UKS ULUSLARARASI
KALİTE SİSTEMLERİ VE
BELGELENDİRME
LTD. ŞTİ.

ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Geçiş Bilgilendirme Kılavuzu

ISO 27001:2022 GEÇİŞ SÜRESİ BİLGİLENDİRME

ISO/IEC 27001:2013 / TS EN ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi 25 Ekim 2022 tarihi itibariyle revize edilerek ISO/IEC 27001:2022 halini almıştır. IAF (Uluslararası Akreditasyon Forumu) tarafından geçiş süresi 3 (üç) yıl olarak belirlenmiştir.

UKS tarafından belgelendirilmiş tüm kuruluşlar mevcut yönetim sistemlerini yeni versiyona uyumlu hale getirmelerini takiben gerçekleştirilecek tetkiklerle geçişleri tamamlanacaktır. 31 Ekim 2025 tarihi itibariyle ISO/IEC 27001:2013 belgelerinin bir geçerliliği kalmayacaktır.

1 Kasım 2023'ten itibaren, UKS Belgelendirme tarafından ISO/IEC 27001:2013/ TS EN ISO/IEC 27001:2017'ye göre ilk belgelendirme tetkikleri veya yeniden belgelendirme tetkikleri gerçekleştirilemeyecektir.

DEĞİŞİKLİKLERE UYUM İÇİN MÜŞTERİLERDEN BEKLENEN ÇALIŞMALAR

1. Yeni Standart şartlarını karşılamak üzere Fark analizi yapılması
2. Gelişim planının hazırlanması
3. Sistemin etkin olarak organizasyonda uygulanabilmesi için tüm personelin farkındalığının yaratılması ve yeterli eğitimlerin tamamlanması
4. Yeni Standart doğrultusunda sistemin güncellenmesi ve etkinliğinin ölçülmesinin sağlanması
5. Uygulanabilirlik beyanının (SoA) güncellenmesi
6. Varsa Risk Tedavi Planının Güncellenmesi

Genel Farklılıklar Hakkında Özet

ISO 27001:2022’de, ISO 27001:2013'ün 114 kontrolü yerine 93 kontrol listelenecek.

Bu kontroller artık 14 maddede değil 4 ana başlık halinde gruplandırılacak:

-İnsanlar (8 kontrol)
-Organizasyonel (37 kontrol)
-Teknolojik (34 kontrol)
-Fiziksel (14 kontrol)

DEĞİŞİKLİK TABLOSU

Kontroller, kategorize edilmelerini kolaylaştırmak için artık beş tür özniteliğe sahip olacak:

-Kontrol tipi (önleyici, tespit edici, düzeltici)
-Bilgi güvenliği özellikleri (gizlilik, bütünlük, erişilebilirlik)
-Siber güvenlik kavramları (tanımlama, koruma, tespit etme, yanıt verme, kurtarma)
-Operasyonel yetenekler (yönetişim, varlık yönetimi, vb.)
-Güvenlik alanları (yönetişim ve ekosistem, koruma, savunma, dayanıklılık)

Ek-A' daki kontrollerin değişiminin yanı sıra ISO/IEC 27001:2022'nin yönetim sisteminde birkaç küçük değişik ile « Annex- SL» ile uyumu sağlanmıştır;

Değişen maddeler şunlardır

4.2 İlgili tarafların iyileştirilmesi

4.4 Bilgi Güvenliği Yönetim Sistemi

6.1.3 Bilgi Güvenliği Risk İşleme

6.2 Bilgi Güv. Amaçları ve bu amaçları başarmak için planlama

6.3 Değişikliklerin Planlanması (Yeni Madde)

7.4 İletişim

8.1 Operasyonel Planlama ve Kontrol

9.1 İzleme, ölçme, analiz ve değerlendirme

9.2 İç Tetkik (**9.2.1 ve 9.2.2** olarak bölünmesi)

9.3 Yönetimin Gözden Geçirmesi (9.3.1, 9.3.2, 9.3.3 olarak bölünmesi)

10.1 ve **10.2**' nin yapılandırılma sırasının Uyumlaştırılmış Yapıya uyarlanması

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	Konfügürasyon yönetimi
8.10	Bilgi Silme
8.11	Veri Maskeleme
8.12	Veri sızıntısını önleme
8.16	İzleme faaliyetleri
8.23	Web filtreleme
8.28	Güvenli Kodlama

Güncellenen Kontroller

Toplam 58 Kontrolün, güncellemesi gerçekleşmiştir.

* Tablo bir sonraki sayfada verilmiştir.

ISO / IEC 27001: 2022 kontrol tanımlayıcısı	ISO / IEC 27001: 2013 kontrol tanımlayıcısı	Kontrol Adı
5.2	6.1.1	Bilgi güvenliği rolleri ve sorumlulukları
5.3	6.1.2	Görevlerin ayrılması
5.4	7.2.1	Yönetim sorumlulukları
5.5	6.1.3	Yetkililerle iletişim
5.6	6.1.4	Özel İlgi grupları ile iletişim
5.11	8.1.4	Varlıkların İadesi
5.12	8.2.1	Bilginin sınıflandırılması
5.13	8.2.2	Bilgilerin etiketlenmesi
5.16	9.2.1	Kimlik yönetimi
5.19	15.1.1	Tedarikçi ilişkilerinde bilgi güvenliği
5.20	15.1.2	Tedarikçi sözleşmelerinde bilgi güvenliğinin ele alınması
5.21	15.1.3	Bilgi ve iletişim teknolojileri (BIT) tedarik zincirinde bilgi güvenliğinin yönetilmesi
5.24	16.1.1	Bilgi güvenliği olay yönetimi planlama ve hazırlama
5.25	16.1.4	Bilgi güvenliği olaylarının değerlendirilmesi ve karara bağlanması
5.26	16.1.5	Bilgi güvenliği olaylarına yanıt
5.27	16.1.6	Bilgi güvenliği olaylarından öğrenme
5.28	16.1.7	Kanıtların toplanması

ISO / IEC 27001: 2022 kontrol tanımlayıcısı	ISO / IEC 27001:2013 kontrol tanımlayıcısı	Kontrol Adı
5.32	18.1.2	Fikri mülkiyet hakları
5.33	18.1.3	Kayıtların korunması
5.34	18.1.4	Kişisel tanımlanabilir bilgilerin gizliliği ve korunması
5.35	18.2.1	Bilgi güvenliğinin bağımsız olarak gözden geçirilmesi
5.37	12.1.1	Belgelenmiş çalışma prosedürleri
6.1	7.1.1	Tarama
6.2	7.1.2	İstihdam şartları ve koşulları
6.3	7.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretim
6.4	7.2.3	Disiplin süreci
6.5	7.3.1	İstihdamın sona ermesi veya değiştirilmesinden sonraki sorumluluklar
6.6	13.2.4	Gizlilik veya ifşa etmeme anlaşmaları
6.7	6.2.2	Uzaktan çalışma
7.1	11.1.1	Fiziksel güvenlik sınırları
7.3	11.1.3	Ofislerin, odaların ve tesislerin güvenliğini sağlamak
7.5	11.1.4	Fiziksel ve çevresel tehditlere karşı koruma
7.6	11.1.5	Güvenli alanlarda çalışmak
7.7	11.2.9	Temiz masa ve temiz ekran
7.8	11.2.1	Ekipman yerleşimi ve koruması

ISO / IEC 27001:2022 kontrol tanımlayıcısı	ISO / IEC 27001:2013 kontrol tanımlayıcısı	Kontrol Adı
7.9	11.2.6	Tesis dışı varlıkların güvenliği
7.11	11.2.2	Yardımcı Programları Destekleme
7.12	11.2.3	Kablolama güvenliği
7.13	11.2.4	Ekipman bakımı
7.14	11.2.7	Ekipmanın güvenli bir şekilde imha edilmesi veya yeniden kullanılması
8.2	9.2.3	Ayrıcalıklı erişim hakları
8.3	9.4.1	Bilgi erişim kısıtlaması
8.4	9.4.5	Kaynak koduna erişim
8.5	9.4.2	Güvenli kimlik doğrulama
8.6	12.1.3	Kapasite yönetimi
8.7	12.2.1	Kötü amaçlı yazılımlara karşı koruma
8.13	12.3.1	Bilgi yedekleme
8.14	17.2.1	Bilgi işlem tesislerinin yedekliliği
8.17	12.4.4	Zaman senkronizasyonu
8.18	9.4.4	Ayrıcalıklı yardımcı programların kullanımı
8.20	13.1.1	Ağ güvenliği
8.21	13.1.2	Ağ hizmetlerinin güvenliği
8.22	13.1.3	Ağların ayrılması
8.25	14.2.1	Güvenli gelişim yaşam döngüsü
8.27	14.2.5	Güvenli sistem mimarisi ve mühendislik ilkeleri
8.30	14.2.7	Dış kaynaklı geliştirme
8.33	14.3.1	Test bilgileri
8.34	12.7.1	Denetim testleri sırasında bilgi sistemlerinin korunması

Birleştirilen Kontroller

Birleştirilen 24 kontrol bulunmaktadır.

* Tablo bir sonraki sayfada verilmiştir.

ISO / IEC 27001: 2022 kontrol tanımlayıcısı	ISO / IEC 27001: 2013 kontrol tanımlayıcısı	Kontrol Adı
5.1	5.1.1, 5.1.2	Bilgi güvenliği politikaları
5.8	6.1.5, 14.1.1	Proje yönetiminde bilgi güvenliği
5.9	8.1.1, 8.1.2	Bilgi Envanteri ve diğer ilişkili varlıklar
5.10	8.1.3, 8.2.3	Bilgilerin ve diğer ilişkili varlıkların kabul edilebilir kullanımı
5.14	13.2.1, 13.2.2, 13.2.3	Bilgi Transferi
5.15	9.1.1, 9.1.2	Erişim kontrolü
5.17	9.2.4, 9.3.1, 9.4.3	Kimlik doğrulama bilgileri
5.18	9.2.2, 9.2.5, 9.2.6	Erişim hakları
5.22	15.2.1, 15.2.2	Tedarikçi hizmetlerinin izlenmesi, gözden geçirilmesi ve değişim yönetimi
5.29	17.1.1, 17.1.2, 17.1.3	Kesinti sırasında bilgi güvenliği
5.31	18.1.1, 18.1.5	Yasal, düzenleyici ve sözleşmeden doğan gereklilikler
5.36	18.2.2, 18.2.3	Bilgi güvenliğine yönelik politika, kural ve standartlara uygunluk
6.8	16.1.2, 16.1.3	Bilgi güvenliği olay raporlaması
7.2	11.1.2, 11.1.6	Fiziksel giriş
7.10	8.3.1, 8.3.2, 8.3.3, 11.2.5	Depolama ortamı
8.1	6.2.1, 11.2.8	Kullanıcı uç nokta cihazları
8.8	12.6.1, 18.2.3	Teknik güvenlik açıklarının yönetimi
8.15	12.4.1, 12.4.2, 12.4.3	Log Kayıtları
8.19	12.5.1, 12.6.2	İşletim sistemlerine yazılım kurulumu
8.24	10.1.1, 10.1.2	Kriptografi kullanımı
8.26	14.1.2, 14.1.3	Uygulama güvenliği gereksinimleri
8.29	14.2.8, 14.2.9	Geliştirme ve kabul aşamasında güvenlik testi
8.31	12.1.4, 14.2.6	Geliştirme, test ve üretim ortamlarının ayrılması
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Değişim yönetimi

Bu kılavuz yeni revizyonun getirdiği yenilikler ve değişikliklerin anlaşılmasına yardımcı olmak için hazırlanmıştır. Kılavuz standardın tümünü içermemekle birlikte Bilgi Güveliği Yönetim Sisteminin kurulması için şart standardın ISO/IEC 27001:2022 standardı ve dikkate alınması gereken birincil kılavuzların standardın atıf yaptığı diğer standart / dokümanlar olduğu unutulmamalıdır.

ISO/IEC 27001:2022 bilgilendirme konularında talepleriniz için bize ulaşın…

UKS Uluslararası Kalite Sistemleri Ve Belgelendirme Ltd. Şti.
www.uksbelgelendirme.com.tr
Adres: Atakent Mah. Dicle Cad. No:35 Ümraniye/İSTANBUL
Tel: 0 216 330 45 77
Fax:0 216 330 67 47

Geçiş İle İlgili Ek Süre ve Tetkik Hesaplaması Bilgilendirmesi bu kılavuza ek olarak yayınlanan Ek-1 Yayınında bahsedilmiştir.