BİLGİ GÜVENLİĞİ DERSİ
3. HAFTA

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

DR. ÖĞR. ÜYESİ FURKAN ATLAN

Kurumsal Bilgi Güvenliği

Kurumsal bilgi güvenliği, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak tanımlanabilir.

Kurumsal Bilgi Güvenliği

Kurumsal bilgi güvenliği; insan, eğitim, teknoloji gibi birçok faktörün etki ettiği ve tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır.

Bu açıdan bakıldığında, bilgi güvenliği sadece teknik süreçlerden meydana gelen bir iş değildir; kurumun her bir çalışanının katkısını ve katılımını gerektiren bir süreçtir

ISO Nedir?

ISO (International Organization for Standardization), farklı alanlarda dünya çapında standartlar geliştirmek amacıyla kurulmuş bir sivil toplum organizasyonudur.

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanan bir standarttır.

IEC, International Electrotechnical Commission ifadesinin kısaltmasıdır. ISO, standartları belirlerken teknik ayrıntıları ve teknik standartları IEC yardımı ile belirler. Daha doğrusu bu işi onlara bırakır. Bu nedenle BGYS'nin bir standart olarak belirlenmesinde ve belirtilmesinde kullanılan tam isim ISO/IEC 27001'dir.

ISO 27002 BGYS KONTROLLERİ

ISO 27001, BGYS ile ilgili kavramsal çerçeveye ışık tutarken yani teorik bilgileri ve tavsiyeleri içerirken, ISO 27002 (BGYS Ek Kontroller) ise bu teorik bilgilerin ve tavsiyelerin pratikte nasıl uygulanacağından bahsetmektedir.

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO 27000 ailesi aslında bilgi güvenliği ve onun diğer başlıklarıyla (risk yönetimi, ek kontrolleri vb.) ilgilenen büyük bir standardizasyon ailesidir.

ISO 27001 gereksinimleri ifade ederken, onun nasıl uygulanacağı ise ISO 27002'de belirtilmiştir.

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO, yayınladığı farklı standartları (9001 Kalite Yönetim Sistemi, 14001 Çevre yönetim sistemi, 18001 iş sağlığı ve güvenliği yönetim sistemi vb.) belirli bir süreden sonra güncellemektedir.

Şu anda ISO 27001 BGYS için kullanılan versiyon ise 2022 yılına ait standarttır.

ISO 27001:2022 versiyonunda bir önceki versiyonuna (2013) göre önemli bir değişiklik gerçekleşmiştir.

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

- **ISO/IEC 27001:2013** Bilgi teknolojisi – Güvenlik teknikleri – Bilgi Güvenliği yönetim sistemleri - gereksinimler
- **ISO/IEC 27001:2022** Bilgi güvenliği, siber güvenlik ve gizlilik koruması –Bilgi Güvenliği yönetim sistemleri - gereksinimler

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO/IEC 27001:2022 Yapısı

Madde 4

- İç ve Dış Hususlar
- İhtiyaç ve beklentiler
- BGYS Kapsamı
- Bilgi Güvenliği Yönetim Sistemi

Madde 5

- Liderlik & Taahhüt
- Politika
- Roller ve Sorumluluklar

Madde 6

- Risk ve Fırsatlara yönelik faaliyetler
- BG Hedefleri
- Değişikliklerin Planlanması

Madde 7

- Kaynaklar
- Farkındalık
- Yetkinlik
- İletişim
- Dokümante Bilgi

Madde 8

- İşletimsel Planlama ve Kontrol
- Bilgi Güvenliği Risk Değerlendirme
- Bilgi Güvenliği Risk İşleme

Madde 9

- İzleme & Ölçme
- İç Tetkik
- Yönetimin Gözden Geçirmesi

Madde 10

- Sürekli İyileştirme
- Uygunsuzluk ve Düzeltici Faaliyet

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO 27001:2022'de siber güvenliğin bir başlık ve konsept olarak BGYS'ye dahil edilmesiyle birlikte bu standardın yönü ve ağırlığı siber güvenliğe doğru kaymıştır.

Siber güvenliğin dahil edilmesinin yanı sıra KVKK'ya uygun bazı yeni maddeler de eklenerek, BGYS standardı en güncel halini almıştır.

Not: ISO 27001:2013 BGYS standardı, bazı siber güvenlik uzmanları tarafından «light» olarak değerlendirilirdi. Şu anda ise teknik anlamda siber güvenliğe daha kapsamlı bir bakış sunmaktadır.

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO 27001:2022 versiyonu ile birlikte 14 madde, 4 ana başlık alt

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO 27001:2013'teki 114 olan kontrol bileşeni, 2022 versiyonunda 93 olmuştur. Kontroller silinmemiştir. Aksine 11 adet

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

11 Yeni Kontrol

Teknolojik Kontroller

- A.8.9 – Konfigürasyon yönetimi
- A.8.10 – Bilgi silme
- A.8.11 – Veri maskeleme
- A.8.12 – Veri sızıntısını önleme
- A.8.16 – İzleme faaliyetleri
- A.8.23 – Web filtreleme
- A.8.28 – Güvenli kodlama

Organizasyonel Kontroller

- A.5.7 – Tehdit İstihbaratı
- A.5.23 - Bulut hizmetlerinin kullanımı için bilgi güvenliği
- A.5.30 - İş sürekliliği için BİT (ICT) hazırlığı

Fiziksel Kontroller

- A.7.4 – Fiziksel güvenlik izleme

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller – Konfigürasyon Yönetimi:

Bu kontrol, uygun bir güvenlik düzeyi sağlamak ve herhangi bir yetkisiz değişikliklerden kaçınmak adına teknolojiniz için tüm güvenlik yapılandırması döngüsünü yönetmenizi gerektirir. Buna yapılandırma tanımı, uygulama, izleme ve inceleme dahildir.

ITSM (Information Technologies Service Management) kontrolüdür. Aynı zamanda ISO 20000 standardıdır.

ITSM, IT hizmetlerini planlama, tasarlama, yönetme ve geliştirme süreçlerinin bütünüdür.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller – Bilgi Silme ve Veri Maskeleme:

Bu kontrol, hassas bilgilerin sızmasını önlemek, gizlilik ve diğer gereksinimlerle uyumluluğu sağlamak için artık gerekmediğinde verileri silmenizi gerektirir. Bu, BT sistemlerinizdeki, çıkarılabilir medyadaki veya bulut hizmetlerindeki silmeyi içerebilir.

KVKK'nın yürürlüğe girmesiyle birlikte verinin bütünlüğü ve gizliliği açısından eklenmiş bir kontrol yapısıdır.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller –Veri Maskeleme:

Bu kontrol, hassas bilgilerin açığa çıkmasını sınırlamak için erişim kontrolü ile birlikte veri maskelemeyi kullanmanızı gerektirir. Bu, öncelikle kişisel veriler anlamına gelir, çünkü bunlar gizlilik düzenlemeleri tarafından yoğun bir şekilde düzenlenir, ancak diğer hassas, gizlilik dereceli veri kategorilerini de içerebilir.KVKK'nın yürürlüğe girmesiyle birlikte verinin bütünlüğü ve gizliliği açısından eklenmiş bir kontrol yapısıdır.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller – Veri Sızıntısını Önleme:

Veri Sızıntısını Önleme (Data Loss Prevention-DLP), hassas verilerin güvenli olmayan şekilde paylaşımı, aktarımı veya kullanımının tespit edilmesi ve önlenmesi için bir güvenlik çözümüdür.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller - İzleme Faaliyetleri:

Bu kontrol, olağandışı faaliyetleri tanımak ve gerekirse uygun olay yanıtını etkinleştirmek için sistemlerinizi izlemenizi gerektirir. Bu, BT sistemlerinizin, ağlarınızın ve uygulamalarınızın izlenmesini içerir.

Güvenlik Bilgi ve Olay Yönetimi (Security Information and Event Management-SIEM), özünde bir veri toplayıcı, arama ve raporlama sistemidir. SIEM, ağ ortamından çok büyük miktarda veri toplar(log), bu verileri birleştirir ve insanlar tarafından erişilebilir hale getirir. Verileri kategorilere ayırır ve düzenleyerek , güvenlik kuralları yazmaya uygun

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller – Web Filtreleme:

Url Content Filtering, belirli kategorilerdeki web sitelerinin tamamına ya da belirli url'lerine erişimin engellenmesini içerir.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Teknolojik Kontroller – Güvenli Kodlama:

Masaüstü, mobil ya da web sitesi uygulamasının daha yazılma aşamasında iken güvenlik açıklarının ve muhtemel saldırıların göz önünde bulundurularak tasarlanması.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Organizasyonel Kontroller - Tehdit İstihbaratı:

Kurumun, kendi belirlediği ekipler ile kendi sistemlerine sızma testleri düzenleyip, sistemin açıklarını, zafiyetlerini önceden test etmesi.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Organizasyonel Kontroller – Bulut Hizmetlerinin Kullanımı için Bilgi Güvenliği:

Bu madde daha önce zaten 27010 kapsamında bir standart idi. Ancak, ISO/IEC 27001 kapsamına dahil edilmiştir.

Bu kontrol, buluttaki bilgilerinizin daha iyi korunması için bulut hizmetlerinde güvenlik gereksinimleri belirlemenizi gerektirir. Buna bulut hizmetlerinin satın alınması, kullanılması, yönetilmesi ve kullanımının sonlandırılması dahildir.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Organizasyonel Kontroller – İş Sürekliliği için BİT Hazırlığı:

Bu kontrol, Bilgi ve İletişim Teknolojinizin (BİT), gerekli bilgi ve varlıkların gerektiğinde kullanılabilir olması için olası kesintilere hazır olmasını gerektirir. Buna hazırlık planlama, uygulama, bakım ve test dahildir.

Sistemlerinizin esnekliğini ve yedekliliğini sağlayan çözümlere yatırım yapmadıysanız, bu tür bir teknolojiyi siteminize dahil etmeniz gerekebilir. Bu çözümlerin, risk değerlendirmenize ve verilerinizin ve sistemlerinizin kurtarılması için ne kadar hızlı ihtiyaç duyduğunuza göre

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Fiziki Kontroller – Fiziksel Güvenlik İzleme:

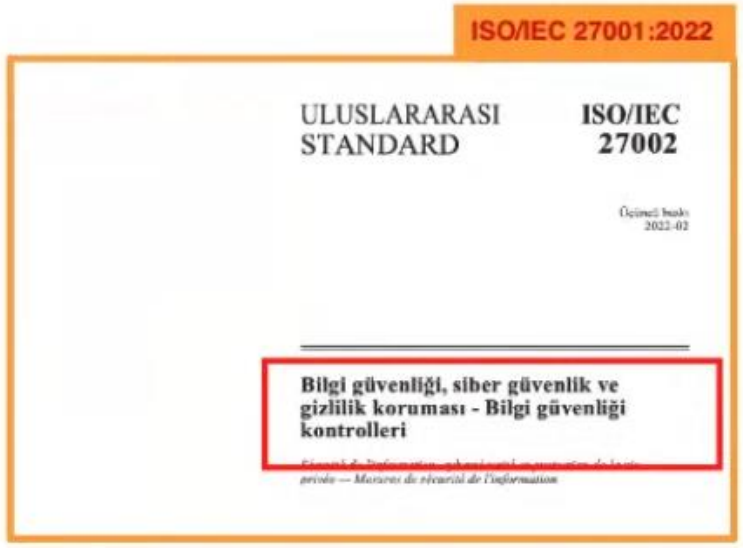
Bu kontrol, yalnızca yetkili kişilerin bunlara erişmesini sağlamak için hassas alanları / bölgeleri izlemenizi gerektirir. Bu, ofislerinizi, üretim tesislerinizi, depolarınızı ve diğer binalarınızı içerebilir.

Örneğin; risklerinize bağlı olarak alarm sistemleri veya video izleme uygulamanız gerekebilir; ilgili alanı / bölgeyi gözlemleyen bir nöbetçi çalışan gibi teknoloji dışı bir çözüm uygulamaya da karar verebilirsiniz.

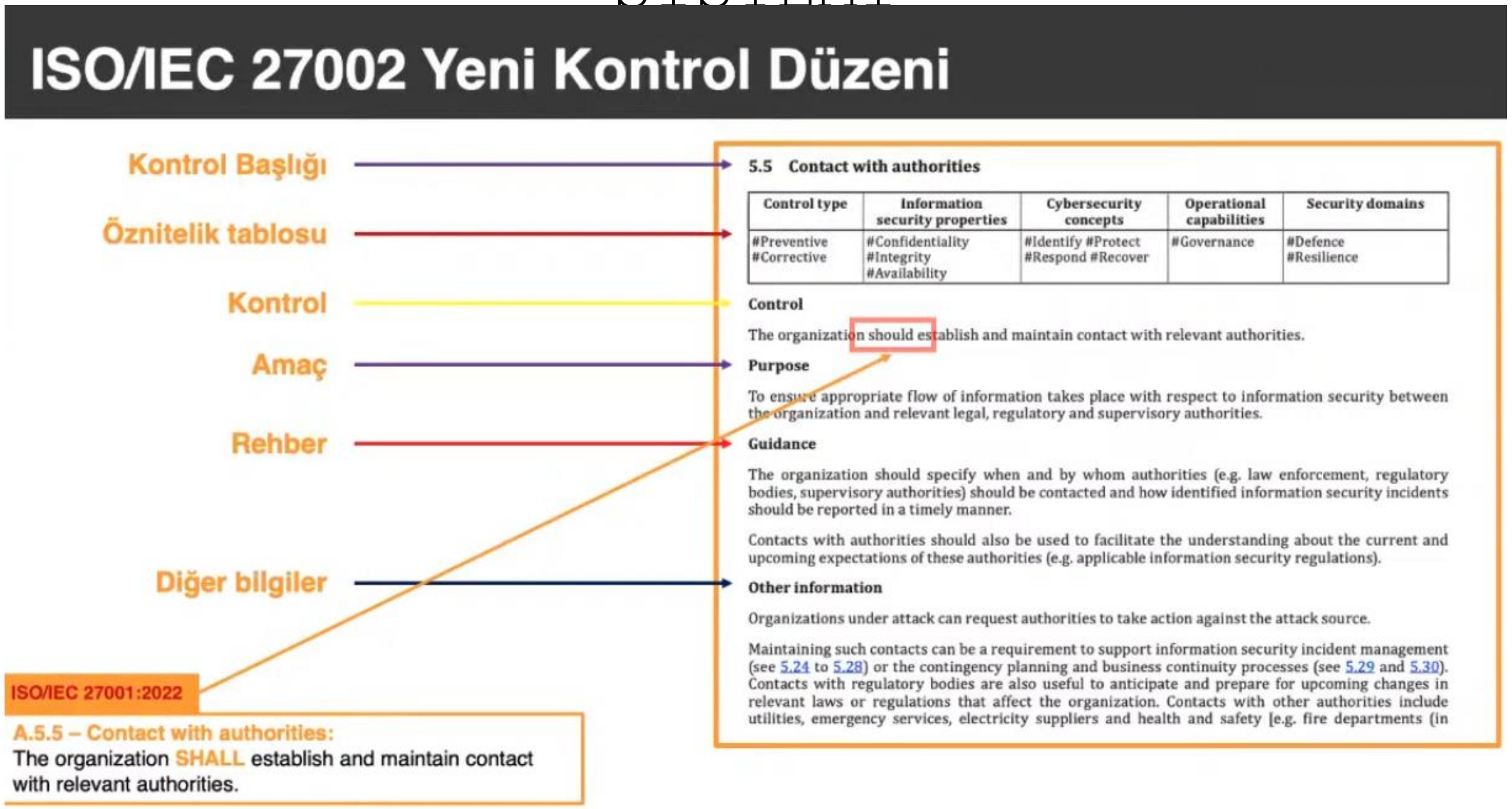
ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO/IEC 27002 Adındaki Değişiklik

- **ISO/IEC 27002:2013** Bilgi teknolojisi – Güvenlik teknikleri – Bilgi Güvenliği kontrolleri için uygulama kuralları
- **ISO/IEC 27002:2022** Bilgi güvenliği, siber güvenlik ve gizlilik koruması –Bilgi Güvenliği kontrolleri



İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ



İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO/IEC 27002 Öznitelik Tablosu

5.5 Contact with authorities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Control

The organization should establish and maintain contact with relevant authorities.

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

Guidance

The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

Other information

Organizations under attack can request authorities to take action against the attack source.

Maintaining such contacts can be a requirement to support information security incident management (see 5.24 to 5.28) or the contingency planning and business continuity processes (see 5.29 and 5.30). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety [e.g. fire departments (in

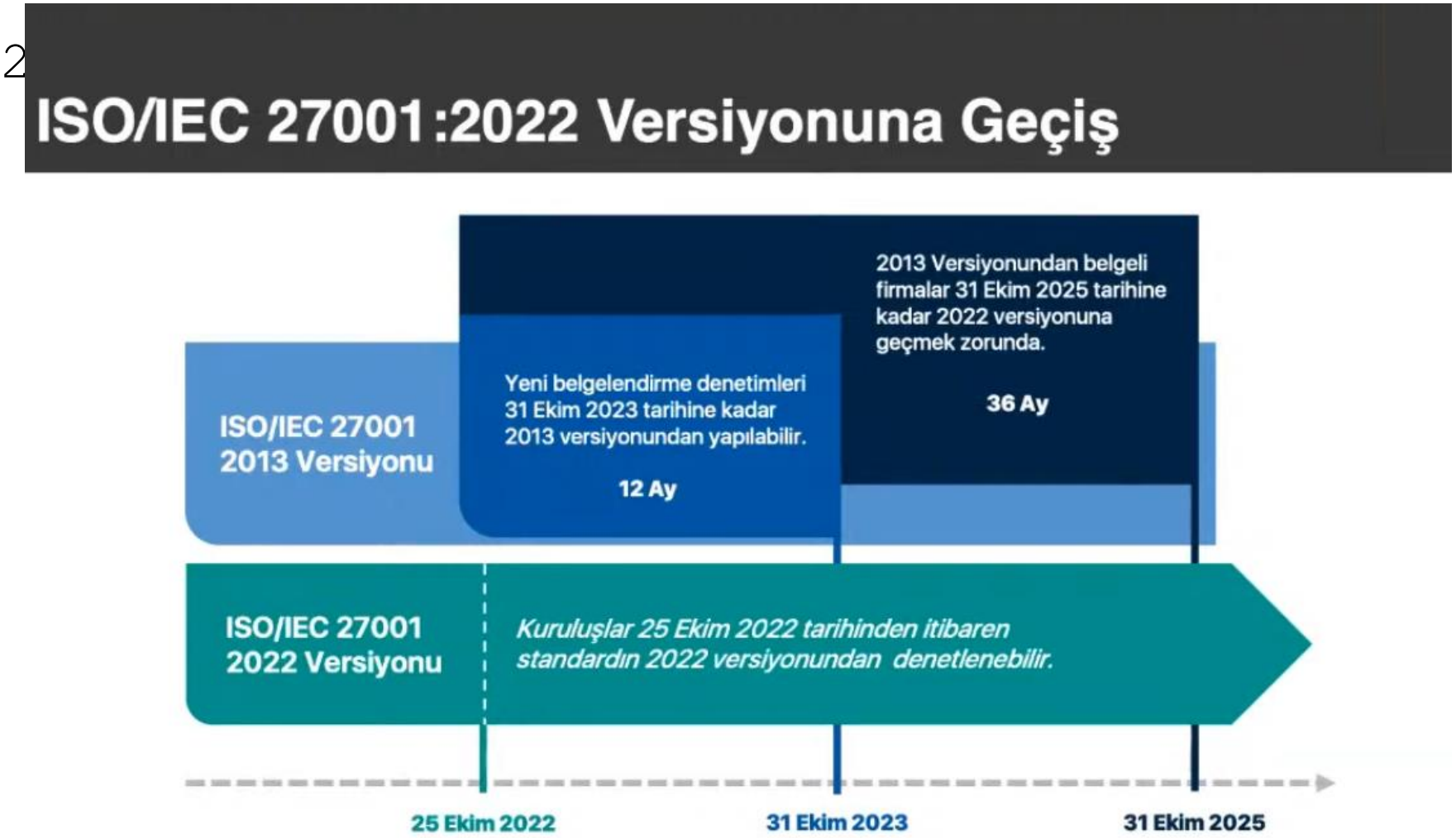
Kontroller 5 nitelik türüne göre etiketlenmektedir.

Nitelik Kategorisi	Nitelik Etiketleri
Kontrol Tipi	#Önleyici #Tespit Edici #Düzeltici
Bilgi Güvenliği Özellikleri	#Gizlilik #Bütünlük #Erişebilirlik
Siber Güvenlik Kavramları	#Belirleme #Koruma #Tespit Etme #Müdahale Etme
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 #Bilgi güvenliği güvencesi
Güvenlik Alanları	#Yönetişim ve Ekosistem #Koruma #Savunma #Dayanıklılık

Öznitelik tablosunun kullanımı zorunlu değildir.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO 27001:2022 versiyonuna geçiş için 31 Ekim 2025 tarihine kadar süre tanınmıştır. Dileyen olursa şu anda da 202



ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO Sertifikası Nasıl Alınır?

Ülkemizde, TÜRKAK (TÜRK AKREDİTASYON KURUMU) tarafından onaylanmış ve ISO 27001 sertifikasını verme yetkinliğine sahip firmalara başvurularak süreç başlatılır.

ISO 27001 Sertifikasının geçerliliği 3 yıldır.

ISO 27001 Sertifikası almak;

Küçük ve orta vadeli firmalar için 1.5 ay; büyük ölçekli firmalar için 4-6 ay arasında değişir.

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

İSO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

GAP (Boşluk) Analizi: Mevcut durumunuz ile olmak istediğiniz durum arasındaki karşılaştırmadır.

SOA (Service Oriented Archictecture-Servis Odaklı Mimari): Bilgisayar sistemlerinin işlevselliklerinin is süreçleri etrafında gruplaştırılarak sistem geliştirilmesi.

ÖRNEK BİR SERTİFİKASYON FİRMASI

ISO/IEC 27001 Geçiş Sürecinde Uygulama Desteği

Kuruluşunuzda başta aşağıdaki faaliyetler olmak üzere birçok sürecin dijitalleşmesini sağlar:

- Süreç Yönetimi
- Varlık Yönetimi
- Risk Yönetimi
- Doküman Yönetimi
- Uygulanabilirlik Bildirgesi (SOA)
- Bilgi Güvenliği Hedefleri
- Performans Yönetimi
- İç Denetim
- Yönetimin Gözden Geçirmesi
- Uygunsuzluk ve Düzeltici Faaliyet Yönetimi
- Kişisel Veri Envanter Yönetimi

KAYNAKLAR

- Safa PAKSU – Linkedin
- Ömer KILINÇ - CFECERT Belgelendirme (https://cfecert.com/tr)