TÜVNORD

Inspired by Knowledge

Müşteri Bilgilendirmesi
“ISO/IEC 27006-1:2024“ – Geçiş

Mevcut ISO 27001 sertifikanızla ilgili önemli bilgiler!

Değerli **ISO 27001 sertifi**kasyon müşterisi,

ISO 27006 standardı gözden geçirilerek Mart 2024’te ISO/IEC 27006-1:2024 olarak yayımlanmıştır. Bu standart, ISO 27001’e dayalı yönetim sistemlerinin denetim ve sertifikalandırma kurallarını tanımlar.

Uluslararası Akreditasyon Forumu” (IAF), 21 Mayıs 2024 tarihli “IAF MD 29 – ISO/IEC 27006-1:2024 Geçiş Gereklilikleri” dokümanında iki yıllık bir geçiş dönemi ve bazı geçiş düzenlemeleri tanımlamıştır. Buna göre, 31 Mart 2026’da sona erecek geçiş döneminden sonra, ISO 27001’e uygun tüm sertifikasyonlar yalnızca ISO 27006’nın yeni baskısına dayanacaktır.

7 Ağustos 2024’te Alman Akreditasyon Kurumu (DAkkS), 6 Kasım 2024’te de Türk Akreditasyon Kurumu TÜRKAK geçiş kurallarını yayımlamıştır. Bu bildirimler, anılan IAF belgesi “IAF MD 29”a atıfta bulunmaktadır. Uygunluk değerlendirme kuruluşlarının yükümlülükleri arasında, akredite edilmiş müşterileri geçiş süreci ve ayrıntılar hakkında bilgilendirmek de yer almaktadır.

Notlar

ISO/IEC 27006-1:2024 standardının Almanca versiyonu, DIN EN ISO/IEC 27006-1:2024, Ağustos 2024’te yayımlanmıştır. Her iki versiyonun içeriği eşdeğerdir; bu dokümanda ISO/IEC 27006-1:2024 için yapılan açıklamalar hem DAkkS hem de TÜRKAK için geçerlidir.

Ayrıca, bu dokümanda ISO/IEC 27001 için yapılan açıklamalar, ISO/IEC 27001 standardının Almanca çevirisi olan DIN EN ISO/IEC 27001 ve Türkçe çevirisi olan TS EN/ISO IEC 27001 için de aynı şekilde geçerlidir.

TÜV NORD CERT, akreditasyonun yeni baskı ISO/IEC 27006-1:2024 standardına genişletilmesi ve geçişi için DAkkS’a ve TÜRKAK’a başvuruda bulunacaktır.

ISO 27001 sertifikasyonunun ISO 27006’nın yeni sürümüne göre sürdürülmesi

Yeni ISO/IEC 27006-1:2024 standard versiyonu, ISO 27001’in kendisi ISO/IEC 27006-1:2024’teki revizyonlardan etkilenmediğinden, bilgi güvenliği yönetim sisteminizin (ISMS) herhangi bir uyarlamaya ihtiyaç duymasını gerektirmez.

Mevcut sertifikaların geçerliliği ve son kullanma tarihi, ISO/IEC 27006-1:2024’teki revizyonlardan etkilenmeyecektir.

IAF, DAkkS ve TÜRKAK tarafından belirlenen bazı özellikler aşağıda dikkatinize sunulmaktadır:

- ISO/IEC 27006-1:2024 gerekliliklerine uygun denetimler, akreditasyonun genişletilmesi ve geçiş süreci tamamlandıktan sonra gerçekleştirilebilir.
- DAkkS ve TÜRKAK tarafından ISO/IEC 27006-1:2024 akreditasyonunun genişletilmesi ve geçişi tamamlandığında (akreditasyon geçişi), TÜV NORD CERT her ilk sertifikalandırma ve yeniden sertifikalandırma denetimini yeni versiyon ISO/IEC 27006-1:2024’e göre gerçekleştirecektir.
- 31 Mart 2026’dan sonra başlayan her denetim, yeni sürüm ISO/IEC 27006-1:2024’e uygun şekilde gerçekleştirilecektir.
- Akreditasyon geçişi tarihinden önce sertifikalandırılan müşteriler için, TÜV NORD CERT, ISO/IEC 27006:2015 veya ISO/IEC 27006-1:2024 sürümlerinden herhangi birini,ISO/IEC 27006-1:2024 akreditasyonu sonrasında yapılacak gözetim denetimleri için kullanabilir.
- Bilgi Güvenliği Yönetim Sisteminize (BGYS) yönelik ek veya değişen bir gereksinim olmadığından, geçiş denetimlerinde ek denetim süresi talep edilmeyecektir.

Akreditasyon geçişinden sonra düzenlenen sertifikalarda, açık şekilde tanımlama yapılabilmesi için geçerli olan ISO/IEC 27006-1:2024 sertifikasyon kurallarına atıf bulunacaktır.

ISO27006 yeni sürümündeki Önemli değişiklikler

Denetim süresi hesaplama gereksinimleri güncellenmesi

Yeni kavramlar, denetim süresinin hesaplanma yöntemini etkilemektedir; özellikle başlangıç personel sayısının belirlenmesi (bkz. ISO/IEC 27006-1:2024, C.2.1 ve C.3.4) ile çok sahalı kuruluşların denetim süresinin hesaplanmasının netleştirilmesi (bkz. ISO/IEC 27006-1:2024, C.6) hususlarında.

Uzaktan denetimler için gereksinimlerin netleştirilmesi

Uzaktan denetim, denetçinin sahaya gitmek yerine dijital olarak bağlandığı denetim türü olarak tanımlanır. Daha önce, ISMS denetimlerinin uzaktan gerçekleştirilen kısmı toplam saha denetim süresinin en fazla %30'u ile sınırlandırılmıştı.

Yeni standardın versiyonuyla bu sınır kaldırılmış olup, denetimin tamamının (yüzde 100'e kadar) uzaktan gerçekleştirilmesi mümkündür. Uygulanacak uzaktan denetim oranı, "uzaktan denetim kullanımına ilişkin risk analizi" sonucunda belirlenir. Bu analizde; mevcut altyapı, sektör, denetim türü, kapsam, kuruluş yapısı gibi çeşitli faktörler dikkate alınır (bkz. ISO/IEC 27006-1:2024, 9.1.3.3).

Burada ele alınan değişiklikler, teklif aşamasında müşteriden talep edilecek bilgilerin öncekine göre biraz daha kapsamlı olduğu anlamına gelmektedir.

Sonuç

Başarılı bir ISO 27001 sertifikasyonunun sürdürülmesi için, sertifikasyon süreçlerinde bazı değişiklikler olsa bile BGYS'nin ISO/IEC 27006-1:2024'e uyarlanması gerekli değildir ve geçiş denetimlerinde ek denetim süresi talep edilmeyecektir.

Sizinle işbirliğimizi aynı şekilde sürdürmeyi dört gözle bekliyoruz.

24-0587-05/25