ISO/IEC 27001:2022 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ İÇİN DENETİM VE DOKÜMANTASYON BEKLENTİLERİ

Bu doküman, ISO/IEC 27001:2022 ve ISO/IEC 27001:2022/Amd 1:2024 kapsamında BGYS belgelendirme, gözetim, yeniden belgelendirme ve uygulanabilir ise geçiş denetimleri öncesinde kuruluşlardan beklenen asgari dokümante bilgi ve uygulama kanıtlarını açıklamak amacıyla hazırlanmıştır.

1. Denetim Öncesi Asgari Hazırlık Beklentileri

- BGYS, kuruluşun kapsamı içerisinde kurulmuş, uygulanıyor, sürdürülüyor ve sürekli iyileştiriliyor olmalıdır. ISO/IEC 27001:2022 madde 4-10 gereklilikleri, uygunluk iddiası bulunan kuruluşlar için hariç tutulamaz.
- Bilgi güvenliği politika ve hedefleri belirlenmiş, ilgili seviyelerde duyurulmuş, ölçülebilir/izlenebilir hale getirilmiş ve sonuçları değerlendirilebilir olmalıdır.
- Standardın madde 4-10 gereklilikleri ile Uygulanabilirlik Bildirgesi kapsamında seçilen Ek A kontrollerini kapsayan en az bir tam iç tetkik çevrimi tamamlanmış ve kayıt altına alınmış olmalıdır.
- BGYS'nin uygunluğu, yeterliliği ve etkinliğinin değerlendirildiği en az bir yönetim gözden geçirme faaliyeti tamamlanmış ve karar/aksiyon kayıtları oluşturulmuş olmalıdır.
- Risk değerlendirme yöntemi, risk kabul kriterleri, risk değerlendirme sonuçları, risk işleme planı, artık risk onayları ve Uygulanabilirlik Bildirgesi güncel ve birbirleriyle tutarlı olmalıdır.
- İlk belgelendirme denetimleri için, standardın gerektirdiği kayıtlar ile işletim/izleme kanıtlarının denetim tarihinden önce tercihen en az 3 aylık uygulanmış geçmişi ibraz edilebilir olmalıdır. Kapsam ve faaliyet yapısı gereği daha uzun dönemli kanıt gerekebilir.
- Dış kaynaklı prosesler, tedarikçi hizmetleri, bulut hizmetleri ve ilgili bilgi güvenliği kontrolleri kapsam içinde değerlendirilmeli; ilgili sözleşme, SLA, güvenlik şartları ve performans izleme kayıtları hazır bulundurulmalıdır.
- Kurumun 2013 versiyonu referanslı eski BGYS dokümanları bulunuyorsa, ISO/IEC 27001:2022 Ek A yapısına göre boşluk analizi, güncel SoA, güncel risk işleme planı ve yeni/değişen kontrollerin uygulama/etkinlik kanıtları hazır bulundurulmalıdır.

Bu beklentilerden herhangi biri denetim tarihi itibarıyla karşılanamıyorsa, denetim planlamasından önce YBM ile irtibat kurulmalıdır.

2. Standart ve Geçişe İlişkin Güncel Notlar

Konu	Güncel beklenti / açıklama
ISO/IEC 27001:2022	ISO/IEC 27001:2013'ün yerini alan 3. baskıdır. Madde 4-10 yönetim sistemi gereklilikleri ile Ek A bilgi güvenliği kontrolleri referans seti birlikte dikkate alınmalıdır.
Ek A kontrol yapısı	2013 versiyonundaki 14 alanda 114 kontrol yerine, 2022 yapısında 4 tema altında 93 kontrol yer almaktadır: Organizasyonel, İnsan, Fiziksel ve Teknolojik kontroller.
SoA ve risk ilişkisi	SoA yalnızca bir kontrol listesi değildir; kuruluşun gerekli kontrolleri, dahil etme gerekçelerini, uygulama durumunu ve hariç tutulan Ek A kontrolleri için gerekçeleri göstermelidir.
Amd 1:2024 iklim değişikliği	Kuruluş, madde 4.1 kapsamında iklim değişikliğinin BGYS için ilgili bir konu olup olmadığını belirlemeli; madde 4.2 kapsamında ilgili tarafların iklim değişikliği ile ilişkili gereklilikleri olabileceğini dikkate almalıdır.
ISO/IEC 27006-1:2024	BGYS denetim ve belgelendirme kuruluşları için ISO/IEC 17021-1'e ek gereklilikleri belirtir; bu nedenle denetim kapsamı, denetim süresi, yetkinlik ve denetim kanıtı beklentileri belgelendirme programına göre doğrulanır.

3. Madde Bazlı Dokümante Bilgi ve Kanıt Beklentileri

Madde	Başlık	Beklenen dokümante bilgi / kanıt
4.1	Kuruluşun bağlamı	İç/dış hususlar listesi; bilgi güvenliği hedeflenen çıktılarına etkiler; iklim değişikliğinin BGYS açısından ilgili olup olmadığının değerlendirilmesi.
4.2	İlgili taraflar	İlgili taraflar ve bilgi güvenliği gereklilikleri; yasal, düzenleyici, sözleşmesel şartlar; uygun ise iklim değişikliği bağlantılı beklentiler.
4.3	BGYS kapsamı	Kapsam dokümanı; sınırlar, lokasyonlar, ürün/hizmetler, prosesler, arayüzler, bağımlılıklar, dış kaynaklı faaliyetler.
4.4	BGYS süreçleri	BGYS süreçleri ve etkileşimleri; süreç sorumluları; proses kriterleri; uygulama ve iyileştirme kayıtları.
5.1-5.3	Liderlik, politika, roller	BGYS politikası; üst yönetim taahhüdü; görev, yetki ve sorumluluklar; raporlama ve karar mekanizması.
6.1.1	Risk ve fırsatlar	BGYS'nin hedeflenen çıktılarını etkileyen risk/fırsatlar; aksiyon planları; etkinlik değerlendirme yöntemi.
6.1.2	Bilgi güvenliği risk değerlendirme	Risk değerlendirme yöntemi; risk kabul kriterleri; varlık/bilgi kapsamı; gizlilik-bütünlük-erişilebilirlik etkileri; risk sahipleri; risk analiz ve değerlendirme sonuçları.
6.1.3	Risk işleme ve SoA	Risk işleme seçenekleri; gerekli kontroller; Ek A ile karşılaştırma; SoA; risk işleme planı; risk sahiplerinin artık risk onayı.
6.2	Bilgi güvenliği hedefleri	Ölçülebilir hedefler; sorumlular; kaynaklar; terminler; izleme ve sonuç değerlendirme kayıtları.
6.3	Değişikliklerin planlanması	BGYS değişiklikleri için planlı uygulama yaklaşımı; etki/risk değerlendirmesi; sorumlu ve onay kayıtları.
7.1-7.5	Destek	Kaynak planı; yetkinlik ve eğitim kayıtları; farkındalık kanıtları; iletişim planı; dokümante bilginin oluşturulması,

		güncellenmesi, erişimi, saklanması, revizyon ve imha kontrolü.
8.1	Operasyonel planlama ve kontrol	BGYS operasyon kriterleri; proses kontrol kayıtları; planlı/plansız değişikliklerin kontrolü; dış kaynaklı proseslerin kontrolü.
8.2	Risk değerlendirme tekrarı	Planlı aralıklarla ve önemli değişikliklerde yapılan güncel risk değerlendirme sonuçları.
8.3	Risk işleme uygulaması	Risk işleme planının uygulanması; kontrol uygulama kanıtları; kapanış ve etkinlik değerlendirme kayıtları.
9.1	İzleme, ölçme, analiz ve değerlendirme	Ne, nasıl, ne zaman ve kim tarafından izlenecek/ölçülecek; ölçüm sonuçları; BGYS performansı ve etkinlik değerlendirmesi.
9.2	İç tetkik	İç tetkik programı; kriter ve kapsam; tarafsız tetkikçi atamaları; raporlar; bulgu ve aksiyon kayıtları.
9.3	Yönetim gözden geçirme	Önceki YGG aksiyonları, bağlam/ilgili taraf değişiklikleri, performans geri bildirimi, uygunsuzluklar, ölçüm sonuçları, tetkik sonuçları, hedef gerçekleşmeleri, ilgili taraf geri bildirimleri, risk değerlendirme ve risk işleme durumu, iyileştirme fırsatları; karar ve değişiklik ihtiyaçları.
10.1-10.2	İyileştirme ve düzeltici faaliyet	Sürekli iyileştirme kayıtları; uygunsuzluk tanımı; düzeltme; sonuçlarla ilgilenme; kök neden; benzer uygunsuzluk analizi; aksiyonlar; etkinlik doğrulaması; gerekli BGYS değişiklikleri.

4. Uygulanabilirlik Bildirgesi (SoA) İçin Beklenen İçerik

- Kuruluş tarafından gerekli görülen tüm bilgi güvenliği kontrolleri açıkça listelenmelidir; kontroller yalnızca ISO/IEC 27001 Ek A'dan değil, kuruluşun risk ve gerekliliklerine göre başka kaynaklardan da seçilebilir.
- Ek A kontrolleriyle karşılaştırma yapılmalı ve gerekli herhangi bir kontrolün gözden kaçırılmadığı doğrulanmalıdır.
- Her kontrol için dahil etme gerekçesi, uygulama durumu, uygulanmayan kontroller için plan/termin ve hariç tutulan Ek A kontrolleri için gerekçe bulunmalıdır.
- SoA; risk değerlendirme sonuçları, risk işleme planı, yasal/sözleşmesel şartlar, tedarikçi/bulut gereklilikleri ve kontrol uygulama kanıtları ile tutarlı olmalıdır.
- SoA güncelliği; kapsam değişikliği, varlık/proses değişikliği, önemli teknoloji değişikliği, olay, tedarikçi değişikliği, risk değerlendirme güncellemesi ve iç/dış tetkik bulguları sonrasında gözden geçirilmelidir.

5. ISO/IEC 27001:2022 Ek A Kontrol Temaları İçin Örnek Kanıtlar

Ek A	Denetimde beklenebilecek doküman ve uygulama kanıtları
5 Organizasyonel kontroller	Bilgi güvenliği politikaları; roller ve sorumluluklar; görevlerin ayrılığı; otoriteler ve uzman gruplarla iletişim; tehdit istihbaratı; projelerde bilgi güvenliği; bilgi ve ilişkili varlık envanteri; kabul edilebilir kullanım; varlıkların iadesi; sınıflandırma/etiketleme/bilgi transferi; erişim kontrol kuralları; kimlik, kimlik doğrulama ve erişim hakları; tedarikçi, ICT tedarik zinciri ve bulut hizmetleri yönetimi; olay yönetimi; kesinti sırasında bilgi güvenliği ve ICT sürekliliği; yasal/sözleşmesel gereklilikler; fikri mülkiyet, kayıtlar ve kişisel veri; bağımsız gözden geçirme; uyum; dokümante işletim prosedürleri.
6 İnsan kontrolleri	İşe alım öncesi kontroller; işe alım şartları; bilgi güvenliği farkındalık/eğitimleri; disiplin süreci; işten ayrılma/görev değişikliği sonrası sorumluluklar; gizlilik taahhütleri; uzaktan çalışma güvenliği; bilgi güvenliği olay bildirim mekanizması.
7 Fiziksel kontroller	Fiziksel güvenlik sınırları; fiziksel giriş kontrolleri; ofis/oda/tesis güvenliği; fiziksel güvenlik izleme; dış ve çevresel tehditlere karşı koruma; güvenli alanlarda çalışma; temiz masa/temiz ekran; ekipman yerleşimi ve koruma; tesis dışı varlıklar; depolama ortamları; destekleyici altyapı hizmetleri; kablo güvenliği; ekipman bakımı; ekipmanın güvenli imhası veya yeniden kullanımı.
8 Teknolojik kontroller	Kullanıcı uç nokta cihazları; ayrıcalıklı erişim hakları; bilgi erişim kısıtlaması; kaynak koduna erişim; güvenli kimlik doğrulama; kapasite yönetimi; zararlı yazılıma karşı koruma; teknik açıklık yönetimi; konfigürasyon yönetimi; bilgi silme; veri maskeleme; veri sızıntısı önleme; yedekleme; bilgi işleme tesislerinin yedekliliği; kayıt tutma; izleme faaliyetleri; saat senkronizasyonu; ayrıcalıklı yardımcı programlar; yazılım kurulumu; ağ güvenliği; ağ hizmetleri güvenliği; web filtreleme; kriptografi; güvenli geliştirme yaşam döngüsü; uygulama güvenliği; güvenli sistem mimarisi ve mühendislik; güvenli kodlama; güvenlik testleri; dış kaynaklı geliştirme; geliştirme/test/üretim ortamlarının ayrılması; değişiklik yönetimi; test bilgileri; tetkik testlerinde bilgi sistemlerinin korunması.

6. Kuruluşlarda Bulunması Tavsiye Edilen Temel BGYS Dokümanları

Doküman grubu	Örnek doküman/kayıtlar
Yönetim sistemi dokümanları	BGYS El Kitabı veya süreç tanımları; dokümante bilgi kontrol prosedürü; kapsam; politika; hedef takip formu; iç tetkik prosedürü/programı; YGG prosedürü/gündemi; düzeltici faaliyet prosedürü; yasal ve sözleşmesel şartlar listesi.
Risk ve kontrol dokümanları	Risk değerlendirme metodolojisi; risk envanteri; risk işleme planı; SoA; artık risk onayları; kontrol etkinlik ölçüm planı; izleme ve ölçüm sonuçları.
Varlık ve erişim yönetimi	Bilgi ve ilişkili varlık envanteri; varlık sahipliği; kabul edilebilir kullanım kuralları; erişim kontrol politikası; kullanıcı yetkilendirme ve periyodik erişim gözden geçirme kayıtları; ayrıcalıklı erişim kayıtları.
Tedarikçi ve bulut	Tedarikçi değerlendirme formu; bilgi güvenliği şartları; SLA/sözleşme ekleri; bulut hizmeti kullanım, yönetim ve çıkış kriterleri; tedarikçi performans ve değişiklik izleme kayıtları.
Olay, süreklilik ve teknik operasyon	Olay yönetimi prosedürü; olay kayıtları ve kök neden/öğrenilen dersler; iş sürekliliği ve ICT sürekliliği planları; yedekleme ve geri dönüş test kayıtları; zafiyet, konfigürasyon, değişiklik, loglama, izleme ve kapasite yönetimi kayıtları.
İnsan ve fiziksel güvenlik	Görev tanımları; eğitim/farkındalık kayıtları; gizlilik taahhütleri; uzaktan çalışma kuralları; fiziksel erişim kayıtları; ziyaretçi kayıtları; temiz masa/temiz ekran kontrolleri; ekipman bakım/imha kayıtları.

7. Uygunsuzlukların Sınıflandırılması

Uygunsuzluklar genel olarak majör ve minör olarak sınıflandırılır. Sınıflandırma; gerekliliğin niteliği, sistematiklik düzeyi, bilgi güvenliği riskine etkisi, benzer uygunsuzlukların yaygınlığı ve kuruluşun kontrol etkinliğine göre yapılır.

Sınıf	Açıklama
Minör uygunsuzluk	Yönetim sisteminin genel yapısını çökertmeyen, sistematik olmayan veya sınırlı bir alanda görülen; önemli bilgi güvenliği riski ya da kontrol zafiyeti oluşturmayan kısmi sapmalar.
Majör uygunsuzluk	Bir ISO/IEC 27001 gerekliliğinin veya önemli bir BGYS prosesinin kurulmamış/uygulanmamış olması; aynı gerekliliğe ilişkin sistematik minör uygunsuzluklar; önemli bilgi güvenliği riski doğuran durumlar; veri kaybı, yetkisiz erişim/sızıntı, yasal/sözleşmesel uyumsuzluk veya kritik kontrol eksikliği riski oluşturan bulgular.

8. Uygunsuzluklara Cevap ve Düzeltici Faaliyet Beklentisi

- Kuruluş, tespit edilen uygunsuzluklar için kendi düzeltici faaliyet sistemini kullanmalı; YBM uygunsuzluk numarasına referans vermeli ve belirlenen süreler içinde cevap sunmalıdır.
- Cevap; uygunsuzluğun kontrol altına alınması ve düzeltilmesi, sonuçların ele alınması, kök nedenin belirlenmesi, benzer uygunsuzlukların var olup olmadığının değerlendirilmesi, gerekli aksiyonların uygulanması ve etkinlik doğrulamasını içermelidir.
- Kök neden, yönetimin kontrol edebileceği gerçek sistem/proses nedenini göstermelidir. “Personel hatası”, “eğitim eksikliği”, “standart bilinmiyordu” veya “tek seferlik durum” gibi yüzeysel ifadeler tek başına yeterli kabul edilmez.
- Uygulama kanıtı sunulmayan düzeltici faaliyetler genel olarak kabul edilmez. Uygulama için süre gerektiren faaliyetlerde hedef tarih, geçici kontrol ve gerekçe belirtilmelidir.
- Düzeltici faaliyetler yalnızca mevcut hatanın giderilmesine değil, tekrarın ve başka yerde oluşmasının önlenmesine odaklanmalıdır.

9. Geçiş / Güncelleme Denetimleri İçin Ek Beklentiler (Uygulanabilir ise)

- ISO/IEC 27001:2013 referanslı belge veya doküman yapısından ISO/IEC 27001:2022’ye geçiş söz konusu ise kuruluş, ISO/IEC 27001:2022 boşluk analizini tamamlamış olmalıdır.
- SoA, ISO/IEC 27001:2022 Ek A kontrol yapısı ve kuruluşun kendi risk gerekliliklerine göre güncellenmiş olmalıdır.
- Risk işleme planı, yeni/değiştirilmiş kontroller ve artık risk onayları ile uyumlu şekilde güncellenmiş olmalıdır.
- Yeni veya değiştirilmiş kontrollerin uygulanması ve etkinliği, yalnızca doküman incelemesiyle değil, uygun uygulama kanıtlarıyla doğrulanabilir olmalıdır.
- Geçiş denetimi; gözetim, yeniden belgelendirme veya ayrı denetim ile birlikte yürütülebilir. Geçiş hedeflerine ulaşılıp ulaşılmadığı denetim sonucuna göre belgelendirme kararında değerlendirilir.

10. Kaynaklar

- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, Edition 3, 2022-10.
- ISO/IEC 27001:2022/Amd 1:2024, Amendment 1: Climate action changes, 2024-02.
- ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, Edition 3, 2022-02.
- IAF MD 26:2022, Transition Requirements for ISO/IEC 27001:2022.
- ISO/IEC 27006-1:2024, Requirements for bodies providing audit and certification of information security management systems — Part 1: General.
- YBM D-38 Denetim ve Dokümantasyon Beklentileri (BGYS), Revizyon 0, 29.08.2015.

11. Revizyon Bilgisi

Revizyon	Tarih	Açıklama
0	29.08.2015	İlk yayın.
1	04.05.2026	ISO/IEC 27001:2022, ISO/IEC 27001:2022/Amd 1:2024, ISO/IEC 27002:2022 Ek A kontrol yapısı ve IAF MD 26:2022 geçiş beklentileri dikkate alınarak güncellendi. Eski Ek A madde referansları 2022 yapısına göre revize edildi.

Not: Bu doküman, denetim öncesi bilgilendirme ve hazırlık rehberi niteliğindedir. Standardın ve akreditasyon/program kurallarının güncel baskıları ile belgelendirme kuruluşu kararları esas alınır.