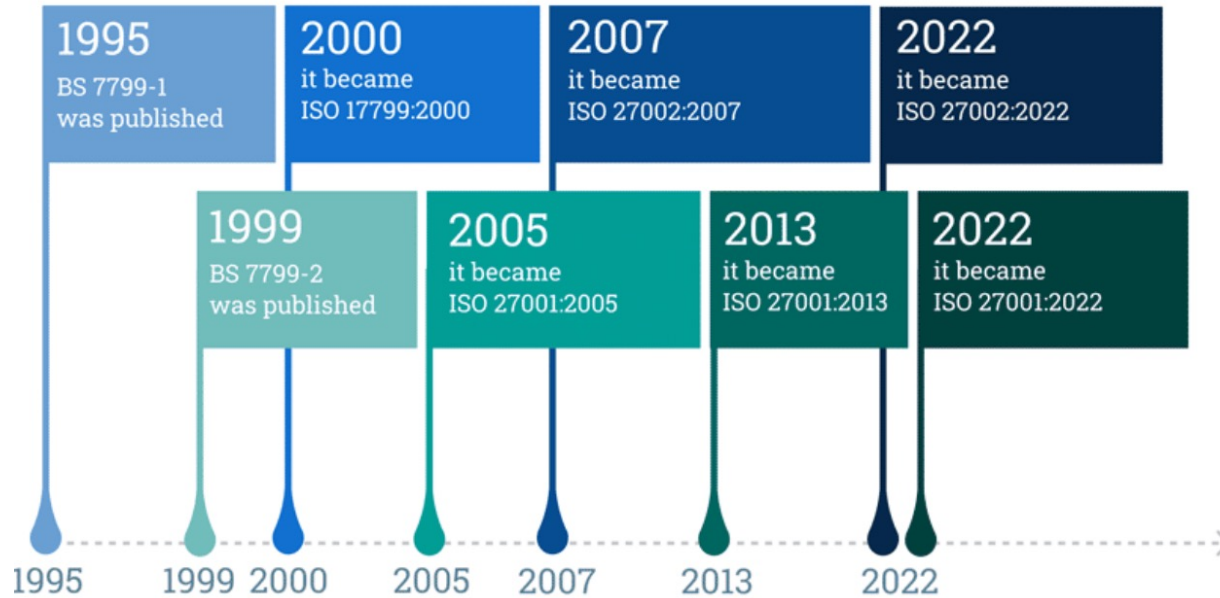
ISO 27001:2022 Zaman Çizelgesi

TARİH	AKTİVİTE
25 Ekim 2022	ISO/IEC 27001:2022 standardının yayınlanması
31 Ekim 2023	Tüm akredite Belgelendirme Kuruluşlarının geçişinin tamamlanması
31 Ekim 2023	Bu tarihten itibaren Belgelendirme Kuruluşları başvuruları yalnızca ISO/IEC 27001:2022'ye göre almaktadır.
31 Ekim 2025	Tüm sertifikalı müşterilerin ISO/IEC 27001:2022'ye geçişinin tamamlanması



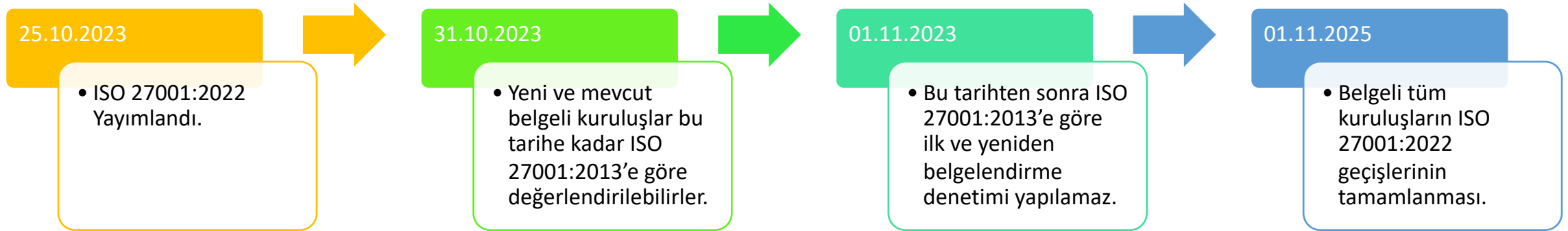
ISO 27001 Tarihçesi

ISO 27001 & ISO 27002 history



ISO 27001:2022 Zaman Çizelgesi

ISO/IEC 27001:2022 standardı 25 Ekim 2022'de yayınlandı. Uluslararası Akreditasyon Forumu (IAF), yeni sürüm için geçiş koşullarını MD 26 belgesinde duyurdu. Geçiş süreci için 3 yıllık süre tanınmaktadır.



Geçiş ile ilgili neler yapılmalı?

- Geçiş denetimleri, önceden planlanmış bir gözetim/yeniden belgelendirme incelemesiyle bağlantılı olarak veya ayrı bir denetimde gerçekleştirilebilir.
- Geçiş denetimi, özellikle teknolojik bilgi güvenliği kontrollerinin gözden geçirilmesi için sadece belgelerin incelenmesine dayanmayacak;
- Müşteriler tarafından seçilen yeni veya değiştirilmiş bilgi güvenliği kontrollerinin uygulanması ve etkinliği.
- ISO/IEC 27001:2022'nin boşluk analizi bilgi güvenliği yönetim sisteminde (ISMS) değişiklik ihtiyacı belirlenmelidir.
- Uygulanabilirlik Beyanı'nın (SoA) Güncellenmesi
- Risk işleme planının güncellenmesi (varsa)
- SoA'larına göre müşteriler tarafından uygun şekilde seçilen yeni veya değiştirilmiş kontrollerin uygulanması ve etkinliği.

geçiş için yapılması gerekenler

- *Yeniden sertifikalandırma denetimiyle birlikte geçiş gerçekleştirildiğinde, geçiş denetimi için minimum (0,5) günlük ek bir denetim gerçekleştirilecektir.*
- *Geçiş, bir gözetim denetimi veya ayrı bir denetim sırasında olduğunda, sertifikalı müşterinin geçişini doğrulamak için (1,0) günlük ek bir denetim gerçekleştirilecektir.*
- *Geçiş denetimi başarıyla tamamlanırsa, sertifika belgesi ISO/IEC 27001:2022'ye uygunluğu yansıtacak şekilde güncellenecektir; ancak, mevcut sertifika döngüsünün sona erme tarihi değiştirilmeyecektir”*

Temel Değişiklikler

- **4.2 İlgili tarafların iyileştirilmesi**

İlgili taraf gereksinimlerinden hangisinin BGYS aracılığıyla ele alınması gerektiğinin bir analizini gerektiren (c) maddesi eklenmiştir.

- **4.4 BGYS'nin iyileştirilmesi**

“ihtiyaç duyulan süreçler ve etkileşimleri dahil” ifadesi eklenmiştir. Bu kapsayıcılık, farklı bireysel süreçler arasında sorunsuz geçişi sağlama ihtiyacını yansıtmakta ve süreçler arasındaki etkileşime ve birinden diğerine teslim etmeye odaklanmakta.

Süreç etkileşimlerinin oluşturulması istenmektedir.

- **5.3 Rol ve Sorumluluklar**

(Kurumsal roller, sorumluluklar ve yetkiler), rollerin iletişiminin kuruluş içinde dahili olarak yapıldığını açıklığa kavuşturmak için bir ifade eklenmiştir.

- **6.1.3 Risk yönetiminin iyileştirilmesi**

Temel Değişiklikler

- **6.2 Hedefin İyileştirilmesi**

Hedeflerin izlenmesinin gerekliliğini içeren d maddesi eklenmiştir.

- **6.3 Değişiklik yönetiminin eklenmesi**

Bu yepyeni bir alt maddedir ve 2015 yılında ISO 9001'e girişi yansıtmaktadır. Burada, değişikliğin amacı ve potansiyel sonuçları, BGYS'nizi nasıl etkileyebileceği, kaynakların mevcudiyeti ve sorumlulukların ve yetkililerin tahsisi veya yeniden tahsisi gibi faktörleri göz önünde bulundurmanız gerekecektir.

- **7.4 İletişimin İyileştirilmesi**

İletişim için süreçlerin ayarlanmasını gerektiren (e) maddesi silinmiştir.

Temel Değişiklikler

- **8.1 Operasyonel planlamanın yeniden düzenlenmesi**

Güvenlik süreçleri için kriterlerin oluşturulması ve bu kriterlere göre süreçlerin uygulanması için yeni gereksinimler eklenmiştir. Aynı maddede, hedeflere ulaşmak için planların uygulanması şartı kaldırılmıştır.

- **9.1 İzlemenin iyileştirilmesi**

- **9.2'yi 9.2.1 Genel / 9.2.2 olarak bölünmesi**

9.2.1 ve 9.2.2 olarak bölünmüştür.

Temel Değişiklikler

- **9.3“ü 9.3.1”e bölme Genel / 9.3.2 / 9.3.3 (ve ekstra bir konunun eklenmesi)**

Madde 9.3.2 c) Dikkate alınması gereken bir diğer yeni gereklilik ise “BGYS ile ilgili ilgili ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikler”dir. Burada, bu ihtiyaçları, beklentileri ve bunu yaptığınıza dair kanıtları nasıl izleyebileceğinizi ve gözden geçirebileceğinizi düşünmeniz gerekecektir.

Yani, ilgili taraflardan gelen girdilerin onların ihtiyaçları ve beklentileri ile ilgili ve BGYS ile ilgili olması gerektiğini açıklayan yeni maddedir.

- **10.1 İyileştirme ve 10.2 Uygunsuzluklar**

Madde 10'da (İyileştirme), alt maddeler yer değiştirmiştir, bu nedenle ilki Sürekli iyileştirme (10.1) ve ikincisi Uygunsuzluk ve düzeltici faaliyet (10.2) olup, bu maddelerin metni değişmemiştir.

ISO 27002 (EK-A Kontrolleri)

ISO/IEC 27002:2013

14 Başlık ve 114 Kontrol

ISO 27002:2022

4 Başlık ve 93 Kontrol

- Organizasyonel
 - İnsan
 - Teknolojik
 - Fiziksel
-

ISO 27002 (EK-A Kontrolleri)

YENİ KONTROLLER

- 5.7** Tehdit istihbaratı
- 5.23** Bulut hizmetlerinin kullanımı için bilgi güvenliği
- 5.30** İş sürekliliği için ICT hazırlığı
- 7.4** Fiziksel güvenlik izleme
- 8.9** Yapılandırma yönetimi
- 8.10** Bilgi silme
- 8.11** Veri maskeleyme
- 8.12** Veri sızıntısının önlenmesi 8.16 İzleme faaliyetleri
- 8.23** Web filtreleme
- 8.28** Güvenli kodlama

Detaylı Bilgi İçin



DSR Uluslararası Gözetim ve Belgelendirme Hiz. Ltd. Şti.

Yeşilbağlar mah. Helis Beyaz Ofis A Blok K:2 D:207 Pendik/İSTANBUL

info@dsrbelgelendirme.com.tr, 0(216) 606 06 35

Ocak 2023