ISO 27002:2013 VE ISO 27002:2005 ARASINDAKİ TEMEL FARKLAR NELERDİR?

ISO 27002:2005 standardının yeni sürümü ISO 27002:2013 olarak 01/10/2013 tarihli olarak yayımlandı.

Temel değişiklikler;

Kontrol Sayısı: Kontrol sayısı 133'ten 114'e düşürüldü.

Bölüm Sayısı: Kontrol sayısının azalmasına rağmen bölüm sayısı 11'den 14'e çıktı.

Bölümlerin Yapısı: Yeni standart üzerinde yer alan temel başlıklar aşağıdaki gibidir;

Bölümlerin Yapısındaki Temel Değişiklikler

Kriptografi ayrı bir bölüm haline getirilmiştir. (A-10)

Tedarikçi ilişkileri ayrı bir bölüm haline getirilmiştir. (A-15)

İletişim ve operasyon yönetimi ayrılarak ayrı birer bölüm haline gelmiştir. Yeni sürümde A-12 Operasyonların Güvenliği ve A-13 İletişim Güvenliği olarak iki ayrı bölüm mevcuttur.

Bölümlerin incelenmesi;

5- Bilgi Güvenliği Politikaları
6- Bilgi Güvenliği Organizasyonu
7- İnsan Kaynakları Güvenliği
8- Varlık Yönetimi
9- Erişim Kontrolü
10- Kriptografi
11- Fiziksel ve Çevresel Güvenlik
12- Operasyon Güvenliği
13- İletişim Güvenliği
14- Sistem Edinim, Geliştirme ve Bakımı
15- Tedarikçi İlişkileri
16- Bilgi Güvenliği İhlal Olayı Yönetimi
17- İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönü
18- Uyum

Yeni Eklenen Kontroller

A. 6.1.5 Proje yönetiminde bilgi güvenliği
A.12.6.2 Yazılım kurulumu ile ilgili kısıtlama
A.14.2.1 Güvenli geliştirme politikası
A.14.2.5 Güvenli sistem mühendisliği prensipleri
A.14.2.8 Sistem güvenlik testi
A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası
A.15.1.3 Bilgi ve iletişim teknolojileri tedarik zinciri
A.16.1.4 Bilgi güvenliği olaylarını değerlendirme ve karar alma
A.16.1.5 Bilgi güvenliği ihlal olaylarına tepki verme
A.17.2.1 Bilgi işleme tesislerinin erişilebilirliği

Güvenlik Kategorilerinin Yerleştirilmesi

- Mobil cihazlar ve uzaktan çalışma daha önce erişim kontrolü bölümündeydi; şimdi ise bilgi güvenliği organizasyonunun (6) altında 6.2 inci kısım olarak yer almaktadır.
- Ortam işleme daha önce iletişim ve operasyon yönetimi altındayken, şimdi varlık yönetimi (8) altında 8.3 üncü kısım olarak yer almaktadır.
- İşletim sistemi erişim kontrolü ile uygulama ve bilgi erişim kontrolü, sistem ve uygulama erişim kontrolü olarak birleştirilmiş ve Erişim kontrolü (9) altında 9.4 üncü kısım olarak kalmıştır.
- Operasyonel yazılım kontrolü daha önce bilgi sistemleri edinim, geliştirme ve bakımın altında tek bir kontrolken, şimdi 12.5 olarak operasyon güvenliği altında ayrı bir kısımdır.
- Bilgi sistemleri denetim hususları uyum bölümünden operasyon güvenliği altına 12.7 inci kısım olarak aktarılmıştır.
- Bilgi değişimi iletişim güvenliğinin (13) altında 13.2 inci kısım olarak yer almıştır.
- Tartışmalı bir kategori olan uygulamalarda doğru işleme kaldırıldı. Önceki standartta ise bilgi sistemi edinim, geliştirme ve bakımın altında yer almaktadır.
- Elektronik ticaret hizmetleri ayrı bir kategori olmaktan çıkartılarak, kontrolleri bilgi sistemi güvenlik gereksinimleri ile birleştirildi (14.1).
- Bilgi güvenliği olay yönetimi altındaki 2 kategori tek bir başlıkta birleştirildi. İş sürekliliği bölümüne ise yeni bir kategori eklenerek (Yedekleme 17.2). Bu kategori temel olarak felaketten kurtarma ile ilgili.

Yeni Kontroller

14.2.1- Güvenlik geliştirme politikası- Yazılım ve bilgi sistemleri geliştirme için kurallar

14.2.5- Güvenli sistem mühendisliği prensipleri- Sistem mühendisliği ilkeleri

14.2.6- Güvenli geliştirme ortamı- Geliştirme ortamı oluşturulması ve korunması

14.2.8- Sistem güvenlik testi- Güvenlik fonksiyonları testleri

16.1.4- Bilgi güvenliği olayları değerlendirme ve karar alma- Olay yönetiminin bir parçası

17.2.1- Bilgi işleme tesislerinin erişilebilirliği- Yedekleme

Çıkartılan Kontroller

6.2.2- Müşterilerle ilgilenirken güvenliği ifade etme

10.4.2- Mobil koda karşı kontroller

10.7.3- Bilgi işleme prosedürleri

10.7.4- Sistem dokümantasyonu güvenliği

10.8.5- İş bilgi sistemleri

10.9.3- Herkese açık bilgi

11.4.2- Dış bağlantılar için kullanıcı kimlik doğrulama

11.4.3- Ağlarda teçhizat tanımlama

11.4.4- Uzak tanı ve yapılandırma portu koruma

11.4.6- Ağ bağlantı kontrolü

11.4.7- Ağ yönlendirme kontrolü

12.2.1- Giriş verisi geçerleme

12.2.2- İç işleme kontrolü

12.2.3- Mesaj bütünlüğü

12.2.4- Çıkış verisi geçerleme

11.5.5- Oturum zaman aşımı

11.5.6- Bağlantı süresinin sınırlandırılması
11.6.2- Hassas sistem yalıtımı
12.5.4- Bilgi sızması
14.1.2- İş sürekliliği ve risk değerlendirme
14.1.3- Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme
14.1.4- İş sürekliliği planlama çerçevesi
15.1.5- Bilgi işleme olanaklarının kötüye kullanımını önleme
15.3.2- Bilgi sistemleri denetim araçlarının korunması

ISO 27002 yapısı tamamen ISO 27001 kontrolleri ile uyumlu olduğundan tüm değişiklikler yeni IS0 27001 EK-A sı içinde geçerlidir. Değişikliklerin çoğu aslında mevcut ISO 27002 nin yanlış yapısının düzeltilmesi ve yeni kontrollerin eklenmesini içeriyor. Ağ güvenliği ve geliştirme sürecinde ise bazı değişiklikler mevcut. Bu alanlarda yeni standarda göre daha esnek bir tarif ve nasıl uygulama yapılacağı kısmında serbestlik vardır.

ISO 27001 Bilgi Güvenliği Hizmetleri: http://www.btyon.com.tr/bilgi_guvenligi.php

ISO 27001 Bilgi Güvenliği Eğitimleri: http://www.btyon.com.tr/bilgi_guvenligi_egitimleri.php

ISO 27001 Danışmanık Hizmeti: http://www.btyon.com.tr/iso-27001-danismanlik.php