CI|cert

01.12.2022

ISO/IEC 27001:2022 REVİZYONU YAYINLANDI

TEMEL DEĞİŞİKLİKLER

Standardın bu versiyondaki değişiklikler, esas olarak, Şubat 2022 de ISO/IEC 27002'nin yeni versiyonunun yayınlanmasıyla öngörülen ve güvenlik kontrollerinin eklendiği, silindiği veya birleştirildiği Ek A'da yer almaktadır. Orta seviyedeki bu değişikliklerin yanı sıra standardın madde 4'ten madde 10'a kadar olan ana kısmında minör seviyede değişiklikler mevcuttur. ISO 27001:2013'ten önemli hiçbir şart kaldırılmamıştır.

YÖNETİM SİSTEMİNDEKİ DEĞİŞİKLİKLER

4.2c) İlgili tarafların gereksinimlerden hangisinin bilgi güvenliği yönetim sistemi aracılığıyla karşılanacağı (genişletilmiş şart)

6.3) Değişikliklerin planlanması (ilave şart)

8.1) Süreçler için kriterler oluşturmak ve bu kriterler için kontrolleri uygulamak (genişletilmiş şart)

9.3.2c) Yönetimin gözden geçirme girdisi- ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikler (genişletilmiş şart)

EK A GÜVENLİK KONTROLLERİNDEKİ DEĞİŞİKLİKLER

ISO/IEC 27001, finansal bilgiler ve fikri mülkiyetten çalışan detaylarına ve daha fazlasına kadar şirketlere bilgi varlıklarını güvende tutmak için risklerini yönetmesi ve tehditlere karşı korunmasına bir çerçeve sağlayan uluslararası bir standarttır.

2022 versiyonunda şirketlerin üstesinden gelmesi gereken yeni senaryolar ele alınmaktadır. Siber güvenlik ve gizlilik konularını içerecek şekilde genişletilen, kontrol dili yenilenen ve ek rehberlik eklenen bu değişiklikler, şirketlerin risklerini yönetirken hiçbir şeyin atlanmadığından emin olmasına ve gerektiği gibi takip etmesine yardımcı olacaktır.

YENİ GÜVENLİK KONTROLLERİ	
A.5.7	Tehdit istihbaratı
A.5.23	Bulut hizmetlerinin kullanımı için bilgi güvenliği
A.5.30	İş sürekliliği için BİT hazırlığı
A.7.4	Fiziksel güvenlik izleme
A.8.9	Konfigürasyon yönetimi
A.8.10	Bilgi silme
A.8.11	Veri maskeleme
A.8.12	Veri sızıntısı önleme
A.8.16	İzleme faaliyetleri
A.8.23	Web filtreleme
A.8.28	Güvenli kodlama

YENİ VERSİYONA GEÇİŞ İÇİN…

Geçiş için hazırlanmaya mümkün olduğunca erken başlamanızı ve gerekli değişiklikleri yönetim sisteminize dahil etmek için uygun şekilde planlamanızı öneririz

Geçiş için önerilen adımlar:

- ❖ Standardın yeni versiyonun içeriğini ve gerekliliklerini öğrenin. Değişikliklere odaklanın.
- ❖ Kuruluşunuzdaki ilgili personelin eğitimli olduğundan ve gereksinimleri ve önemli değişiklikleri anladığından emin olun.
- ❖ Yeni gereklilikleri karşılamak ve bir uygulama planı oluşturmak için ele alınması gereken boşlukları belirleyin.
- ❖ Eylemleri uygulayın ve yeni gereksinimleri karşılamak için yönetim sisteminizi güncelleyin.

CİCERT geçiş tetkiklerini yürütürken aşağıdakilerin kontrolünü sağlayacaktır

- ISO/IEC 27001:2022'nin boşluk analizi ve müşterinin BGYS'sinde değişiklik ihtiyacı;
- Uygulanabilirlik beyanının güncellenmesi (SoA);
- Varsa, risk işleme planının güncellenmesi;
- Müşteriler tarafından seçilen yeni veya değiştirilmiş kontrollerin uygulanması ve etkinliği.

✓ *Geçiş Eğitimi*
✓ *Boşluk Analizi*
✓ *Geçiş tetkikleri*

için bizimle iletişime geçebilirsiniz

Geçiş süresi 3 yıl olarak belirlendi. Bu nedenle mevcut 2013 versiyonlu sertifikaların Kasım 2025'ten önce yeni sürüme geçirilmesi gerekmektedir.

Geçiş tetkiki, 3 yıllık geçiş döneminde herhangi bir programlı tetkik sırasında gerçekleştirilebileceği gibi, özel geçiş tetkiki olarak da gerçekleştirilebilecektir

Cicert, 2023 yılı ikinci yarısından itibaren geçiş tetkiklerini yapmaya ve yeni versiyonda başvuruları almaya başlayacaktır

CI|cert

Cicert Belgelendirme Hizmetleri Ltd. Şti.
Soğanlık Yeni Mah. Fuatpaşa Sok.
Kartal İstofis No: 12 Daire: 10 Kartal
İstanbul, 34880

+(90) 0 216 546 05 26
cicert@cicert.com.tr
www.cicert.com.tr