For the latest from BDO Turkey, follow us

BDO Yayıncılık A.Ş.

Eski Büyükdere Cad. No.14
Park Plaza Kat:4
34398 Maslak/İstanbul
Turkey

Tel: +90 212 365 62 00
Fax: +90 212 365 62 02
e-mail: bdo@bdo.com.tr
www.bdo.com.tr

Sirküler Tarihi : 31.10.2022
Sirküler No : 2022/001

ISO 27001'İN YENİ SÜRÜMÜ YAYINLANDI

İş dünyası, hükümetler ve toplum için büyüyen bir tehdit haline gelen siber saldırıların neden olduğu maliyetlerin ve yıkıcı etkilerin boyutu giderek artıyor. Buna paralel olarak bir kuruluş için, bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gereklilikleri belirten ISO/IEC 27001'in yeni ve geliştirilmiş bir sürümü yayınlandı[1].

Bilgi güvenliği yönetimi konusunda dünyanın en iyi bilinen standardı, günümüzün giderek dijitalleşen dünyasında kuruluşlar için hayati önem taşıyan bilgi varlıklarının güvence altına alınması için izlenmesi gereken yolu ve uygulanması gereken kontrolleri içermektedir.

Öncelikle ISO 27001 ve 27002 arasındaki farkı hatırlatalım:
ISO 27001, bilgi güvenliği için bir yönetim sistemi uygulamak için gereklilikleri içerirken, ISO 27002, güvenliğinizi geliştirmek için uygulayabileceğiniz bir dizi güvenlik kontrolü (veya "önlemi") biçimindeki en iyi uygulamaları içerir.
ISO 27001, Ek A'daki ISO 27002'deki kontrollerden yararlanır (ancak normatif biçimde yeniden yazılmıştır; örneğin, "gerekir" yerine "olmalı" ifadesini kullanır[2])

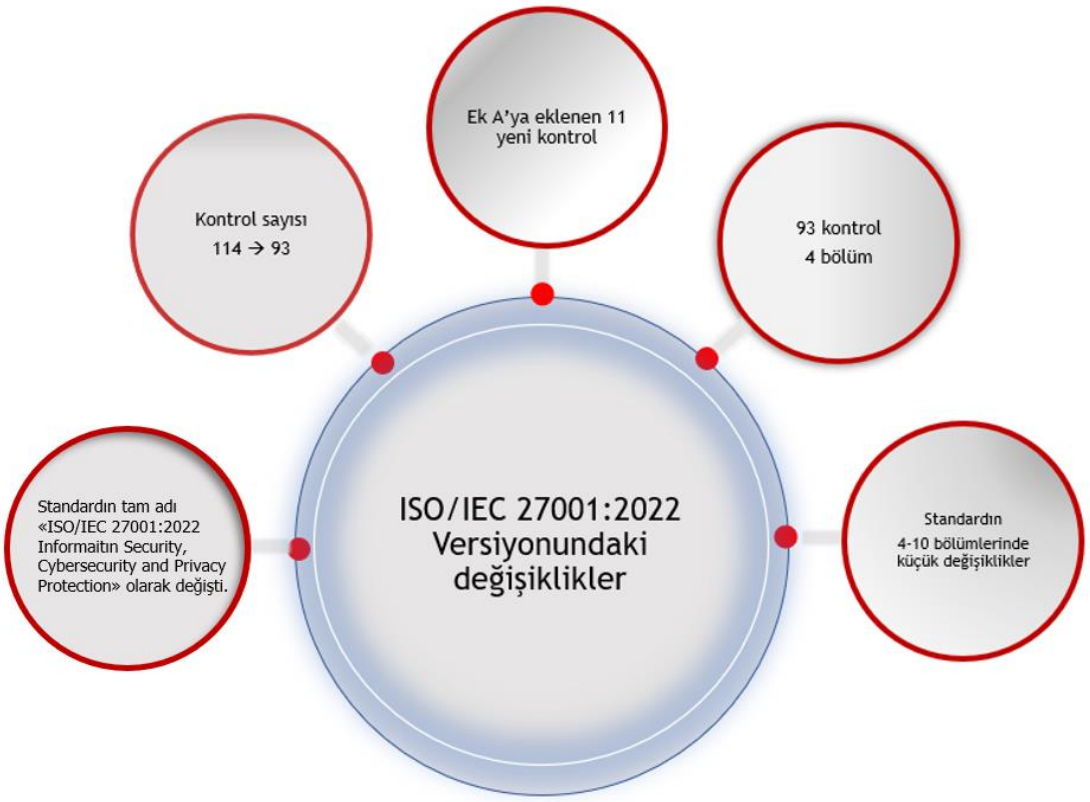
ISO 27001, sertifikalanılacak standartken, ISO 27002 "*sadece*" uygulama pratiklerini (code of practice) anlatır.

[1] https://www.iso.org/standard/825875.html
[2] İngilizce versiyonda : it uses "shall" instead of "should"

Sirkülerimizde aşağıdaki soruların yanıtlarını vermeye çalışacağız;

- Temel değişiklikler nelerdir?
- Bu değişiklikler, zaten ISO 27001:2013 sertifikasına sahip kuruluşları nasıl etkileyecek?
- ISO 27001 sertifikasına sahip olmak isteyen kuruluşlar ne yapacak?
- ISO / IEC 27001: 2022'ye nasıl hazırlanmalı?

TEMEL DEĞİŞİKLİKLER NELERDİR ?



Önceki sürümün 14 bölümünden ziyade, ISO 27002:2022 artık sadece dört bölüme ve iki eke sahiptir:

- Organizasyonel kontroller (madde 5): Bu bölüm, 37 kontrolden oluşan çeşitli organizasyonel konularla ilgili tüm kontrolleri içerir.
- İnsan kontrolleri (madde 6): Bu bölüm, 8 kontrolden oluşan insan kaynakları güvenliği ile ilgili kontrollere odaklanmaktadır.
- Fiziksel kontroller (madde 7): Bu bölüm, 14 kontrolden oluşan fiziksel çevre ile ilgili kontrollere odaklanmaktadır.
- Teknolojik kontroller (madde 8): Bu bölüm, 34 kontrolden oluşan teknolojik çözümlerle ilgili kontrollere odaklanmaktadır.
- Ek A – Öznitelikleri kullanma: Bu ek, tüm yeni denetimlerin bir matrisini sağlar ve özniteliklerini karşılaştırır ve denetimlerin özniteliklerine göre nasıl kullanılabileceği konusunda öneriler sunar.
- Ek B – ISO/IEC 27002:2013 ile yazışmalar: Bu ek, bu sürümdeki kontroller ile önceki 2013 sürümündeki kontroller arasında bir eşleme sağlar.

Bölüm sayısının azaltılması ve kontrollerin nasıl kullanılacağına dair rehberlik içeren bir ekin eklenmesi, kontrollerin uygulanabilirliğini ve sorumlulukların belirlenmesini anlamayı kolaylaştırmaktadır.

Standardın kendisi önceki sürümden önemli ölçüde daha uzundur ve kontroller yeniden sıralanmış ve güncellenmiştir. Bazı kontroller birleştirilmiş veya kaldırılmış ve bazı yeni kontroller eklenmiştir.

Ek A'daki kontrolleri değiştirmenin yanı sıra, ISO 27001:2022'nin yönetim sisteminde birkaç küçük değişiklikle "*Annex- SL*" ile uyumu sağlanmıştır; değişen maddeler şunlardır:

- 4.2 İlgili tarafların iyileştirilmesi
- 4.3 Kapsamın İyileştirilmesi
- 6.1.3 Risk tedavisinin iyileştirilmesi
- 6.3'ün eklenmesi değişiklik yönetimi
- 8.1 Operasyonel planlamanın iyileştirilmesi
- 9.2'nin 9.2.1 Genel / 9.2.2 Denetim programı olarak bölünmesi
- 9.3'ün 9.3.1 Genel / 9.3.2 Girdi / 9.3.3 Çıktı olarak bölünmesi

ISO 27002:2022'DEKİ (EK A) DEĞİŞİKLİKLER :

Yeni Eklenen Ek A Kontrolleri

5.7 Tehdit istihbaratı
5.23 Bulut hizmetlerinin kullanımı için bilgi güvenliği
5.30 İş sürekliliği için Bilgi ve İletişim Teknolojileri hazırlığı
7.4 Fiziksel güvenlik izleme
8.9 Yapılandırma yönetimi
8.10 Bilgi silme
8.11 Veri maskeleme
8.12 Veri sızıntısı önleme
8.16 İzleme faaliyetleri
8.23 Web filtresi infaz
8.28 Güvenli kodlama

- Yeniden adlandırılan kontroller: Toplam 23 kontrolün, daha kolay anlaşılması için isimleri değiştirildi; ancak, özleri eski standartta olduğu gibi aynı kaldı.

6.2.2 Uzaktan çalışma	6.7 Uzaktan çalışma
9.2.1 Kullanıcı kaydı ve kaydının silinmesi	5.16 Kimlik yönetimi
9.2.3 Ayrıcalıklı erişim haklarının yönetimi	8.2 Ayrıcalıklı erişim hakları
9.4.2 Güvenli oturum açma prosedürleri	8.5 Güvenli kimlik doğrulama
9.4.5 Program kaynak koduna erişim kontrolü	8.4 Kaynak koduna erişim
7.3.1 İstihdam sorumluluklarının sona ermesi veya değiştirilmesi	6.5 İşin feshi veya değiştirilmesinden sonraki sorumluluklar
11.1.1 Fiziksel güvenlik çevresi	7.1 Fiziksel güvenlik çevreleri
11.2.6 Şirket dışındaki ekipman ve varlıkların güvenliği	7.9 Şirket dışındaki varlıkların güvenliği
11.2.9 Temiz masa temiz ekran politikası	7.7 Temiz masa temiz ekran
12.2.1 Kötü amaçlı yazılımlara karşı kontroller	8.7 Kötü amaçlı yazılımlara karşı koruma
12.7.1 Bilgi sistemleri denetim kontrolleri	8.34 Denetim testi sırasında bilgi sistemlerinin korunması
13.1.1 Ağ kontrolleri	8.20 Ağ güvenliği
13.1.3 Ağlarda ayrımcılık	8.22 Ağların ayrılması
14.2.1 Güvenli geliştirme politikası	8.25 Güvenli geliştirme yaşam döngüsü
14.2.5 Güvenli sistem mühendisliği ilkeleri	8.27 Güvenli sistem mimarisi ve mühendislik ilkeleri
14.3.1 Test verilerinin korunması	8.33 Test bilgileri
15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası	5.19 Tedarikçi ilişkilerinde bilgi güvenliği
15.1.2 Tedarikçi anlaşmalarında güvenliğin ele alınması	5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması
15.1.3 Bilgi ve iletişim teknolojisi tedarik zinciri	5.20 Tedarikçi anlaşmalarında bilgi güvenliğinin ele alınması
16.1.1 Sorumluluklar ve prosedürler	5.24 Bilgi güvenliği olay yönetimi planlaması ve hazırlanması
16.1.4 Bilgi güvenliği olaylarının değerlendirilmesi ve karara bağlanması	5.25 Bilgi güvenliği olaylarının değerlendirilmesi ve karara bağlanması
17.2.1 Bilgi işlem tesislerinin mevcudiyeti	8.14 Bilgi işlem tesislerinin yedekliliği
18.1.4 Kişisel olarak tanımlanabilir bilgilerin gizliliği ve korunması	5.34 Kişisel Bilgilerin Gizliliği ve Korunması

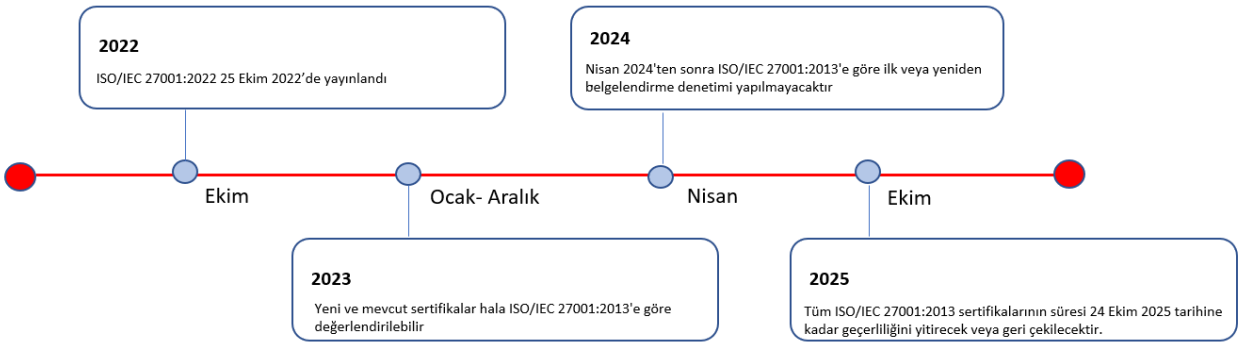
- Geri kalan kontrollerden 35 tanesi aynen korunmuş, 58 tanesi 24 adet yeni kontrol içinde birleştirilmiştir.
- Bu değişiklikler, süreçlerin ve faaliyetlerin bilgi güvenliği yönlerine odaklanmaya yardımcı olacak ve Bilgi Güvenliği Yönetim Sistemi'nin uygulanması ve sürdürülmesi için harcanan çabaları azaltacaktır.
- Kontrollerin kategorize edilmelerini kolaylaştırmak için beş tür "**öznitelik**" tanımlanmıştır:
  - Kontrol tipi (önleyici, tespit edici, düzeltici)
  - Bilgi güvenliği özellikleri (gizlilik, bütünlük, erişilebilirlik)
  - Siber güvenlik kavramları (tanımlama, koruma, algılama, yanıtlama, kurtarma)

- Operasyonel yetenekler (Yönetişim, Varlık yönetimi, Bilgi koruması, İnsan kaynakları güvenliği, Fiziksel güvenlik, Sistem ve ağ güvenliği, Uygulama güvenliği, Güvenli yapılandırma, Kimlik ve erişim yönetimi, Tehdit ve güvenlik açığı yönetimi, Süreklilik, Tedarikçi ilişkileri güvenliği, Yasal ve uyumluluk, Bilgi güvenliği olay yönetimi ve Bilgi güvenliği güvencesi.)
- Güvenlik alanları (yönetişim ve ekosistem, koruma, savunma, dayanıklılık)

- Bu özellikler, hangi kontrollerin işletmeyle ilgili kriterlere göre (yani, yalnızca bilgi güvenliği ile ilgili değil) uygulanabilir olduğunun belirlenmesini ve ISO 27002 kontrollerinin NIST Risk Yönetimi Çerçevesi gibi diğer benzer güvenlik çerçevelerine entegrasyonunu kolaylaştıracaktır.

BU DEĞİŞİKLİKLER, ZATEN ISO 27001:2013 SERTİFİKASINA SAHİP KURULUŞLARI NASIL ETKİLEYECEK ?

Uluslararası Akreditasyon Forumu (IAF), ISO 27001:2022'nin yayınlanmasından itibaren kuruluşların geçiş yapmak için 36 ayları olduğunu belirten bir belge yayınladı[3]. Buna dayanarak tahmini olarak geçiş süreci aşağıdaki gibi gerçekleşecek ve kuruluşların Ekim 2025'e kadar güncellenen Standarda uyması gerekecektir.



- 24 Ekim 2025'ten sonra tüm ISO 27001:2013 sertifikalarının geçerliliği sona erecektir. Bu nedenle Ekim 2025 tarihine kadar BGYS'nizin güncellenmesi ve sertifikanızın ISO 27001:2022'ye geçirilmesi gerekmektedir.

- Belgelendirme kuruluşunuzun bu süre içinde bir geçiş değerlendirmesi yapması ve size güncellenmiş bir sertifika vermesi gerekecektir.

- Geçiş değerlendirmesi, BGYS'nizi Ek A kontrollerindeki değişiklikler de dahil olmak üzere ISO 27001:2022'nin yeni gerekliliklerine göre güncelleyip güncellemediğinizi belirleyecektir.

- Gözetim denetimi yeniden belgelendirme denetimi veya bağımsız bir değerlendirmeyle geçiş yapabilirsiniz. Tipik olarak bu, ek denetim süresi gerektirecektir.

3 https://iaf.nu/iaf_system/uploads/documents/IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf

- Teknik olarak, ISO 27001'de önerilen değişiklik, daha uygun görürseniz, Ekim 2025'e kadar 2013 kontrol setini kullanmaya devam etmek için kapıyı açık bırakmaktadır. Bu durumda, Uygulanabilirlik Bildirgenizde bunu belirten yalnızca bir satır metin eklemek yeterli olacaktır.

- Bununla birlikte, çoğu kuruluş, paydaşların beklentilerine uygun olması için bir sonraki denetimlerinden önce uygulamalarını taşımayı seçecektir.

ISO / IEC 27001: 2022'YE NASIL HAZIRLANMALIYIZ ?

Geçiş için aşağıdaki temel etkinlikler dikkate alınmalıdır:

- BGYS operasyonuna katılanlar için eğitim programı oluşturmak
- ISO 27002:2022'deki 93 kontrol hakkında bilgi edinmek
- Kuruluşunuza uygulanan hangi kontrollerin etkilendiğini belirlemek
- Belgelerinizi geçiş için hazırlamak

Boşluk Analizi Yapın

Kuruluşlar, mevcut Bilgi Güvenliği Yönetim Sistemlerini ziyaret etme ve risk kayıtlarını ve risk değerlendirmelerini gözden geçirerek uygunluk ve uygulanabilirliklerini belirleme fırsatına sahiptir. ISO 27001 standardının 2013 sürümü ile 2022 sürümü arasında hiçbir kontrol silinmemiş olsa da yeni kontrollerin birleşmesi, güncellenmesi ve tanıtılması şu anda bunları nasıl yönettiğinizi etkiler.

Öznitelikleri Dikkate Alın

- ISO 27002:2022 standardında Özniteliklerin kullanıma sunulmasıyla, kuruluşlar öznitelikleri uygulamak için gözden geçirme sürecini kullanabilirler. Özniteliklerin yararı, farklı perspektiflerden veya temalardan görüldüğü gibi kontrollerin farklı görünümlerini veya kategorizasyonlarını oluşturabilmektir.
- Örneğin, kontrollerinizi kontrol türleri (önleyici, tespit edici veya düzeltici kontroller) açısından görüntüleyebilir veya bunu farklı güvenlik özelliklerine (gizlilik, bütünlük, kullanılabilirlik) veya farklı operasyonel yeteneklere (yönetim, kimlik ve erişim yönetimi, yasal ve uyumluluk vb.) dayalı olarak yapabilirsiniz.

Uygulanabilirlik Bildirgenizi (SOA) optimize edin

Bu gözden geçirmeyi gerçekleştirirken, kuruluşlar, yeniden adlandırılan kontrollerin yanı sıra birleştirilmiş ve yeni kontroller de dahil olmak üzere kontrollerin 2022 versiyonuna dayalı paralel bir Uygulanabilirlik Bildirgesi (Beyanı) oluşturmayı düşünmelidir. Bu, geçiş için planlanan zaman çizelgesinden kaynaklanmaktadır. Geçiş denetiminizden önce gerçekleştirilen denetimlerin yine de 2013 sürümüyle uyumlu olması ve dolayısıyla bu ilgili gereksinimlere atıfta bulunması gerekecektir.

Geçiş Kaynaklarını Göz Önünde Bulundurun

- ISO 27001:2022 gereklilikleri değişmemiş olsa da Ek A'da listelenen kontrollere yönelik güncelleme, kuruluşların bu güncellemeleri nasıl uygulayacaklarını düşünmelerini gerektirmektedir.
- BGYS iç denetçilerinizi eğitmek, neyin gerekli olduğunu ve kuruluşun herhangi bir boşluğu doldurmasına nasıl yardımcı olacaklarını anlamalarını sağlamak için bir zorunluluktur. Kuruluşların risk değerlendirmeleri ve tedavileri üzerindeki etkisinin belirlenmesi için kontrol sahiplerinin de eğitim programına dahil edilmesi gerekmektedir.
- Bir eğitim programına sahip olmak aynı zamanda değişiklik yönetimine yardımcı olur ve personelinize değişikliklere uyum sağlamaları için zaman ve fırsat verir.

Saygılarımızla.