

REHBER

ISO 27001 Sertifikasyonuna Hazırlık Rehberi

ISO 27001 sertifikasına giden yolu sade adımlara ayıran, ilk kez başlayan kurumlar için pratik bir rehber hazırladık.



REHBER

YAKLAŞIK 7 DK OKUMA

ISO 27001

BU REHBERDE

1. ISO 27001 nedir, ne sağlar?
2. Yol haritası: altı adımda sertifikasyon
3. Kapsamı doğru belirlemek
4. Risk değerlendirme ve Uygulanabilirlik Bildirgesi (SoA)
5. Belgelendirme tetkiki öncesi kontrol listesi
6. Sık yapılan hatalar

01 ISO 27001 nedir, ne sağlar?

ISO 27001, bir Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) gereksinimlerini tanımlayan uluslararası standarttır. Amacı bilgi güvenliğini kişilere ve tek tek araçlara bırakmak yerine risk temelli, sürekli iyileştirilen bir yönetim sistemine dönüştürmektir. Sertifika, bağımsız bir belgelendirme kuruluşunun yaptığı tetkiklerle verilir ve genellikle üç yıl geçerlidir; bu sürede yıllık gözetim tetkikleri yapılır.

Neden önemli? Müşteri ve ihale şartnamelerinde ISO 27001 giderek daha sık aranıyor. Ancak asıl değer, riskleri bilerek yönetmek ve kanıtlayabilmektir.

02 Yol haritası: altı adımda sertifikasyon

Her kurumun süresi farklıdır; ancak sıra neredeyse hep aynıdır:



03 Kapsamı doğru belirlemek

Kapsam, sonraki her adımın zeminidir. Çok geniş seçilirse proje uzar; çok dar seçilirse sertifikanın değeri düşer.

- Hangi iş birimleri, lokasyonlar ve süreçler kapsamda?
- Hangi bilgi varlıkları ve sistemler bu süreçlere dayanıyor?
- Dış tedarikçilere ve bulut hizmetlerine bağımlılıklar neler?
- Kapsam dışı bırakılan bir alan varsa gerekçesi yazılı mı?

İpucu: Dar bir kapsamla başlayıp sonraki yıllarda genişletmek mümkündür.

04 Risk değerlendirme ve Uygulanabilirlik Bildirgesi (SoA)

Standart, hazır bir kontrol listesini uygulamanızı değil, risklerinize göre kontrol seçmenizi ister.

- Bilgi varlıklarının envanterini çıkarın ve sahiplerini belirleyin.
- Tehdit ve zafiyetleri belirleyip olasılık ve etkiyi derecelendirin.
- Her risk için işleme kararı verin: azalt, aktar, kabul et veya kaçın.
- Ek A'daki 93 kontrolden (ISO 27001:2022) hangilerinin uygulandığını, hangilerinin gerekçesiyle hariç tutulduğunu SoA'da gösterin.

05 Belgelendirme tetkiki öncesi kontrol listesi

☐ Kapsam bildirimi onaylandı	☐ Bilgi güvenliği politikası yayımlandı ve duyuruldu
☐ Risk değerlendirme ve risk işleme planı güncel	☐ SoA hazır ve güncel

☐ İç tetkik yapıldı, bulgular kapatıldı

☐ Yönetimin gözden geçirme toplantısı yapıldı ve kayıt altına alındı

☐ Farkındalık eğitimi ve olay kayıtları mevcut

☐ Düzeltici faaliyetler kayıt altında

06

Sık yapılan hatalar

- Sertifika için doküman yığmak, uygulamayı atlamak
- Yönetim desteğini ve kaynak ayrımını baştan almamak
- Risk değerlendirmesini formalite olarak doldurmak
- İç tetkiki geç ve yüzeysel yapmak
- Kapsamı gereğinden geniş seçip projeyi uzatmak

ISO 27001 yolculuğunuza birlikte başlayalım Mevcut durumunuzu birlikte değerlendirip size uygun bir yol haritası çıkaralım.

// İLETİŞİM

Bize ulaşın

İhtiyacınızı ve mevcut durumunuzu paylaşın; size uygun kapsamı ve yol haritasını birlikte belirleyelim. Bilgi formumuzu doldurabilir veya doğrudan bize ulaşabilirsiniz.

Troy Bilgi Teknolojileri Ticaret Limited Şirketi

Atatürk Mah. Vedat Günyol Cad. 44M/2

Ataşehir / İstanbul

T 0-216-575 5222 **E** info@troybilgiteknolojileri.com



Hizmet sayfası ve bilgi formu için QR kodu okutun