ISO/IEC 27001:2022 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ GEÇİŞ REHBERİ

A. AMAÇ:

Bu doküman ile BBS'den ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi standartlarından belgeli olan kuruluşlara ve aday kuruluşlara ISO/IEC 27001:2022 standardına geçiş konusunda rehberlik edilmesi amaçlanmaktadır.

B. KAPSAM:

Bu doküman BBS'nin ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 standardına göre belgelendirdiği kuruluşların ve aday kuruluşların ISO/IEC 27001:2022 standardına geçiş ve denetim süreçlerini kapsamaktadır.

C. UYGULAMA:

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardı 25.10.2022 tarihinde Bilgi Güvenliği, Siber Güvenlik ve Gizlilik Koruması – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler başlığı altında revizyona uğramıştır. Bu rehber, gerçekleşen revizyon bağlamında BBS tarafından belgelendirilecek ve mevcut ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 standardından ISO/IEC 27001:2022 standardına geçiş yapacak kuruluşlar için gerekli bilgilendirmeyi içermektedir. Bu bilgilendirme ile BBS kendi müşterilerinin geçiş sürecine ilişkin bilgisini artırmayı ve geçiş sürecini kolaylaştırmayı amaçlamaktadır.

C.1. Ekim 2022'de yayınlanan ISO/IEC 27001:2022 Standardında önemli değişiklikler olmuştur. ISO/IEC 27001:2022 Standardı; Standart ISO direktifi Ek SL'ye göre hazırlanmıştır. Uyumlaştırılmış Yapı olarak adlandırılan yapıya adaptasyonla birlikte, süreç oryantasyonuna yönelik gecikmiş gereklilik, etkin bir BGYS'nin odağına yerleştirilmiştir. Etkili yönetim sistemlerinin temeli, açık süreçler ve bunların etkileşimlerinin yanı sıra bu süreçlerin kontrolü için hedef odaklı kriterlerdir.

Revize edilen ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi standardındaki **temel değişlikler** şunlardır;

1. Madde 4.4; BGYS'nin uygulanması ve sürdürülmesi için **gerekli süreçlerin ve bunların** BGYS içindeki **etkileşimlerinin** tanımlanması gerekliliği açıkça ifade edilmiştir.
2. Madde 5.3; bilgi güvenliği ile ilgili rollere ilişkin sorumluluk ve yetkilerin kurum içinde bilinmesine yönelik açık bir gereklilikle desteklenmiştir.
3. Madde 6.3; Değişikliklerin Planlanması maddesi yeni standarda ilave edilmiştir.
4. Madde 7.4; BGYS ile ilgili iç ve dış iletişimin nasıl kurulacağı vurgulanmıştır.
5. Madde 8.1; Süreçlere ve kontrollere ilişkin kriterlere vurgu yapılmıştır.
6. Madde 9.2; İç Denetim ve Madde 9.3 Yönetimin Gözden Geçirmesi Uyumlaştırılmış Yapıya uyarlanmıştır. Madde 9.2; 9.2.1 ve 9.2.2 olarak, Madde 9.3 ise 9.3.1, 9.3.2 ve 9.3.3 olarak alt bölümlere ayrılmıştır.
7. Madde 10.1 ve Madde 10.2'nin yapılandırılma sırası Uyumlaştırılmış Yapıya uyarlanmıştır.

Ek A'daki kontrol setine atıfta bulunan ISO/IEC 27001'deki temel ve açık gereklilikler, Madde 6.1.3 c)'ye göre, kuruluşa özgü bilgi güvenliği kontrolleri ile Ek A'dakiler arasındaki karşılaştırma süreci ve Madde 6.1.3 d), Uygulanabilirlik Bildirgesinin hazırlanması gereksinimleri devam etmektedir.

ISO/IEC 27001:2022'nin normatif Ek A'sındaki olası bilgi güvenliği kontrollerinin listesi, ISO/IEC 27002:2022'den aynı şekilde türetilmiştir. ISO/IEC 27001:2022 standardının EK-A maddeleri 15 Şubat 2022'de yayınlanmış olan ISO/IEC 27002:2022 standardına uygun olarak revizyona uğramıştır.

Buna göre daha önce 14 madde halinde düzenlenmiş, 35 kontrol hedefi altında bilgi güvenliği risklerini ele almak için kullanılabilecek toplam 114 kontrol içermekte olan EK-A kısmı 2022 versiyonda aşağıda belirtilen 4 madde altında toplanmıştır;

- A.5 Organizasyonel kontroller (37 kontrol ile).
- A.6 Kişisel kontroller (8 kontrol ile)
- A.7 Fiziksel kontroller (14 kontrol ile)
- A.8 Teknik kontroller (34 kontrol ile)

Yeni ISO/IEC 27001:2022 standardının Ek A'sı artık toplam 93 kontrol içermektedir ve bunlardan aşağıdaki 11 kontrol yenidir:

- 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 Bilgilerin silinmesi
- A.8.11 Veri maskeleme
- A.8.12 Veri sızıntısının önlenmesi
- A.8.16 Faaliyet izleme
- A.8.23 Web filtreleme
- A.8.28 Güvenli kodlama

ISO/IEC 27001:2022'nin Ek A'sı kontrolleri adlandırmakla sınırlıyken, ISO/IEC 27002:2022uygulama kılavuzu bunları kategorize etmek için daha fazla seçenek sunar. Burada, her kontrole farklı görünümlere ve bakış açılarına izin veren beş öznitelik atanmıştır. Öznitelikler veya öznitelik değerleri, farklı kurumsal görünümler için filtreleme, sıralama veya görüntüleme amacıyla kullanılabilir.
Beş öznitelik şunlardır:

- **Kontrol türü**, bir önlemin bir bilgi güvenliği olayının meydana gelmesiyle ilgili riski ne zaman ve nasıl değiştirdiği perspektifinden kontrollerin görünümü için bir niteliktir.
- **Bilgi güvenliği özellikleri**, kontrolleri önlemin hangi koruma hedefini desteklemeyi amaçladığı perspektifinden görmeye yönelik bir niteliktir.
- **Siber güvenlik kavramları**, kontrollere ISO/IEC TS 27110'da açıklanan siber güvenlik çerçevesiyle nasıl eşleştikleri perspektifinden bakar.
- **Operasyonel yetenek**, kontrolleri operasyonel bilgi güvenliği yetenekleri perspektifinden değerlendirir ve önlemlerin pratik bir kullanıcı görünümünü destekler.
- **Güvenlik alanları**, kontrollerin dört bilgi güvenliği alanı perspektifinden görülmesini sağlayan bir niteliktir.

C.2. ISO/IEC 27001:2022 Sertifikalarının Geçerliliği ve Geçiş Süreci

ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 sertifikaları yeni standardın yayınlanmasından sonra 3 yıl içinde geçerliliğini kaybedecektir. Bu standartlardan belgeli olan kuruluşların **en geç 31 Ekim 2025'e kadar** geçişlerini tamamlamaları gerekmektedir. 2022 versiyonuna geçişinizi ilk belgelendirme denetiminde yapılabileceğiniz gibi gözetim ve yeniden belgelendirme tetkiklerinizde de sağlayabilirsiniz. Diğer yandan **31 Ekim 2023 tarihi sonrasında 2013 ve 2017 versiyonlardan ilk belgelendirme ve yeniden belgelendirme işlemleri yapılamayacaktır.** BBS olarak TÜRKAK geçiş sürecimizi TÜRKAK'ın duyurusunu yayınlaması itibariyle ilk akreditasyon denetimimizde tamamlamayı hedeflemekteyiz. Siz müşterilerimiz ve müşteri adaylarımızdan da beklentimiz etkin bir geçiş planı hazırlamanız ve yapacağınız plan sonrasında en uygun sürede geçiş çalışmalarınızı tamamlamanızdır.

C.3. BBS'nin Müşteri Kuruluşlarından Bekledikleri

BBS hali hazırda ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 belgesi bulunan kuruluşlarından ISO/IEC 27001:2022'e geçiş ile ilgili bazı hazırlıklar yapmasını beklemektedir. Bu geçiş süreci içinde kuruluşların kesintisiz ve eksiksiz olarak belgelerini güncelleyip devam ettirmeleri için bazı düzenlemeleri yapması etkili ve iyi bir uygulama olacaktır. Bunun için belgeli kuruluşların ISO/IEC 27001:2022'e bir geçiş planı ile geçişlerini planlamaları gerekmektedir.

Bu geçiş planında şu adımların belirtilmesi tavsiye edilmektedir;

1. Yeni şartların karşılanması için kuruluş içindeki farklılıkların belirlenmesi,
2. Uygulama planının geliştirilmesi,
3. Kuruluşun etkililiği için ilgili tarafların tümünün bilinçlendirilmesi ve eğitim çalışmalarının tamamlanması,
4. Revize edilen şartların karşılanması için Bilgi Güvenliği Yönetim Sisteminin güncellenmesi ve etkililiğinin doğrulanması,
5. Geçiş ile ilgili çalışmaların BBS ile paylaşılması.

C.4. ISO/IEC 27001:2022 Standardı Geçişi ile İlgili İzlenecek Prosedür

BBS olarak ISO/IEC 27001:2022 BGYS geçişi ile ilgili olarak yapmanız gerekenler aşağıda maddeler halinde belirtmiştir. Olası her türlü sonuca karşı en geniş kapsamda hazırlanan bu kısa kılavuz siz BBS ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Belgeli müşterilerimiz/müşteri adaylarımız için tüm belirsizlikleri ortadan kaldıracak düzeyde hazırlanmıştır.

ISO/IEC 27001:2022 Geçiş Süreci Aşamaları;

1. ISO/IEC 27001:2022 Geçiş Planının siz müşterilerimiz tarafından planlanması ve BBS ile net olarak paylaşılması (Geçiş sürecinin gözetim veya yeniden belgelendirme tetkiki ile birlikte mi olacağı ya da ekstra bir geçiş tetkiki mi talep edildiği),
2. BBS tarafından hazırlanan ekte verilen PLN.BGYS.01 - ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Geçiş Planının doldurulup Belgelendirme Hizmet Sorumlularımız ile paylaşılması,
3. BBS Belgelendirme personeli ile görüşülerek geçişin tamamlanmasının istenildiği tarihin belirlenmesi,
4. Geçiş planındaki adımların uygulanılması ve geçiş çalışmalarının tamamlanması,
5. Geçiş, Gözetim tetkiki veya Yeniden Belgelendirme tetkikinin önceden belirlenen tarihte gerçekleştirilmesi,
6. Uygunsuzlukları kapatmak için verilen süre içinde uygunsuzlukların kapatılması,
7. BBS tarafından olumlu sonuçlanan geçiş sonucu sertifikanızın tarafınıza ulaştırılmasıdır.

Kuruluşunuzun talebi ile geçiş tetkikinin gözetim tetkiki ile aynı anda yapılması durumunda kuruluşunuz, ISO/IEC 27001:2022 geçişi için yeter seviyede uygunluk gösterememişse bir sonraki gözetim tetkiki esnasında geçişini yapabilir. Eğer bir sonraki gözetim tetkik tarihinin 31 Ekim 2025'den sonra olması durumunda; kuruluşunuzun ilgili tetkikinin 31 Ekim 2025 tarihinden önce sonuçlanacak şekilde yapılması planlanacaktır. Kuruluş 31 Ekim 2025'den önce bu tetkikin yapılmasını kabul etmezse 31 Ekim 2025 tarihinde ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 standardı yürürlükten kalkacağı için kuruluşun ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 belgesi otomatik olarak iptal edilecektir. Bu durum geçiş denetiminin ekstra bir denetimle planlanması durumunda da geçerlidir. Geçiş denetiminin 31 Ekim 2025 tarihinden önce sonuçlanmış olması gerekmektedir. 31 Ekim 2025 tarihine kadar yeni versiyona geçişi gerçekleştirmeyen kuruluşlar için bu tarihten sonra ilk belgelendirme süreci uygulanacaktır.

Geçiş denetimlerinde uygulanacak denetim süreleri, tarafınızdan gönderilecek PLN.BGYS.01 ISO/IEC 27001:2022 Bilgi Güvenliği Yönetim Sistemi Geçiş Planının tarafımızca incelenmesi sonucu kuruluşunuza bildirilecektir. ISO/IEC 27001:2013 ve ISO/IEC 27001:2017 belgesine sahip kuruluşlarımızın belgelerinin devamı ve istenmeyen durumlarla karşılaşmamaları için gerekli çalışmaları yapmaya başlamalarını önemle tavsiye ederiz.
Saygılarımızla…
BBS BELGELENDİRME EĞİTİM VE GÖZETİM HİZMETLERİ A.Ş.

Hazırlayan (BGYS Sor.)	Gözden Geçiren (BM)	Onaylayan (GM)
Yunus YILMAZ TARİH: 01.12.2022	Aydın DEMİR TARİH: 01.12.2022	Yusuf YILMAZ TARİH: 01.12.2022