ISO 27001 Risk ve Varlık Envanteri Kontrol Listesi

Bilgi varlıklarını, sahiplerini, tehditleri, kontrolleri ve risk aksiyonlarını hazırlık öncesinde eşleştirin.

Sürüm	1.0	Güncelleme	2026-08-23
Kapsam	Bilgi teknolojileri ve tüm sektörler	Teknik durum	Teknik inceleme bekliyor

Kullanım

Her satırı evet, kısmen, hayır veya kapsam dışı olarak değerlendirin. Kanıt alanına belge adı yerine erişilebilir kayıt, tarih ve sorumlu bilgisi yazın. Açıkları sorumlu, termin ve doğrulama yöntemiyle aksiyona dönüştürün.

Varlıklar	Bilgi, uygulama, cihaz, hizmet ve tesis varlıkları envanterde mi?	Varlık envanteri, sahiplik kaydı	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
Sınıflandırma	Varlıkların önem, gizlilik ve erişilebilirlik seviyesi tanımlı mı?	Sınıflandırma kuralı, kayıt	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
Risk	Tehdit, zafiyet, etki ve olasılık birlikte değerlendiriliyor mu?	Risk değerlendirmesi	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
Kontroller	Risklere karşı teknik, fiziksel ve yönetsel kontroller atanmış mı?	Kontrol planı, sorumlu matrisi	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
Erişim	Yetki talebi, onay, gözden geçirme ve iptal kayıtları tutuluyor mu?	Erişim kayıtları	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
Olay	Bilgi güvenliği olayları sınıflandırılıyor ve öğrenimler aksiyona bağlanıyor mu?	Olay kaydı, aksiyon planı	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
Süreklilik	Yedekleme, kurtarma ve kritik hizmet bağımlılıkları test ediliyor mu?	Test raporu, kurtarma kaydı	☐ Evet ☐ Kısmen ☐ Hayır Not: _____
İyileştirme	İç tetkik ve yönetim kararları risk kaydına geri besleniyor mu?	Tetkik ve YGG kanıtı	☐ Evet ☐ Kısmen ☐ Hayır Not: _____

Sınırlama

Bu kaynak genel hazırlık ve öz değerlendirme amacıyla sunulur. İşletmeye özel mevzuat, risk değerlendirmesi, hukuki görüş, belgelendirme veya resmî uygunluk kararının yerine geçmez. Kullanıcı güncel gereklilikleri ve kendi saha koşullarını ayrıca doğrulamalıdır.