ISO 27000 VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ: STANDARTLAR VE UYGULAMALAR

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@solutionhome.net
Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Anahtar Kelimeler: *ISO 27001 • BGYS • Bilgi Güvenliği • Risk Yönetimi • Ek-A Kontrolleri • PDCA • Belgelendirme*

burakolgun.com

ÖZET

Bilgi, günümüz dijital ekonomisinin en değerli varlığı olarak öne çıkmakta; siber tehditler ve veri ihlallerinin hızla artması, kuruluşları bilgi güvenliğini stratejik bir yönetim meselesi olarak ele almaya zorlamaktadır. Bu bağlamda ISO/IEC 27000 standartlar ailesi ve bu ailenin sertifikalandırılabilir çekirdeği olan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), dünya genelinde bilgi güvenliği yönetiminin ortak dili haline gelmiştir. Bu derleme makale; ISO 27000 standartlar ailesini, ISO/IEC 27001:2022 revizyonunun getirdiği yapısal değişiklikleri, PDCA döngüsü temelli BGYS mimarisini, 93 kontrolü kapsayan Ek-A yapısını, risk yönetimi metodolojisini, zorunlu dokümantasyon gerekliliklerini, belgelendirme sürecini, ISO 27001'in Türk mevzuatıyla entegrasyonunu, Türkiye'deki uygulama örneklerini, küresel sertifika büyüme trendlerini ve 2025 geçiş zorunluluğunu kapsamlı biçimde ele almaktadır. ISO Survey 2024 verilerine göre dünya genelinde 96.709 geçerli sertifikaya ulaşan standart, 2018'den bu yana yüzde yüzü aşan bir büyüme kaydetmiştir. Bu büyüme, bilgi güvenliğinin kurumsal öncelikler arasındaki kalıcı yerini somutlaştırmaktadır.

Anahtar Kelimeler: *ISO 27001, ISO 27002, BGYS, bilgi güvenliği yönetim sistemi, PDCA döngüsü, Ek-A kontrolleri, risk yönetimi, uygulanabilirlik bildirgesi, SoA, varlık envanteri, belgelendirme, TSE, TÜRKAK, KVKK, siber güvenlik*

ABSTRACT

Information has emerged as the most valuable asset in today's digital economy, and the rapid increase in cyber threats and data breaches is compelling organizations to treat information security as a strategic management issue. In

this context, the ISO/IEC 27000 family of standards and its certifiable core, ISO/IEC 27001 Information Security Management System (ISMS), have become the common language of information security management worldwide. This review article comprehensively addresses the ISO 27000 standards family, structural changes brought by the ISO/IEC 27001:2022 revision, PDCA cycle-based ISMS architecture, the Annex A structure covering 93 controls, risk management methodology, mandatory documentation requirements, certification process, integration of ISO 27001 with Turkish legislation, implementation examples in Turkey, global certification growth trends and the 2025 transition requirement. According to ISO Survey 2024 data, the standard has reached 96,709 valid certificates worldwide, achieving growth of over 100% since 2018.

Keywords: *ISO 27001, ISO 27002, ISMS, information security management system, PDCA cycle, Annex A controls, risk management, statement of applicability, SoA, asset inventory, certification, TSE, TÜRKAK, KVKK, cybersecurity*

1. Giriş

Bilgi güvenliği, 21. yüzyılın en kritik kurumsal yönetim meselelerinden biri haline gelmiştir. IBM'in 2024 tarihli Veri İhlali Maliyeti Raporu, küresel ortalama veri ihlali maliyetinin 4,88 milyon dolara ulaştığını, son dört yılın en yüksek değeri olduğunu ve 2020'ye kıyasla yüzde onluk bir artışı temsil ettiğini ortaya koymaktadır. Sağlık sektöründe bu rakam, on dördüncü yıl üst üste en yüksek sektörel değeri koruyarak 9,77 milyon dolara ulaşmıştır. Bu veriler, bilgi güvenliğinin artık yalnızca bir BT meselesi değil; kurumsal yönetim, hukuki uyumluluk ve iş sürekliliği açısından stratejik öneme sahip bir yönetim disiplini olduğunu tartışmasız biçimde ortaya koymaktadır.

Bu bağlamda ISO/IEC 27001, bilgi güvenliği yönetimini sistematik, risk temelli ve sürekli iyileştirme felsefesiyle ele alan uluslararası standart olarak öne çıkmaktadır. ISO'nun (ISO, 2022) tanımına göre standart, 'herhangi bir büyüklük ve sektördeki şirketlere, sahip oldukları ya da işledikleri verilere ilişkin risklerle başa çıkmak için sistemler kurma konusunda rehberlik etmektedir.' ISO Survey 2024 verilerine göre, standart 2024 yılında bir önceki yıla kıyasla yaklaşık iki katına çıkarak 96.709 geçerli sertifikaya ulaşmış; 179.877 sertifikalı alan sayısına erişilmiştir (HEIC, 2025).

Türkiye'de ise kamu kurumları, finans sektörü ve telekomünikasyon şirketleri başta olmak üzere geniş bir kuruluş yelpazesi ISO/IEC 27001 sertifikasyonuna yönelmektedir. TSE, TS EN ISO/IEC 27001:2023 kapsamında belgelendirme ve eğitim faaliyetlerini sürdürmekte; Cumhurbaşkanlığı Dijital Dönüşüm Ofisi bünyesinde yayımlanan Bilgi ve İletişim Güvenliği Rehberi ile ISO 27001 kontrolleri arasında 2024 yılında eşleştirme tablosu hazırlanmıştır (Denetci.org, 2025).

Bu makalenin amacı, ISO 27000 standartlar ailesini ve BGYS uygulamalarını hem teknik hem de yönetimsel boyutlarıyla kapsamlı biçimde ortaya koymaktır. Makale; standart ailesinin yapısı, 2022 revizyonu, BGYS mimarisi, risk yönetimi, Ek-A kontrolleri,

burakoguz.com

belgelendirme süreci, Türkiye'deki yasal çerçeve ve uygulama örnekleri başlıklarında yapılandırılmıştır.

2. ISO 27000 Standartlar Ailesi

2.1 Ailenin Yapısı ve Mantığı

ISO/IEC 27000 serisi, bilgi güvenliği yönetimine ilişkin standartları kapsayan geniş bir standartlar ailesidir. ISO 27000'deki her bir aile üyesinin odaklandığı spesifik bir konu bulunmaktadır: Ailenin büyük resmi sunan çekirdeği ISO 27001 iken, bu konuları uygulamak için diğer aile üyelerine başvurulur (Yüksektepeli, 2013). Bu yapı, modüler ve ölçeklenebilir bir bilgi güvenliği yönetimi altyapısı kurulmasına olanak tanımaktadır.

Ailenin temel mantığı şöyledir: ISO 27001 'ne yapılması gerektiğini' tanımlarken ISO 27002 'nasıl yapılacağını' açıklamaktadır (Secureframe, 2025). ISO 27001 sertifikalandırılabilir bir standart olmasına karşın ISO 27002, kurumların performansını artırmak için uyguladıkları bir kılavuz niteliği taşımakta ve sertifikalandırılamamaktadır. Diğer aile üyeleri ise bu çekirdeği sektörel ya da konu bazlı derinleştiren tamamlayıcı belgeler olarak konumlanmaktadır.

Tablo 1. *ISO/IEC 27000 Standartlar Ailesinin Başlıca Üyeleri*

Standart	Konu	Açıklama
ISO/IEC 27000	Terimler ve Genel Bakış	Temel kavramlar, tanımlar ve ailenin genel yapısı
ISO/IEC 27001	BGYS Gereksinimleri (Sertifikalandırılabilir)	BGYS kurma, uygulama, sürdürme ve iyileştirme gereksinimleri
ISO/IEC 27002	Bilgi Güvenliği Kontrolleri Uygulama Kodu	93 kontrolün amaç, rehberlik ve uygulama detayları
ISO/IEC 27003	BGYS Uygulama Rehberi	ISO 27001'in nasıl uygulanacağına dair pratik rehber
ISO/IEC 27004	Bilgi Güvenliği Ölçme Teknikleri	BGYS performans ölçümü ve izleme yöntemleri
ISO/IEC 27005	Bilgi Güvenliği Risk Yönetimi	Risk değerlendirme ve işleme için metodolojik çerçeve
ISO/IEC 27006	Belgelendirme Kuruluşları İçin Şartlar	Akredite BGYS denetim ve belgelendirme kuruluşları için rehber
ISO/IEC 27017	Bulut Bilişim Güvenliği	ISO 27002 bazlı bulut bilişim bilgi güvenliği kontrolleri
ISO/IEC 27018	Bulutta Kişisel Veri Gizliliği	Bulut ortamında kişisel veri (PII) koruma kontrollleri
ISO/IEC 27031	İş Sürekliliği için BİT Hazırlığı	İş sürekliliği için BİT altyapısı hazırlık rehberi
ISO/IEC 27032	Siber Güvenlik Rehberi	Kuruluşlar arası siber güvenlik koordinasyon rehberi

Standart	Konu	Açıklama
ISO/IEC 27035	Güvenlik Olayı Yönetimi	Bilgi güvenliği olay yönetimi ilkeleri ve süreci
ISO/IEC 27701	Gizlilik Bilgi Yönetimi	ISO 27001'in GDPR/KVKK uyumluluğu için gizlilik uzantısı

Not. Kaynak: Yüksektepeli (2013); Ekşi (2023); KUM Eğitim (2021); ISO (2022) temel alınarak derlenmiştir.

2.2 ISO/IEC 27001 ve ISO/IEC 27002 Arasındaki Fark

ISO 27001 ile ISO 27002 arasındaki fark, bilgi güvenliği pratiklerinde en sık sorulan sorulardan birini oluşturmaktadır. Secureframe'in (2025) açıklamasına göre: 'ISO 27001'i 'ne' olarak, ISO 27002'yi ise uyumluluğun 'nasılı' olarak düşünebilirsiniz.' ISO 27001, BGYS'yi kurmak, sürdürmek ve sürekli iyileştirmek için gereksinimleri tanımlayan ve bağımsız akredite kuruluşlar tarafından dış denetimle sertifikalandırılabilen standarttır. ISO 27002 ise ISO 27001'e tamamlayıcı bir rehber olup Ek A'daki her kontrolün amacını, tasarımını ve uygulamasını daha ayrıntılı açıklamaktadır.

Bu ilişki, bir binanın imar planı ile inşaat teknik şartnamesi arasındaki farka benzetilebilir: ISO 27001 neyin inşa edilmesi gerektiğini belirlerken, ISO 27002 her odanın nasıl donatılacağını tarif etmektedir. Bir kuruluş ISO 27001 ile sertifikalandırılabilir; ancak ISO 27002 sertifikasyonu mevcut değildir — bu standart yalnızca uygulama rehberi niteliği taşımaktadır.

2.3 ISO/IEC 27701: Gizlilik Uzantısı ve GDPR/KVKK İlişkisi

ISO/IEC 27701:2019, ISO 27001'i gizlilik bilgi yönetimi için genişleten bir uzantı standarttır. Bu standart, kuruluşların Kişisel Veri İşleyen (PII İşleyici) veya Kişisel Veri Denetçisi (PII Denetçisi) olarak uyması gereken gizlilik gereksinimlerini ISO 27001 çerçevesine entegre etmektedir. GDPR ve Türkiye'deki 6698 sayılı KVKK ile güçlü bir uyum köprüsü oluşturan bu standart, veri koruma uyumluluğunun ISO 27001 BGYS altyapısı üzerine inşa edilmesini sağlamaktadır.

Vertacert'in (2025) değerlendirmesine göre, ISO 27001 ve KVKK entegrasyonu şu pratik sinerjiyi sunar: Varlık Envanteri ile Kişisel Veri İşleme Envanteri eşleştirilebilir; bilgi güvenliği risk analizine kişisel veri ihlali riskleri eklenebilir; olay yönetimi prosedürü KVKK'nın 72 saatlik bildirim yükümlülüğüne göre revize edilebilir; ISO 27001:2022'nin A.8.10 kontrolü (Bilginin Silinmesi) ile KVKK'nın Saklama ve İmha Politikası birleştirilebilir.

3. ISO/IEC 27001:2022 Revizyonu: Değişiklikler ve Yenilikler

3.1 Revizyonun Arka Planı ve Yayım Süreci

ISO/IEC 27001'in güncel sürümü, Ekim 2022'de yayımlanmıştır. Önceki sürüm olan ISO/IEC 27001:2013'ten bu yana geçen dokuz yıllık süreçte teknoloji ortamı kökten değişmiş; bulut bilişim, uzaktan çalışma, tedarik zinciri saldırıları ve fidye yazılımı gibi yeni tehdit ve risk kategorileri standart güncellemesini zorunlu kılmıştır. LRQA'nın (2025) aktardığı üzere, '2022

burakgun.com

revizyonu; 2013 standardının temel ilke ve süreçlerinin büyük bölümünü korurken, günümüz siber güvenlik ortamını ele alan modernize edilmiş kontroller içermekte ve belirli alanları rafine etmektedir.'

Geçiş takvimi açısından: Yeni standart 25 Ekim 2022'de yayımlandı. Nisan 2024'ten itibaren ISO 27001:2013'e karşı ilk veya yeniden sertifikasyon denetimleri durduruldu. 31 Ekim 2025 tarihinde tüm ISO 27001:2013 sertifikalarının geçerliliği sona erdi veya geri çekilmesi gerekti (SGS, 2024). Bu tarih itibarıyla her sertifikasyon denetimi artık yalnızca 2022 sürümüne göre yapılmaktadır.

3.2 Madde Düzeyindeki Yapısal Değişiklikler

ISO 27001:2022 revizyonu, maddeler düzeyinde pek çok önemli değişiklik getirmiştir. A-LIGN'ın (2025) kapsamlı değerlendirmesine göre bu değişikliklerin başlıcaları şunlardır:

Madde 4.2 — İlgili Tarafların Gereksinimleri: Kuruluşlar artık yalnızca ilgili tarafları listelemekle yetinmeyip, bu tarafların hangi gereksinimlerinin BGYS aracılığıyla karşılanacağını açıkça belgelemelidir. BALTUM'un (2026) ifadesiyle, 'bu durum belgelenmiş analiz gerektirmekte; yalnızca paydaş listesi artık standardı karşılamamaktadır.'

Madde 4.4 — BGYS Kapsamı: Standart artık kuruluşların BGYS için gerekli süreçleri ve bu süreçlerin birbirleriyle etkileşimlerini tanımlamasını zorunlu kılmaktadır. Bu, saf belge temelli uyumluluk anlayışından süreç temelli düşünceye geçişi temsil etmektedir.

Madde 6.2 — Bilgi Güvenliği Amaçları: Bilgi güvenliği amaçları artık izlenebilir nitelikte olmalı ve izlemenin nasıl yapılacağı açıkça belgelenmelidir. Statik bir amaçlar kaydı bu gereksinimi artık karşılamamaktadır.

Madde 6.3 — Değişikliklerin Planlanması (YENİ): Bu tamamen yeni bir alt maddedir. BGYS'ye ihtiyaç duyulan değişiklikler, planlanmış bir şekilde gerçekleştirilmelidir. Bu, yönetim sistemi düzeyinde değişim yönetimini resmileştirmektedir.

Madde 9.3 — Yönetimin Gözden Geçirmesi: Gözden geçirme girdileri artık BGYS ile ilgili ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikleri de açıkça içermelidir. Bu, Madde 4.2'deki yeni gereksinimle doğrudan bağlantılıdır.

Madde 10 — Sürekli İyileştirme (Sıralama Değişikliği): Sıralama değişmiştir: Sürekli iyileştirme (10.1) artık uygunsuzluk ve düzeltici faaliyetten (10.2) önce gelmektedir. Bu, iyileştirmenin yalnızca reaktif değil proaktif olması gerektiği mesajını vermektedir.

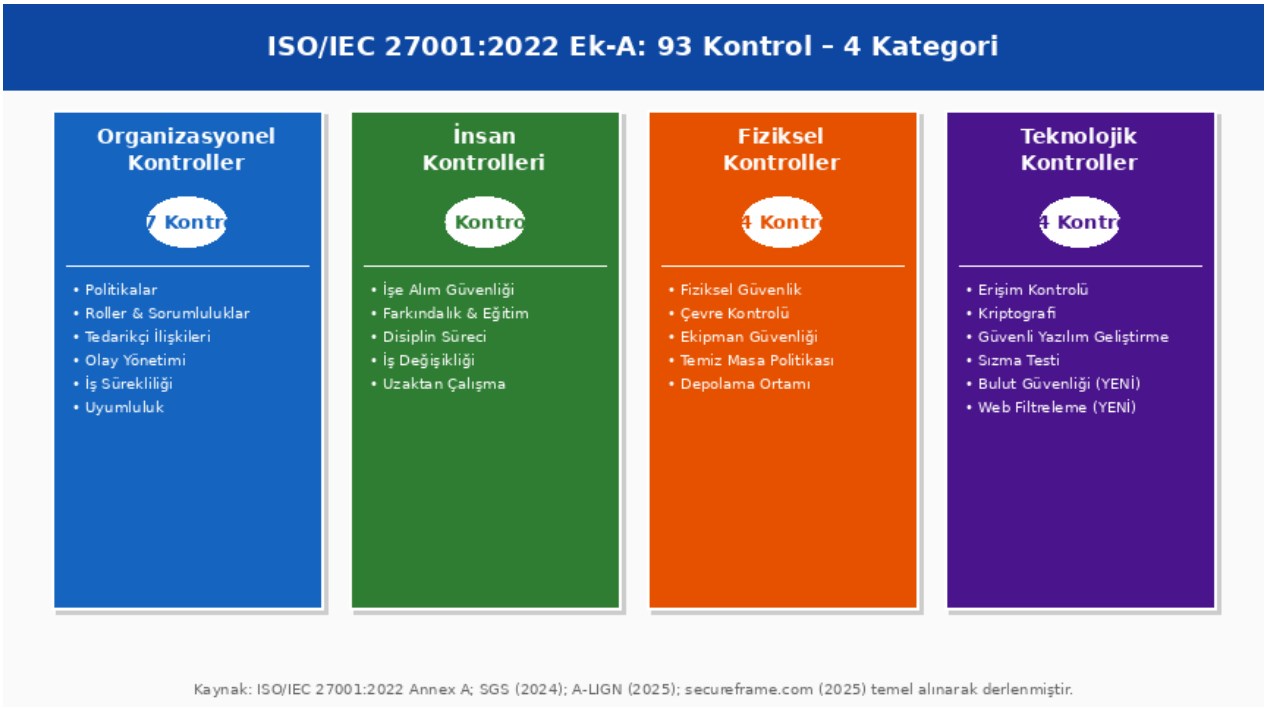
3.3 Ek-A: 114'ten 93 Kontrole Yeniden Yapılanma

ISO 27001:2022'nin en görünür değişikliği, Ek-A'nın yeniden yapılandırılmasıdır. 2013 sürümünde 14 kontrol kategorisinde 114 kontrol yer alırken, 2022 sürümünde 4 kontrol kategorisinde 93 kontrole geçilmiştir. SGS'nin (2024) açıklamasına göre '11 kontrol yeni eklenmiş, 24 kontrol mevcut kontrollerden birleştirilmiş ve 58 kontrol güncellenmiştir.' Bu dönüşüm bir azaltma değil; kontrollerin modernize edilerek yeniden kategorize edilmesidir.

Yeni eklenen 11 kontrol özellikle dikkat çekicidir. Bu kontroller arasında; Tehdit İstihbaratı (A.5.7), Bulut Hizmetleri Kullanım Güvenliği (A.5.23), İş Sürekliliğine Hazırlık (A.5.30), Fiziksel Güvenlik İzleme (A.7.4), Yapılandırma Yönetimi (A.8.9), Bilgi Silme (A.8.10), Veri Maskeleme (A.8.11), Veri Sızıntısı Önleme (A.8.12), İzleme Faaliyetleri

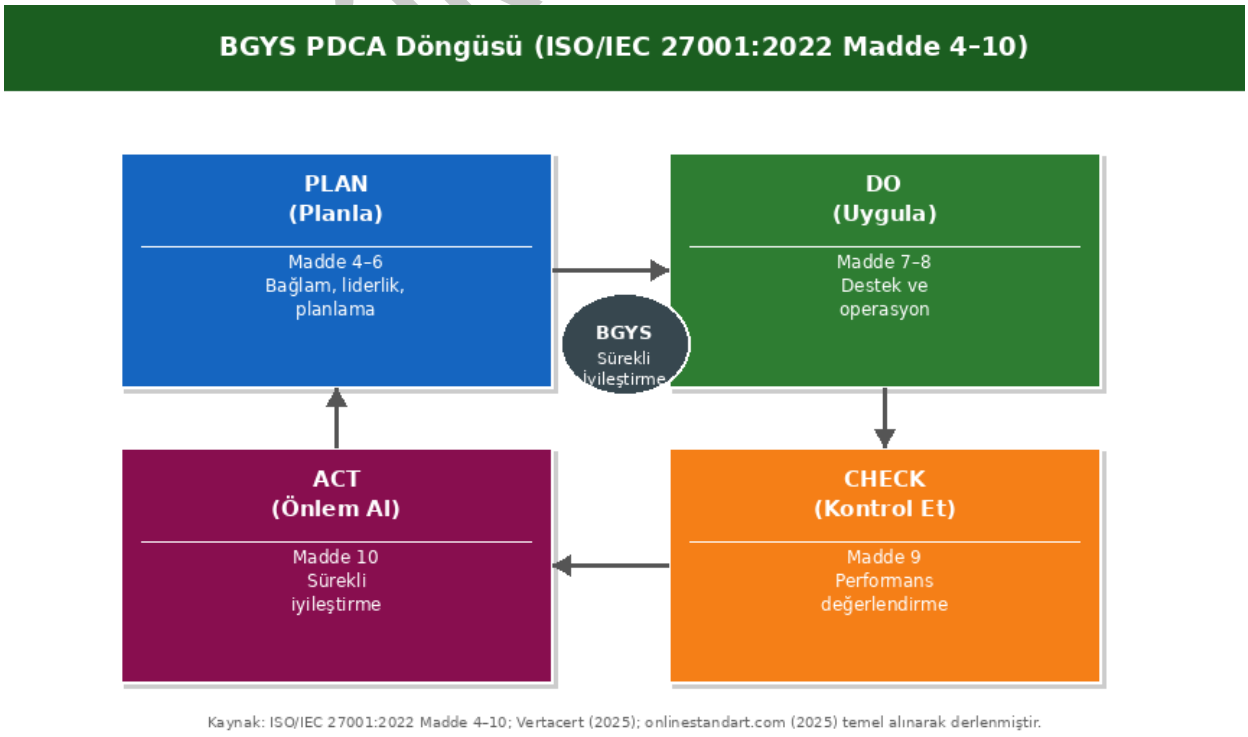
bilgiguvenligi.com

(A.8.16), Web Filtreleme (A.8.23) ve Güvenli Kodlama (A.8.28) yer almaktadır. Bu kontroller; bulut altyapısı, uzaktan çalışma ve hibrit ortamların getirdiği yeni güvenlik gereksinimlerine doğrudan yanıt vermektedir.



Şekil 1. *ISO/IEC 27001:2022 Ek-A: 93 Kontrol — 4 Kategori Dağılımı*

4. BGYS Mimarisi: PDCA Döngüsü ve Madde 4–10 Yapısı



Şekil 2. *BGYS PDCA Döngüsü — ISO/IEC 27001:2022 Madde 4–10 Eşleşmesi*

4.1 PDCA Döngüsü ve Sürekli İyileştirme Felsefesi

ISO/IEC 27001, BGYS'nin Planla-Uygula-Kontrol Et-Önlem Al (PDCA) döngüsü çerçevesinde yönetilmesini esas almaktadır. Bu yaklaşım, ISO 9001 Kalite Yönetim Sistemi ve diğer ISO yönetim standartlarıyla ortak bir yapısal dil oluşturarak entegre yönetim sistemi kurulumunu kolaylaştırmaktadır. BGYS, statik bir uyumluluk çerçevesi değil; tehdit ortamındaki değişimlere ve kurumsal bağlamdaki dönüşümlere yanıt verebilen dinamik bir yönetim mekanizmasıdır (ISO, 2022).

PDCA döngüsünün BGYS'ye yansıması: Plan aşaması; kuruluşun bağlamını, ilgili taraflarını, BGYS kapsamını, bilgi güvenliği risklerini ve bu risklere yönelik hedefleri belirlemesiyle gerçekleşir (Madde 4–6). Do aşaması; belirlenen kontrollerin ve politikaların fiilen uygulanması, destek mekanizmalarının devreye alınması ve BGYS operasyonlarının yürütülmesiyle tamamlanır (Madde 7–8). Check aşaması; BGYS performansının izlenmesi, ölçülmesi, analiz edilmesi ve değerlendirilmesiyle yürütülür (Madde 9). Act aşaması ise uygunsuzlukların giderilmesi ve sürekli iyileştirme faaliyetlerini kapsar (Madde 10).

4.2 Madde 4: Kuruluşun Bağlamı

ISO 27001:2022'nin Madde 4'ü, BGYS'nin iş bağlamından bağımsız bir şablona dönüşmesini önlemek amacıyla kuruluşun iç ve dış faktörlerini sistematik biçimde anlamasını zorunlu kılmaktadır. BALTUM'un (2026) vurguladığı üzere, 2022 revizyonu 'ilgili taraflar, gerekli süreçler ve BGYS içindeki roller dahil kapsamlı bir analiz yapılmasını teşvik etmektedir.'

İç faktörler arasında kuruluşun büyüklüğü ve yapısı, yönetim kültürü, mevcut BT altyapısı, çalışan profili ve iş süreçlerinin karmaşıklığı sayılabilir. Dış faktörler ise yasal ve düzenleyici yükümlülükler, müşteri ve tedarikçi gereksinimleri, rekabet ortamı ve sektörel tehdit panoraması başlıklarında değerlendirilebilir. Türkiye bağlamında dış faktörler arasında özellikle 6698 sayılı KVKK, 5809 sayılı Elektronik Haberleşme Kanunu ve Bilgi Güvenliği Rehberi (CBdDO, 2024) öne çıkmaktadır.

4.3 Madde 5: Liderlik ve Üst Yönetim Taahhüdü

ISO 27001, bilgi güvenliğini yalnızca BT departmanının sorumluluğu olarak değil; üst yönetimin doğrudan sahiplendiği bir kurumsal yönetim meselesi olarak konumlandırmaktadır. Konfirmity'nin (2026) vurguladığı üzere, 'standart; kuruluş bağlamı, liderlik taahhüdü ve tedarikçi yönetimini gerektirmektedir. Çevresel riskler, iş sürekliliği ve insan kontrolleri; yöneticileri, satın alma ve İK departmanlarını ilgilendirmektedir. Siloya dayalı bir yaklaşım denetimlerde başarısızlıkla sonuçlanmaktadır.'

Üst yönetimin BGYS'ye taahhüdü; bilgi güvenliği politikasını onaylamak, BGYS'yi iş hedefleriyle entegre etmek, gerekli kaynakları tahsis etmek, rolleri ve sorumlulukları atamak ve yönetim gözden geçirme toplantılarını düzenli olarak gerçekleştirmek biçiminde somutlaşmaktadır. T.C. Ticaret Bakanlığı'nın (2024) ISO 27001 belgesinde bu taahhüt şöyle ifade edilmektedir: 'Genel Müdürlüğümüzün sahip olduğu bilgi varlıklarının gizlilik, bütünlük

burokon.com

ve erişilebilirliğini sağlamak, teknolojik kaynakları güvence altına almak ve bilgi güvenliği farkındalığını oluşturmak amacıyla kurulmuştur.'

5. Risk Yönetimi: ISO 27001'in Temel Taşı

5.1 Risk Değerlendirme Metodolojisi

ISO/IEC 27001, risk yönetimini BGYS'nin merkezine yerleştirmektedir. Standart, risk değerlendirme metodolojisini dikte etmez; bunun yerine kuruluşun kendi metodolojisini belgeleyip tutarlı biçimde uygulamasını zorunlu kılar. Bu metodoloji belgelemesi, denetçilerin süreci anlayabilmesi ve tekrarlanabilirliği doğrulayabilmesi açısından kritik önem taşımaktadır (Vertacert, 2025).

Yaygın kullanılan risk değerlendirme yaklaşımı şu adımları içermektedir: Varlık Tespiti — Kuruluşun bilgi varlıklarının (donanım, yazılım, veriler, insan kaynakları, fiziksel ortamlar) envantere alınması. Tehdit Analizi — Her varlığa yönelik olası tehditler (siber saldırı, doğal afet, insan hatası, tedarikçi ihlali) tanımlanır. Zafiyet Tespiti — Varlıkların her bir tehdide karşı taşıdığı zayıflıklar belirlenir. Risk Skoru Hesaplama — Olasılık × Etki formülü ya da benzeri bir metodoloji kullanılarak risk seviyeleri sayısallaştırılır.

Vertacert'in (2025) sunduğu somut senaryolar risk değerlendirme sürecini canlandırmaktadır: 'Sunucu odasını su basması' veya 'Muhasebe personelinin oltalama (phishing) mailine tıklaması' gibi senaryolar, tehdit-zafiyet kombinasyonlarının nasıl modellendiğini göstermektedir. Bu senaryolarda çıkan skor, kabul edilebilir risk eşiğinin üzerindeyse azaltma, kaçınma ya da transfer stratejilerinden biri seçilmektedir.

5.2 Risk İşleme Seçenekleri

Risk işleme, değerlendirme aşamasının ardından risklere ne yapılacağına karar verme sürecidir. ISO 27001 dört temel risk işleme seçeneği sunmaktadır.

- **Azaltma (Mitigate):** Kontrol uygulayarak riski kabul edilebilir düzeye indirmek. En yaygın yöntemdir; Ek-A kontrolleri bu seçenek için birincil araç işlevi görür.
- **Transfer Etme (Transfer):** Riski sigorta yaptırmak ya da dışarıdan hizmet satın alarak üçüncü tarafa devretmek. Siber güvenlik sigortası en yaygın örneğidir.
- **Kaçınma (Avoid):** Riski doğuran faaliyetten tamamen vazgeçmek. Düzenleyici uyumluluk maliyeti çok yüksekse bazı hizmetlerin sunulmaması örnek verilebilir.
- **Kabul Etme (Accept):** Riski bilinçli olarak kabul etmek. Risk seviyesi kabul edilebilir eşiğin altında kaldığında ya da azaltma maliyeti riskten büyük olduğunda tercih edilir.

5.3 Uygulanabilirlik Bildirgesi (SoA)

Uygulanabilirlik Bildirgesi (Statement of Applicability — SoA), BGYS'nin en kritik denetim belgesi olarak tanımlanmaktadır. DSR Belgelendirme'nin (2026) aktarımına göre SoA, '93 adet kontrolün hangilerinin seçildiğini gösteren en kritik denetim belgesidir.' Standart kapsamında

burakolgun.com

SoA; seçilen kontrollerin listesini, her kontrolün dahil edilme ya da hariç tutulma gerekçesini, uygulama durumunu ve seçilen kontrolün nasıl uygulandığını içermelidir (A-LIGN, 2025).

SoA, BGYS'nin 'parmak izi' niteliğindedir: İki kuruluşun SoA'sı özdeş olamaz; çünkü risk profili, sektör, kapsam ve iş bağlamı her kuruluşta farklılaşmaktadır. Otomotiv sektöründe faaliyet gösteren bir üretici ile sağlık verisi işleyen bir hastane için öne çıkan kontroller kümesi büyük farklılıklar gösterecektir. Bu bireyselleştirme, ISO 27001'in sektör veya boyuttan bağımsız uygulanabilirliğini sağlayan temel mekanizmadır.

6. Varlık Envanteri ve Sınıflandırma

6.1 Bilgi Varlığı Türleri

Varlık envanteri oluşturma, BGYS kurulumunun ilk adımlarından biridir. KUM Eğitim'in (tarihsiz) açıklamasına göre bilgi varlıkları şu kategorilerde ele alınmaktadır: Yazılım varlıkları — kurumsal uygulamalar, işletim sistemleri, lisanslı yazılımlar, özel geliştirme ürünleri. Donanım varlıkları — sunucular, iş istasyonları, ağ cihazları, depolama sistemleri, mobil cihazlar.

Veri varlıkları — veritabanları, müşteri kayıtları, finansal veriler, ticari sırlar ve kişisel veriler. Servis varlıkları — bulut hizmetleri, internet bağlantısı, veri merkezi hizmetleri. İnsan varlıkları — kritik bilgiye sahip kilit personel, yöneticiler, sistem yöneticileri. Fiziksel varlıklar — sunucu odaları, ofis binaları ve güvenlik altyapısı. Varlık envanterinde her varlık için sahip atanmalı ve gizlilik (C), bütünlük (I), erişilebilirlik (A) açılarından kritiklik puanı belirlenmelidir (Vertacert, 2025).

6.2 GİA Üçgeni: Gizlilik, Bütünlük, Erişilebilirlik

Bilgi güvenliğinin temel üçlüsü olan GİA (Gizlilik-Bütünlük-Erişilebilirlik) veya İngilizce kısaltmasıyla CIA (Confidentiality-Integrity-Availability) üçgeni, tüm BGYS kontrollerinin odaklandığı koruma boyutlarını tanımlamaktadır. CTR'nin (tarihsiz) aktarımıyla, 'Bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün, kullanılabilirliğinin korunmasıdır.'

Gizlilik (Confidentiality): Bilginin yalnızca yetkili kişiler tarafından erişilebilir olmasıdır. Şifreleme, erişim kontrolü ve en az ayrıcalık prensibi bu boyutu destekler.

Bütünlük (Integrity): Bilginin yetkisiz değiştirilmeden korunması ve doğruluğunun güvence altına alınmasıdır. Dijital imza, hash doğrulama ve değişiklik izleme mekanizmaları bu boyutu korur.

Erişilebilirlik (Availability): Yetkili kullanıcıların ihtiyaç duydukları anda bilgiye erişebildiği güvencesidir. Yedekleme sistemleri, yük dengeleme ve iş sürekliliği planları bu boyutu destekler.

burakolgun.com

7. Ek-A Kontrolleri: Dört Kategorinin Derinlemesine İncelemesi

7.1 Organizasyonel Kontroller (37 Kontrol: A.5.1 – A.5.37)

Organizasyonel kontroller, BGYS'nin politika, süreç ve yönetim boyutunu kapsamaktadır. A.5.1 kapsamında bilgi güvenliği politikaları; üst yönetim tarafından onaylanmış, belgelenmiş ve düzenli aralıklarla gözden geçirilmiş olmalıdır. A.5.2–A.5.4 kapsamında roller, sorumluluklar ve görevler ayrılığı düzenlenmektedir: Çıkar çatışmasını önlemek amacıyla aynı bireyin hem bir değişikliği onaylaması hem de uygulaması engellenmelidir.

2022 sürümüne yeni eklenen A.5.7 Tehdit İstihbaratı kontrolü, kuruluşun ilgili bilgi güvenliği tehditlerini toplaması ve analiz etmesini gerektirmektedir. Bu kontrol, tehdit istihbaratı platformlarının (SIEM, ISAC paylaşım mekanizmaları) BGYS kapsamında resmileştirilmesini zorunlu kılmaktadır. A.5.23 ise bulut hizmetleri için bilgi güvenliğini kapsayan yeni bir kontroldür; bu kontrol kapsamında bulut tedarikçi değerlendirme, sözleşme güvenlik maddeleri ve bulut veri yönetimi politikası gereksinimleri tanımlanmaktadır.

A.5.36 Bilgi Güvenliği Politikaları, Kurallar ve Standartlara Uyum kontrolü, kuruluşun tüm çalışanların ve ilgili tarafların kendi bilgi güvenliği politika ve prosedürlerine uyumunu düzenli olarak doğrulamasını gerektirmektedir. A.5.37 Dokümante Edilmiş Operasyon Prosedürleri kontrolü ise bilgi işleme tesislerine ilişkin operasyon prosedürlerinin belgelenmesi ve ilgili kullanıcıların erişimine sunulmasını zorunlu kılmaktadır.

7.2 İnsan Kontrolleri (8 Kontrol: A.6.1 – A.6.8)

İnsan kontrolleri, çalışanların bilgi güvenliği süreçleriyle ilişkisini kapsamaktadır. A.6.1 Taramalar kontrolü, bilgi işleme tesislerine erişimi olan tüm personel için işe alım öncesi doğrulama süreçlerini — kimlik teyidi, referans kontrolü ve varsa güvenlik soruşturması — zorunlu kılmaktadır.

A.6.3 Bilgi Güvenliği Farkındalık, Eğitim ve Öğretim kontrolü, kuruluşun tüm çalışanlarına görev ve sorumluluklarıyla uyumlu bilgi güvenliği farkındalık eğitimi vermesini ve bu eğitimleri kayıt altına almasını zorunlu tutmaktadır. Denetçiler genellikle yıllık eğitim tamamlama oranlarını ve eğitim içeriklerinin mevcut tehdit ortamını yansıtıp yansıtmadığını incelemektedir.

2022 sürümüyle birlikte öne çıkan A.6.7 Uzaktan Çalışma kontrolü, uzaktan çalışma sırasında bilgiye erişim ve işlenmesi için gerekli güvenlik önlemlerini tanımlamaktadır. COVID-19 pandemisinin kalıcı olarak kurumsallaştırdığı uzaktan ve hibrit çalışma modellerinin yarattığı güvenlik boşluğuna doğrudan yanıt veren bu kontrol, VPN politikaları, ekran kilidi zorunluluğu ve ev ağı güvenlik standartlarını kapsamaktadır.

7.3 Fiziksel Kontroller (14 Kontrol: A.7.1 – A.7.14)

Fiziksel kontroller; sunucu odaları, ofis binaları ve diğer hassas alanların fiziksel güvenliğini kapsamaktadır. A.7.1–A.7.2 kapsamında güvenlik perimetri ve fiziksel giriş kontrolleri tanımlanmakta; bu kontroller kart okuyucular, güvenlik kameraları ve ziyaretçi kayıt sistemlerinin kullanımını kapsamaktadır.

burakolgun.com

A.7.4 Fiziksel Güvenlik İzleme, 2022 sürümüne eklenen yeni bir kontroldür. Hassas alanlara yetkisiz fiziksel erişime karşı sürekli izleme sağlanmasını zorunlu kılan bu kontrol, özellikle veri merkezi fiziksel güvenlik izleme sistemlerine doğrudan zemin hazırlamaktadır.

A.7.8 Ekipman Yerleşimi ve Korunması kontrolü; donanımın hem fiziksel hem çevresel tehditler (ısı, nem, su baskını) gözetilerek konumlandırılmasını kapsamaktadır. A.7.9 Ofis Dışındaki Varlıkların Güvenliği; dizüstü bilgisayarlar, akıllı telefonlar ve taşınabilir depolama cihazlarına yönelik güvenlik gereksinimlerini tanımlamaktadır. A.7.14 Ekipmanın Güvenli Bertarafı, depolama ortamlarında kalan verilerin güvenli biçimde imha edilmesini zorunlu tutmaktadır.

7.4 Teknolojik Kontroller (34 Kontrol: A.8.1 – A.8.34)

Teknolojik kontroller, BGYS'nin teknik güvenlik boyutunu en kapsamlı biçimde kapsayan kategorisini oluşturmaktadır. A.8.1 Kullanıcı Uç Noktası Cihazları; dizüstü bilgisayarlar, akıllı telefonlar ve tabletlerde uygulanacak güvenlik politikalarını tanımlar. A.8.2 Ayrıcalıklı Erişim Hakları; yönetici hesaplarının yönetimini ve en az ayrıcalık prensibinin uygulanmasını kapsamer.

A.8.9 Yapılandırma Yönetimi, 2022 sürümünün yeni kontrollerinden biridir. Donanım, yazılım, hizmetler ve ağlar dahil tüm bileşenler için güvenlik yapılandırmalarının kurulması, belgelenmesi, uygulanması, izlenmesi ve gözden geçirilmesini zorunlu kılmaktadır. Bu kontrol, DevSecOps kültürünün BGYS çerçevesine entegrasyonunu doğrudan desteklemektedir.

A.8.11 Veri Maskeleme ve A.8.12 Veri Sızıntısı Önleme (DLP) kontrolleri, 2022 sürümünün veri korumasına verdiği artan önemi yansıtmaktadır. DLP kontrolleri kapsamında kuruluşların hassas verilerin yetkisiz kopyalanması, iletilmesi veya ifşasına karşı teknik önlemler uygulaması gerekmektedir. A.8.23 Web Filtreleme ise çalışanların kötü amaçlı veya uygunsuz web içeriklerine erişiminin sınırlandırılmasına yönelik kontrolleri kapsamaktadır.

A.8.28 Güvenli Kodlama, 2022 sürümüne eklenen ve özellikle yazılım geliştiren kuruluşlar açısından kritik öneme sahip bir kontroldür. OWASP ilkelerine ve güvenli yazılım geliştirme yaşam döngüsü (SDLC) metodolojilerine uygun kodlama pratiklerinin uygulanmasını zorunlu kılmaktadır.

Tablo 2. *ISO/IEC 27001:2022 Ek-A'ya 2022'de Eklenen 11 Yeni Kontrol*

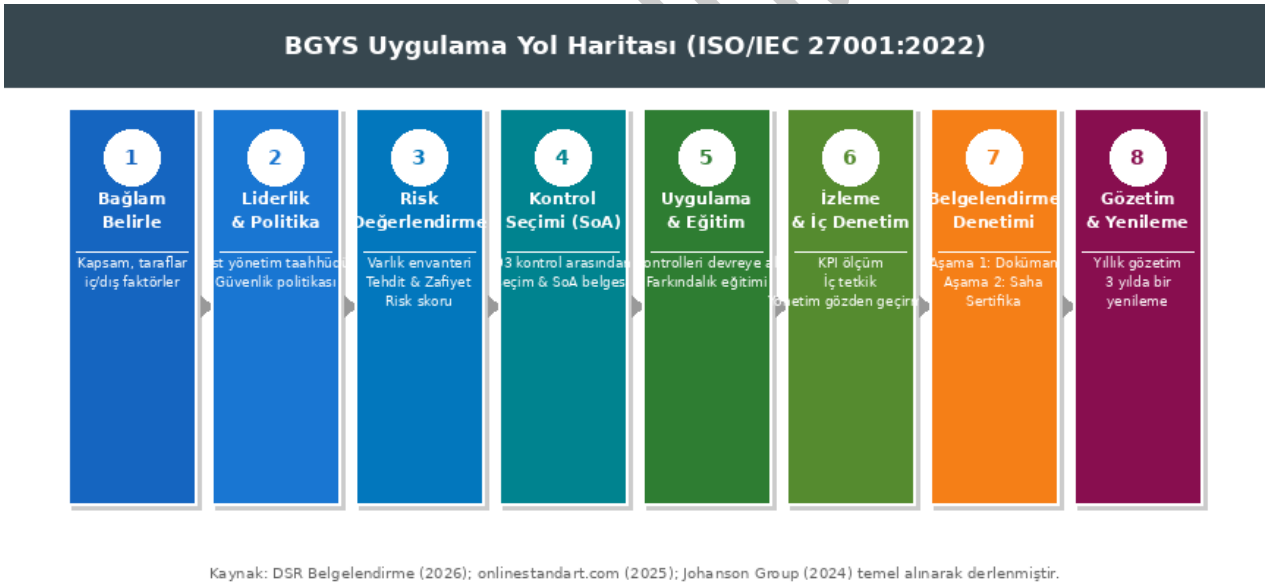
Kontrol No	Kontrol Adı	Kapsam / Gereklilik
A.5.7	Tehdit İstihbaratı	İlgili bilgi güvenliği tehditlerinin toplanması ve analiz edilmesi
A.5.23	Bulut Hizmetleri Güvenliği	Bulut hizmetlerinin edinimi, kullanımı, yönetimi ve çıkışı için güvenlik süreci
A.5.30	İş Sürekliliği Hazırlığı (BİT)	İş sürekliliği için BİT'in iş sürekliliği hedefleri ve gereksinimleriyle uyumu
A.7.4	Fiziksel Güvenlik İzleme	Hassas alanlara yetkisiz fiziksel erişime karşı sürekli izleme
A.8.9	Yapılandırma Yönetimi	Tüm bileşenlerin güvenlik yapılandırmalarının kurulması, izlenmesi ve gözden geçirilmesi

burakgun.com

Kontrol No	Kontrol Adı	Kapsam / Gereklilik
A.8.10	Bilgi Silme	Sistemlerde, cihazlarda ve medyada gereksiz bilginin güvenli silinmesi
A.8.11	Veri Maskeleme	Gizlilik ve uyumluluk gereksinimlerine dayalı hassas veri maskeleme uygulaması
A.8.12	Veri Sızıntısı Önleme	Yetkisiz veri ifşasını önlemek için DLP araçları ve politikalarının uygulanması
A.8.16	İzleme Faaliyetleri	Anomali ve olağan dışı davranışların tespiti için ağ ve sistem izleme
A.8.23	Web Filtreleme	Kötü amaçlı yazılım ve yetkisiz içerik barındıran web sitelerine erişimin kontrolü
A.8.28	Güvenli Kodlama	Yazılım güvenlik açıklarını azaltmak için güvenli kodlama prensiplerinin uygulanması

Not. Kaynak: SGS (2024); A-LIGN (2025); secureframe.com (2025); goteleport.com (2025) temel alınarak derlenmiştir.

8. BGYS Uygulama Yol Haritası



Şekil 3. *BGYS Uygulama Yol Haritası — 8 Aşamalı Süreç Modeli (ISO/IEC 27001:2022)*

8.1 Boşluk Analizi (Gap Assessment)

BGYS kurulum sürecinin ilk adımı, mevcut durum ile ISO 27001 gereksinimleri arasındaki boşlukların sistematik biçimde tespit edilmesidir. A-LIGN'ın (2025) tavsiyesine göre '2013 sürümünden geçiş sürecinde kuruluşlar, mevcut BGYS'yi 2022 sürümüyle eşleştiren bir boşluk değerlendirmesi yapmalı ve hangi değişikliklerin gerektiğini belirlemelidir.' Bu değerlendirme iki boyutu kapsamalıdır: Madde uyumluluk boşluğu (Madde 4–10 gereksinimleri) ve Ek-A kontrol boşluğu (özellikle 11 yeni kontrole ilişkin boşluklar).

8.2 Zorunlu Dokümantasyon Gereklilikleri

ISO/IEC 27001, belirli belge ve kayıtların mevcut olmasını zorunlu kılmaktadır. isodestek.com'un (2025) derlediği zorunlu belgeler listesi şu başlıkları içermektedir:

Zorunlu Belgeler: BGYS Kapsam Dokümanı — BGYS sınırlarını, hangi birimleri ve varlıkları kapsadığını tanımlar (Madde 4.3). Bilgi Güvenliği Politikası — üst yönetimin onayladığı taahhüt belgesi. Bilgi Güvenliği Amaçları — izlenebilir hedefler ve nasıl izleneceğine dair metodoloji. Uygulanabilirlik Bildirgesi (SoA) — 93 kontrolün hangilerinin seçildiğini ve gerekçelerini gösterir. Risk İşleme Planı (RTP) — tespit edilen risklere karşı alınacak aksiyonlar. Risk Değerlendirme Prosedürü — risklerin nasıl belirleneceği ve derecelendirileceği metodoloji.

Zorunlu Kayıtlar: Eğitim, deneyim, beceri kayıtları. İzleme ve ölçme sonuçları. İç tetkik programı ve sonuçları. Yönetim gözden geçirmesi sonuçları. Uygunsuzluk ve düzeltici faaliyet kayıtları. Risk değerlendirme sonuçları ve risk işleme planının uygulanma kanıtları.

8.3 İç Denetim ve Yönetim Gözden Geçirmesi

ISO 27001'in sürekli iyileştirme mekanizması; iç denetim ve yönetim gözden geçirmesi aracılığıyla işlemektedir. İç denetim, BGYS'nin standart gereksinimlerini karşılayıp karşılamadığını ve planlanmış süreçlerin etkin biçimde uygulanıp uygulanmadığını değerlendirmektedir. onlinestandart.com'un (2025) aktarımına göre, dış denetimden önce iç denetim ve yönetim gözden geçirmesinin tamamlanmış olması zorunludur.

Yönetim gözden geçirmesi, üst yönetimin BGYS performansını periyodik olarak değerlendirdiği bir toplantı sürecidir. 2022 revizyonuyla birlikte bu toplantı girdileri; önceki gözden geçirmelerin takip aksiyonları, iç ve dış sorunlardaki değişiklikler, bilgi güvenliği performans göstergeleri ve ilgili tarafların ihtiyaç ve beklentilerindeki değişiklikleri içermelidir.

9. Belgelendirme Süreci

9.1 Aşama 1 Denetimi: Doküman İncelemesi

ISO 27001 belgelendirme süreci iki aşamalı bir bağımsız dış denetimden oluşmaktadır. Birinci aşama denetiminde; akredite denetim kuruluşunun deneyimli denetçisi, kuruluşun zorunlu dokümantasyonunu — özellikle BGYS kapsamı, bilgi güvenliği politikası, risk değerlendirme prosedürü ve Uygulanabilirlik Bildirgesi'ni — kapsamlı biçimde inceler. Bu aşamanın amacı, kuruluşun ikinci aşamaya hazır olup olmadığını belirlemektir.

9.2 Aşama 2 Denetimi: Saha Denetimi

DSR Belgelendirme'nin (2026) aktarımına göre, ikinci aşama belgelendirme denetiminin temel sorusu şudur: 'Hazırladığınız BGYS dokümanlarını uyguluyor musunuz?' Bu aşamada denetçi; kontrollerin sahada nasıl uygulandığını, çalışanların güvenlik politikalarına uyumunu, teknik önlemlerin etkinliğini ve kayıtların tutarlılığını yerinde gözlemler. Aşama 2 denetiminin sonuçları ve tavsiyeleri genellikle aynı gün içinde bildirilmektedir.

burakogun.com

Denetim kapsamında uygunsuzluklar iki düzeyde sınıflandırılır: Majör uygunsuzluklar, zorunlu bir gereksinimin karşılanmaması ya da uygulamanın tamamen yokluğunu ifade eder ve sertifika verilmesini engeller. Minör uygunsuzluklar, gereksinimin kısmen karşılandığı ancak eksiklikler içerdiği durumları tanımlar; belirli bir süre içinde düzeltici faaliyet tamamlanarak sertifika alınabilmektedir (Johanson Group, 2024).

9.3 Gözetim Denetimleri ve Yenileme

Sertifika alındıktan sonra süreç sona ermez. ISO 27001 sertifikası üç yıl geçerlidir; bu süre boyunca yıllık gözetim denetimleri (surveillance audit) zorunludur. DSR Belgelendirme'nin (2026) belirttiği üzere, 'ISO sertifikasyonunun itibarı, sürekli gelişim ilkesine dayanır.' Üçüncü yılın sonunda yenileme (recertification) denetimi yapılmakta ve yeni sertifika yüklenir. Türkiye'den T.C. Ticaret Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü örneğinde bu süreç somutlaşmaktadır: '13.12.2022 tarihi itibarıyla ISO 27001 sertifikasına sahip olan Genel Müdürlüğümüz, 10.12.2024 tarihinde güncel sertifikasını yayımlamıştır'(BTGM, 2024).

10. Zorunlu Dokümantasyon ve Kayıtlar

10.1 Zorunlu Dokümante Bilgiler

ISO/IEC 27001:2022, standart maddelerinde açıkça zorunlu tutulan 16 tür dokümante bilgi belirlemiştir. isodestek.com'un (2025) listesine göre bu belgeler şunlardır: BGYS kapsamı, bilgi güvenliği politikası, bilgi güvenliği amaçları, uygulanabilirlik bildirgesi, risk işleme planı, risk değerlendirme ve risk işleme raporu, bilgi güvenliği görevleri ve sorumlulukları, varlık envanteri, varlıkların kabul edilebilir kullanımı, erişim kontrol politikası, BT yönetimi için işletim prosedürleri, güvenli sistem mühendisliği prensipleri, tedarikçi güvenlik politikası, bilgi güvenliği ihlal olayına yanıt prosedürü, bilgi güvenliği sürekliliğinin uygulanması ve uygulanabilir yasal/sözleşmesel gereksinimlerin tanımlanması.

10.2 Zorunlu Kayıtlar

Belgelere ek olarak ISO 27001, belirli faaliyetlerin kanıtı olarak tutulması gereken kayıtları da tanımlamaktadır. Bu zorunlu kayıtlar şunlardır: Eğitim, deneyim, beceri ve nitelik kayıtları; izleme ve ölçme sonuçları; iç tetkik programı ve sonuçları; yönetim gözden geçirmesi sonuçları; uygunsuzluk ve düzeltici faaliyet kayıtları.

DSR Belgelendirme'nin (2026) tespitine göre, her madde için ayrı bir doküman yazmak zorunlu değildir; birden fazla gereksinim tek bir belgede karşılanabilir. Öte yandan bazı gereksinimler için birden fazla doküman gerekebilmektedir. Belgeleme mimarisi, kuruluşun büyüklüğüne ve karmaşıklığına uyarlanmalıdır.

burakorgun.com

11. Türkiye'de BGYS: Yasal Çerçeve ve Uygulama Örnekleri

11.1 Türk Mevzuatı ve ISO 27001 İlişkisi

Türkiye'de ISO/IEC 27001, TS EN ISO/IEC 27001:2023 adıyla Türk standardı olarak benimsenerek uygulanmaktadır. TSE (Türk Standardları Enstitüsü), bu standart kapsamında hem belgelendirme hem de eğitim hizmetleri sunmakta; TÜRKAK akreditasyonuyla çalışan bağımsız belgelendirme kuruluşları da sertifikasyon hizmeti vermektedir.

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), ISO 27001 ile güçlü bir uyum sinerji sunmaktadır. Kanunun kişisel veri güvenliği için öngördüğü teknik ve idari tedbirler, ISO 27001 kontrollerinin büyük bölümüyle örtüşmektedir. Özellikle erişim kontrolü, şifreleme, veri imhası ve ihlal bildirimi konularında iki çerçevenin entegre uygulanması hem verimlilik hem de uyumluluk açısından en akılcı yaklaşımı oluşturmaktadır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin 2024 yılında yayımladığı Bilgi ve İletişim Güvenliği Rehberi ile ISO 27001 kontrolleri arasındaki eşleştirme tablosu, kamu kurumları için kritik bir entegrasyon aracı niteliği taşımaktadır. Denetci.org'un (2025) aktarımına göre bu tablo, 'kurum ve kuruluşların halihazırda yürüttükleri BGYS süreçlerini Rehber uygulama adımları ile entegre etmelerine yardımcı olmak amacıyla hazırlanmıştır.'

11.2 Kamu Sektöründe Uygulama Örnekleri

Türkiye'de pek çok kamu kurumu ISO 27001 sertifikasına sahiptir. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı, 2014 yılında BGYS kurulum çalışmalarına başlamış ve TSE denetimini tamamlayarak sertifika almıştır. Bakanlığın BGYS belgesi şu çerçevede yapılandırılmıştır: Bakanlık tarafından çalışanlara veya ilgili taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün, aksini gerektiren kanun hükümleri veya protokol bulunmadıkça Bakanlığa aittir (ÇŞİDB, tarihsiz).

T.C. Ticaret Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü, Aralık 2022'de ISO 27001 sertifikasını almış; ardından 2024'te İkinci Gözetim Denetimini başarıyla tamamlayarak güncel sertifikasını yayımlamıştır. Bakanlığın BGYS gerekçesi şöyle ifade edilmektedir: 'Genel Müdürlüğümüzün sahip olduğu bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak, teknolojik kaynakları güvence altına almak ve bilgi güvenliği farkındalığını oluşturmak' (BTGM, 2024).

11.3 Özel Sektör Uygulamaları ve Motivasyonlar

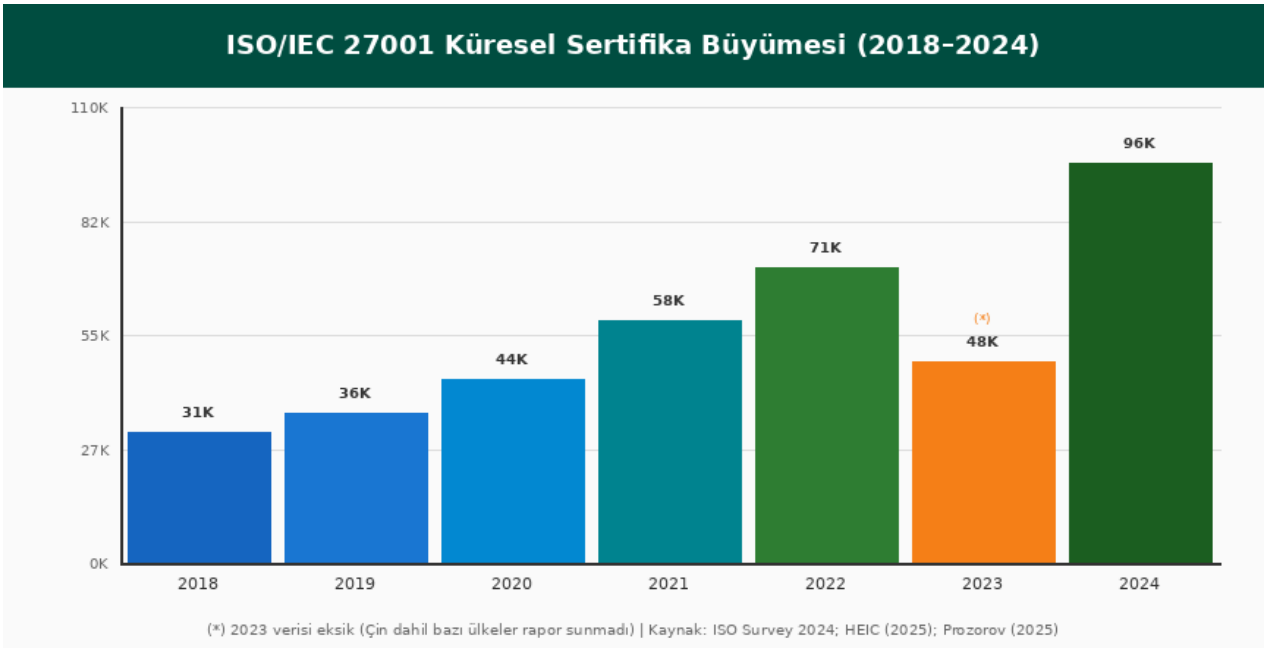
Türk özel sektöründe ISO 27001 sertifikasyonuna olan ilgi, özellikle finans, telekomünikasyon, savunma ve BT hizmetleri sektörlerinde son yıllarda belirgin biçimde artmıştır. isonedir.com'un (tarihsiz) tespitine göre ISO 27001 sertifikası şu avantajları sunmaktadır: Artan müşteri güveni, uluslararası ticaret kapısı (özellikle AB pazarına erişimde), veri ihlali ve siber saldırı risklerinin azaltılması, yasal ve düzenleyici yükümlülüklerin karşılanması ve kurumsal itibarın güçlendirilmesi.

Belgelendirme maliyetleri Türkiye'de çeşitli faktörlere bağlı olarak önemli ölçüde değişmektedir. DSR Belgelendirme'nin (2026) aktarımına göre fiyatlandırmayı etkileyen başlıca unsurlar: Kuruluşun büyüklüğü (toplam çalışan sayısı denetim süresini doğrudan

burakoguz.com

etkiler), sektörel riskler (faaliyet gösterilen sektörün karmaşıklığı ve veri hassasiyeti), kapsam genişliği (tek lokasyon mu çok lokasyon mu) ve mevcut güvenlik olgunluk düzeyidir.

12. Küresel Sertifika Eğilimleri ve Piyasa Büyümesi



Şekil 4. *ISO/IEC 27001 Küresel Sertifika Büyümesi 2018–2024 (ISO Survey 2024)*

12.1 ISO Survey 2024: Tarihin En Yüksek Büyümesi

ISO'nun yılda bir kez yayımladığı ISO Survey'in 2024 baskısı, bilgi güvenliği yönetimi alanında tarihsel bir büyümeyi kayıt altına almıştır. HEIC'in (2025) analizine göre: 'Geçerli sertifika sayısı neredeyse iki katına çıkarak 2023'teki 48.671'den 2024'te 96.709'a yükselmiştir. Sertifikalı alan sayısı da 179.877'ye ulaşmıştır.' Bu artış, dünya genelinde siber güvenlik ve veri korumaya verilen önceliğin belirgin biçimde büyüdüğünü doğrulamaktadır.

2024 verilerinde önemli bir metodolojik değişiklik de göze çarpmaktadır: ISO Survey ilk kez IAF CertSearch küresel veritabanından derlenen anonimleştirilmiş ve toplulaştırılmış verileri kullanmıştır. Bu metodolojik dönüşüm, belgelendirme kuruluşlarının gönüllü raporlamasına dayanan önceki yıllara kıyasla çok daha güvenilir ve kapsamlı bir veri seti ortaya koymuştur. 2023 verisindeki düşüşün gerçek bir gerilemeyi değil, eksik raporlamayı yansıttığı bu bağlamda netleşmektedir (Prozorov, 2025).

12.2 Coğrafi Dağılım ve Türkiye'nin Konumu

ISO 27001 sertifikasyonunda coğrafi dağılım incelendiğinde, Asya-Pasifik bölgesinin — özellikle Japonya, Çin ve Hindistan'ın — küresel liderliği sürdürdüğü görülmektedir. Avrupa'da ise Birleşik Krallık, Almanya ve İtalya önde gelen ülkeler arasında yer almaktadır. DISC InfoSec'in (2025) analizine göre, Polonya, Güney Kore ve ABD da son yıllarda belirgin büyüme kaydetmiştir.

Türkiye'de ISO 27001 sertifika sayısına ilişkin kamuoyuyla paylaşılmış güncel bir veri bulunmamakla birlikte, TSE'nin aktif belgelendirme programları ve BGYS eğitimlerine olan ilginin artması sertifika sayısının büyüdüğünün önemli göstergeleridir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin kamu kuruluşları için hazırladığı eşleştirme tablosu ve BTK'nın bilgi güvenliği gerekliliklerine yönelik artan düzenleyici baskı, Türkiye'de sertifikasyon talebini hızlandırmaya devam etmektedir.

12.3 2025 Geçiş Zorunluluğu ve Sektörel Etkiler

31 Ekim 2025 itibariyle tüm ISO 27001:2013 sertifikaları geçerliliğini yitirdi. BALTUM'un (2026) değerlendirmesine göre, 'BGYS'yi statik bir uyumluluk tatbikatı olarak değerlendiren kuruluşlar için bu geçiş önemli bir çalışma gerektirmiştir.' Bu geçiş sürecindeki temel zorunluluklar şunlardır: 2022 baskısı kapsamında boşluk analizi yapılması, Ek-A'daki revize kontrollere karşılık gelen uygulanabilirlik bildirgesi ve risk işleme planının güncellenmesi, kuruluş tarafından uygulanabilir seçilen yeni veya değiştirilmiş kontrollerin etkinliğinin doğrulanması.

Konfirmity'nin (2026) tespiti özellikle dikkat çekicidir: 'Sertifikasyon artık salt bir onay kutusundan ibaret değildir. Denetçiler artık kontrol etkinliğini incelemektedir. Kanıtlar, kontrollerin zaman içinde işlediğini ve riski azalttığını göstermelidir. Alıcılar da sertifikaları bir başlangıç noktası olarak kullanmakta, ardından ayrıntılı güvence artefaktları talep etmektedir. Gerçek güvenlik olmaksızın uyumluluk, kuruluşları maliyetli ihlallere maruz bırakmaktadır.'

13. BGYS, Siber Güvenlik Olgunluğu ve Diğer Çerçevelerle İlişki

13.1 NIST CSF ile Karşılaştırma

ISO 27001 ve NIST Siber Güvenlik Çerçevesi (CSF), bilgi güvenliği yönetiminin iki önemli referans çerçevesini oluşturmaktadır. Temel farkları şöyle özetlenebilir: ISO 27001, yönetim sistemi standardı olup sertifikalandırılabilirken NIST CSF, gönüllü bir çerçeve olup sertifikalandırılamamaktadır. ISO 27001 küresel kabul görürken NIST CSF öncelikle ABD merkezlidir. Bununla birlikte iki çerçeve birbiriyle örtüşen kontrol alanlarına sahip olup entegre uygulanmaları mümkündür.

13.2 ISO 27001 ve ISO 22301 Entegrasyonu

ISO 22301 İş Sürekliliği Yönetim Sistemi standardı ile ISO 27001'in entegre uygulanması, birbirini tamamlayan iki yönetim sistemi çerçevesini tek bir entegre yapı altında birleştirmektedir. ISO 27001'in A.5.30 ve A.8.16 kontrolleri, iş sürekliliği ile doğrudan ilişkilidir. Özellikle kritik altyapı işleten kuruluşlar için bu entegrasyon, hem güvenlik hem de süreklilik hedeflerini tek bir yönetim sistemi altında karşılamayı mümkün kılmaktadır.

13.3 Yapay Zeka ve Bulut Güvenliğinin BGYS'ye Etkileri

2024 yılında yürürlüğe giren AB Yapay Zeka Yönetmeliği ve bulut hizmetlerinin kurumsal BT altyapısına hâkimiyeti, BGYS kapsamını ve içeriğini köklü biçimde dönüştürmektedir. ISO

burakolgun.com

27001:2022'nin A.5.23 (Bulut Hizmetleri Güvenliği) ve A.5.7 (Tehdit İstihbaratı) kontrolleri bu dönüşümü yansıtmaktadır. Ancak yapay zeka sistemlerinin karar alma süreçlerine entegrasyonu, veri zehirleme (data poisoning) ve model çalma gibi yeni saldırı vektörleriyle birlikte ISO 27001:2022 mevcut kontrol setinin ötesinde yeni tehditler ortaya çıkarmaktadır.

ISO/IEC 27001'in 2022 sürümü baskı tarihinde büyük ölçüde ana akım haline gelmemiş olan üretici yapay zeka tehditlerini henüz kapsamamaktadır. Bu boşluğu gidermek amacıyla ISO/IEC SC 27 çalışma grubu bünyesinde yapay zeka güvenliğine yönelik yeni standartlar geliştirilmekte; ISO/IEC 42001 Yapay Zeka Yönetim Sistemi standardı ise yapay zeka sistemlerine özgü yönetim gereksinimlerini tanımlamaktadır.

14. BGYS Uygulamalarının Başarı ve Başarısızlık Faktörleri

14.1 Kritik Başarı Faktörleri

Uluslararası BGYS uygulama deneyimlerine dayanan araştırmalar, başarılı uygulamaların birkaç ortak özelliği paylaştığını ortaya koymaktadır.

- **Üst yönetim taahhüdü:** Konfirmity'nin (2026) vurguladığı üzere, 'silolaşmış yaklaşım denetimlerde başarısızlıkla sonuçlanmaktadır.' BGYS, salt BT projesi değil; üst yönetimin sahiplendiği kurumsal bir yönetim sistemidir.
- **Risk odaklı yaklaşım:** Belirleyici fark, BGYS'nin gerçek risk profilini yansıtmasıdır. Şablon uygulamalar yerine kuruluşa özgü risk değerlendirmesi, hem güvenlik etkinliğini hem de denetim başarısını artırmaktadır.
- **Kapsam doğru belirlenmesi:** Çok geniş kapsam, kaynak israfı ve yönetilemeyen bir sisteme yol açar. Çok dar kapsam ise kritik varlıkları dışarıda bırakır. Kapsam, iş riskini ve kuruluşun kapasitesini dengeleyen bilinçli bir karardır.
- **Süreklilik kültürü:** BGYS'nin yalnızca denetim döneminde aktive olan bir süreç değil, operasyonun ayrılmaz parçası olması, uzun vadeli başarının en kritik güvencesini oluşturmaktadır.

14.2 Yaygın Uygulama Hataları

BGYS uygulama hatalarından en sık görülenler şunlardır:

- **Doküman odaklı uyumluluk:** Kontrollerin kâğıt üzerinde mevcut olması ancak sahada uygulanmaması, Aşama 2 denetiminde en sık karşılaşılan başarısızlık nedenidir.
- **Güncel olmayan risk değerlendirmesi:** Tehdit ortamı sürekli değişirken risk değerlendirmesinin yıllık döngüyle güncellenmemesi, BGYS'yi gerçek riske karşı körelten yaygın bir hatadır.
- **Farkındalık eğitiminin ihmal edilmesi:** Teknik kontroller ne kadar güçlü olursa olsun, insan faktörü en zayıf halka olmayı sürdürmektedir. Yıllık zorunlu eğitimlerin önemsenerek tasarlanması zorunludur.

burakgun.com

- **Tedarikçi yönetiminin göz ardı edilmesi:** Tedarik zinciri saldırılarının giderek yaygınlaşmasıyla birlikte, üçüncü taraf güvenlik değerlendirmesinin BGYS kapsamına dahil edilmesi artık zorunluluktur.

15. Sonuç

ISO/IEC 27001 ve geniş anlamda ISO 27000 standartlar ailesi, bilgi güvenliği yönetimini sistemli, risk temelli ve ölçülebilir bir disipline dönüştüren uluslararası çerçevedir. ISO Survey 2024'ün ortaya koyduğu 96.709 geçerli sertifika ve 2018'den bu yana yüzde yüzü aşan büyüme oranı, bu çerçevenin küresel kabul gören bir yönetim standardına dönüştüğünü tartışmasız biçimde göstermektedir.

2022 revizyonu, standart için kritik bir uyum güncellemeyi temsil etmektedir: Madde 6.3'ün planlanmış değişim yönetimi gereksinimi, 11 yeni Ek-A kontrolü ve yapısal 'özellik' bazlı kontrol çerçevesi — bu değişikliklerin tamamı bulut, uzaktan çalışma, tedarik zinciri saldırıları ve yapay zeka gibi günümüz tehdit ortamının gerekliliklerine yanıt vermektedir. 31 Ekim 2025 geçiş tarihi ile birlikte artık yalnızca 2022 sürümü geçerliliğini korumaktadır.

Türkiye'de ise BGYS uygulamalarının kamu ve özel sektörde ivme kazandığı görülmektedir. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin ISO 27001 kontrolleri ile Bilgi ve İletişim Güvenliği Rehberi'ni eşleştiren tablosu, KVKK'nın teknik tedbir gereksinimleri ve TSE'nin aktif belgelendirme programları, Türkiye'nin bilgi güvenliği yönetim kapasitesini uluslararası standartlara taşıma yolundaki kararlı adımlarını somutlaştırmaktadır.

Sonuç olarak, ISO 27001 sertifikasyon süreci yalnızca bir uyumluluk ödevi değil; bilgi varlıklarını koruyan, iş sürekliliğini güvence altına alan ve paydaşlarla güven inşa eden stratejik bir yönetim yatırımıdır. Konfirmity'nin (2026) keskin tespiti bu sonucu özetlemektedir: 'Gerçek güvenlik olmaksızın uyumluluk, kuruluşları maliyetli ihlallere maruz bırakmaktadır.' BGYS'nin yaşayan ve gelişen bir sistem olarak yönetilmesi, dijital çağda sürdürülebilir bilgi güvenliğinin tek gerçekçi güvencesini oluşturmaktadır.

Kaynakça

A-LIGN. (2025, April 3). Unveiling ISO 27001:2022: The 9 critical updates you need to know. https://www.a-lign.com/articles/unveiling-iso-270012022-the-9-critical-updates-you-need-to-know

BALTUM. (2026, March 12). ISO 27001:2022 transition — What you need to know before the deadline. https://baltum.org/blog/iso-27001-2022-transition-guide/

BTGM. (2024). ISO 27001 Bilgi Güvenliği Yönetim Sistemi. T.C. Ticaret Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü. https://btgm.ticaret.gov.tr/haberler/iso-27001-bilgi-guvenligi-yonetim-sistemi

CTR. (tarihsiz). ISO 27001 Bilgi Güvenliği Yönetim Sistemi. https://belgelendirme.ctr.com.tr/iso-27001.html

ÇŞİDB. (tarihsiz). TSE ISO IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi. T.C. Çevre, Şehircilik ve İklim Değişikliği Bakanlığı. https://cbs.csb.gov.tr/tse-iso-iec-27001-2017-bilgi-guvenligi-yonetim-sistemi-88763

burakgun.com

Denetci.org. (2025, September 14). Bilgi ve İletişim Güvenliği Rehberi ile ISO 27001 Kontrolleri Eşleştirme Tablosu. https://denetci.org/bilgi-ve-iletisim-rehberi-guvenligi-ile-iso-27001-kontrolleri-eslestirme-tablosu/

DISC InfoSec Blog. (2025, May 12). Historical data on the number of ISO/IEC 27001 certifications by country. https://blog.deurainfosec.com/historical-data-on-the-number-of-iso-iec-27001-certifications-by-country-across/

DSR Belgelendirme. (2026, March 6). ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi Nedir? https://dsrbelgelendirme.com.tr/iso-27001-belgesi/

DSR Belgelendirme. (2026). ISO 27001 Doküman Listesi. https://dsrbelgelendirme.com.tr/iso-27001-dokuman-listesi/

Ekşi, B. (2023, August 13). ISO 27000 ailesi hangi standartlardan oluşur. https://www.burakeksi.com/iso-27000-ailesi-hangi-standartlardan-olusur/

goteleport.com. (2025). ISO 27001:2022 requirements explained for 2025. https://goteleport.com/blog/iso-iec-27001-2022-explained/

HEIC. (2025, October 21). ISO 27001 certifications nearly double in 2024 as global organizations prioritize cybersecurity. https://heic.eu/iso-27001-certifications-nearly-double-in-2024-as-global-organizations-prioritize-cybersecurity/

IBM. (2024). Cost of a data breach report 2024. IBM Security. https://www.ibm.com/reports/data-breach

isodestek.com. (2025, January 20). ISO/IEC 27001 BGYS için zorunlu dokümante edilmiş bilgi. https://isodestek.com/iso-iec-27001-bgys-icin-zorunlu-dokumante-edilmis-bilgi/

isonedir.com. (tarihsiz). ISO 27001 nedir, ISO 27001 belgesi nasıl alınır? https://www.isonedir.com/iso-27001-nedir/

ISO. (2022). ISO/IEC 27001:2022 — Information security management systems. International Organization for Standardization. https://www.iso.org/standard/27001

Johanson Group. (2024). ISO 27001:2022 transition guide. https://www.johansonllp.com/iso-27001-transition-guide

Konfirmity. (2026). ISO 27001: What changed in 2026 — a guide for busy teams. https://www.konfirmity.com/blog/iso-27001-what-changed-in-2026

KUM Eğitim Danışmanlık. (tarihsiz). ISO27001 Bilgi Güvenliği standardında Varlık Yönetimi. https://www.kum.com.tr/iso27001-bilgi-guvenligi-standardinda-varlik-yonetimi

KUM Eğitim Danışmanlık. (2021). ISO 27000 standartlar serisi kaç standarttan oluşuyor? https://www.kum.com.tr/blog/iso-27000-standartlar-serisi-kac-standarttan-olusuyor

LRQA. (2025, May 13). Preparing for ISO 27001:2022 transition by October 2025. https://www.lrqa.com/en-us/insights/articles/preparing-for-iso-270012022-transition-by-october-2025/

onlinestandart.com. (2025, July 1). ISO 27001 Bilgi Güvenliği Kitabı Bölüm 2 — İşletmelere Rehber. https://onlinestandart.com/rehber/iso-27001-bilgi-guvenligi-yonetim-sistemi-bolum-2/

burakeksi.com

Polat, Ç. (2026, March 16). Bilgi Güvenliği Yönetim Sistemi (BGYS) Nedir? https://www.cagripolat.com/iso27001/bilgi-guvenligi-yonetim-sistemi-bgys-nedir

Prozorov, A. (2025, October 2). ISO Survey 2024: ISO/IEC 27001 certificates. Patreon. https://www.patreon.com/posts/iso-survey-2024-140260314

secureframe.com. (2025, August 25). ISO 27001:2022 and ISO 27002:2022 explained: How to comply before October 2025 deadline. https://secureframe.com/blog/iso-27001-2022

SGS. (2024, May 10). ISO/IEC 27001 transition: What you should know. https://www.sgs.com/en-us/news/2024/05/iso-iec-27001-transition-what-you-should-know

sigmateknoloji.com.tr. (2022). ISO 27001 Bilgi Güvenliği Yönetim Sistemi. https://sigmateknoloji.com.tr/iso-27001-bilgi-guvenligi-yonetim-sistemi/

TSE. (2026, January 15). TS EN ISO/IEC 27001:2023 Bilgi Güvenliği Yönetim Sistemi Temel Eğitimi. https://www.tse.org.tr/duyuru/tse-bgys-egitimleri-subat-2026/

TSE. (tarihsiz). TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) Belgelendirmesi. https://www.tse.org.tr/bilgi-guvenligi-yonetim-sistemi-bgys-belgelendirmesi-ts-iso-iec-27001/

Vertacert. (2025, December 26). ISO 27001 Belgesi Nedir? BGYS kurulumu, 2022 revizyonu ve fiyatları. https://www.vertacert.com/iso-27001-bilgi-guvenligi-yonetim-sistemi/

Yüksektepeli, O. (2013). ISO 27000 ailesi standartları nedir? https://www.mshowto.org/iso-27000-ailesi-standartlari-nedir.html

burakolgun.com