# Bilgi Güvenliği Standartları ve Bilgi Güvenliği Hedefleri

## ISO 2700X

# # Bilgi Güvenliği Standartları

- Veri ve bilginin meta gibi alınıp satıldığı zamanlarda, onları korumak esastır. Bunu yapmanın bir yolu, ISO/IEC 2700x serisi bilgi güvenliği standartlarına dayalı bilgi güvenliği yönetimini uygulamaktır.
- ISO 27000 standartları her geçen gün büyüyen ISO/IEC ISMS standart ailesinin bir parçasıdır. ISO 27000 standart serisi; ISO 27001, ISO 27002 ISO 27003… vb Bilgi teknolojisi- Güvenlik teknikleri- Bilgi güvenliği yönetimi sistemleri-genel bakış ve tanımlar başlıklarını kapsayan uluslararası standartları içeren bir standart ailesidir.
- Sertifikasyon olarak ISO 27001 standardının sertifikasyonu olup ISO 27001 Belgesi vardır.

# Bilgi Güvenliği Standartları: ISO 2700X Standart Ailesi

- ISO 2700x serisindeki bilgi güvenliğine yönelik bireysel standartlar, bilgi güvenliği alanındaki çeşitli konuları ele alır. Örneğin, uluslararası standart, ISO 27001 Bir bilgi güvenliği yönetim sistemini (BGYS), ISO 27701 bir veri koruma yönetim sistemini ele alır. ISO 27017, bulut bilişim için bilgi güvenliği önlemleri hakkında rehberlik, ISO 27005 ise bilgi güvenliği risk yönetimi için yönergeler sağlar.

# Bilgi Güvenliği Standartları:

- Tüm sektörlerdeki şirketler, bilgi güvenliği için bu standartların sistematik olarak yapılandırılmış yaklaşımından yararlanabilir. Gizli verilerin kaybolmaya ve kötüye kullanıma karşı korunmasını sağlar ve (potansiyel) tehditlerin güvenilir bir şekilde belirlenmesine ve azaltılmasına yardımcı olur. Yaklaşım, kurumsal BT sistemlerinin kullanılabilirliğini sağlamaya yardımcı olur, böylece iş süreçlerinin, BT ve süreç maliyetlerinin optimizasyonuna ve iş ve sorumluluk risklerinin en aza indirilmesine katkıda bulunur.

# Bilgi Güvenliği Standartları:

- ISO 27000 standartları, Uluslararası Standardizasyon Örgütü'nün ve Uluslararası Elektroteknik Komisyonu'nun ortaklığında kurulan Birleşik Teknik Komite'ye bağlı bir alt komite tarafından geliştirilmektedir. Şimdi bu standartları tanıyalım.

# Bilgi Güvenliği Standartları

**TS ISO/IEC 27001 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemi – Gereksinimler (Information technology - Security techniques - Information security management systems – Requirements) Standardı?**

- ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ana standardı olup Sistem kurulumu ve Belgelendirme bu standart üzerinden yapılmaktadır. Genel olarak ISO 27001 standardı aşağıdaki amaçları gerçekleştirmektedir.

# ISO 27001 standardı

- Kurumun / kuruluşun bilgi güvenlik risklerini, bilgi varlıklarına yönelik tehditleri, varlıkların açıklıklarını sistematik olarak denetlemek;
- Risk işleme planları, artık risklerin transferleri ile tutarlı bilgi güvenliği kontrollerini tanımlamak ve gerçekleştirmek, riskleri kabul edilebilir seviyeler çekmek
- Bilgi güvenliği kontrollerinin sürekliliğini bilgi güvenliği esaslarına göre sağlamak üzere yönetim süreçlerini kabul etmek ve uygulamak

# Bilgi Güvenliği Standartları

**TS ISO/IEC 27002 Bilgi Teknolojileri – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemi için Uygulama Kodları (Information technology - Security techniques - Code of practice for information security management) Standardı?**

- ISO 27002 Bilgi Güvenliği Yönetim Sistemi için Uygulama Kodları Standardı ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ikinci standardı olup ISO 27001 Bilgi Güvenliği Yönetim Sistemi ne göre istem kurmuş firmaların performanslarını arttırmak için uyguladıkları bir standarttır. Genel olarak ISO 27002 standardı aşağıdaki amaçları gerçekleştirmektedir.

# ISO 27002 standardı

- Risklerin değerlendirilmesi
- Güvenlik politikalarının hazırlanması
- Kurumların güvenlik yönetimi organizasyonlarının kurulması
- Varlık yönetiminin kurulması
- Kurum insan kaynaklarının, alt yüklenici veya dış kaynak çalışanlarının yönetimi
- Fiziksel ve çevresel güvenliklerin sağlanması
- Erişim kontrollerinin denetlenmesi
- Güvenlik uygulamaları için kurumsal gelişim, edinme ve gereksinimlerin karşılanması
- Olay ihlal yönetiminin kurulması
- İş sürekliliği prosedür veya planlarının hazırlanması
- Teknik ve yasal mevzuata uyumluluk

# Bilgi Güvenliği Standartları

**TS ISO / IEC 27003 Bilgi Teknolojileri – Güvenlik Teknikleri - Güvenliği Yönetim Sistemi için Uyarlama, gerçekleştirme Kılavuzu (Information Technology - Security techniques - Information security management system implementation guidance) ?**

- ISO 27003 Standardı Ocak 2010'da yayınlanmıştır ve kılavuz standarttır. Genel bir standarttır ve zorunluluk yoktur. ISO 27001 Standardına göre sistem kurarken veya sistemin sürekliliğini sağlarken aşağıdaki işlemler için genel bir çerçeve çizer ve yardımcı olur.

# ISO 27003 Standardı

- Sunu
- Kapsam
- Terimler tanımlar
- Standardın yapısı
- BGYS projesini uygulama, kabul etme ve onaylama
- BGYS kapsam ve politikasını tanımlama
- Kurum analizi yapma
- Risk değerlendirme ve işleme planlarını yönetme
- BGYS tasarımı

# Bilgi Güvenliği Standartları

**TS ISO/IEC 27004 Bilgi Teknolojileri – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemi – Ölçekler, Raporlar Standardı (Information technology -- Security techniques -- Information security management -- Measurement) ?**

- ISO 27004 standardı Aralık 2009'da yayınlanmıştır. Genel bir standarttır ve zorunluluk yoktur. ISO 27001 Standardına göre sistem kurarken veya sistemin sürekliliğini sağlarken aşağıdaki işlemler için yardımcı olur.

# ISO 27004 standardı

- BGYS ölçeklerine bakış
- Yönetim karşılıkları
- Ölçü ve ölçekleri geliştirmek
- Ölçme işlemleri
- Veri analizi ve ölçüm sonuçlarının raporlanması
- BGYS ölçüm programlarını değerlendirmek ve iyileştirmek

# Bilgi Güvenliği Standartları

**TS ISO / IEC 27005 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemlerin Risk Yönetimi Standardı (2008 Information technology -- Security techniques -- Information security risk management) ?**

- ISO/IEC 27005 Bilgi Güvenliği Yönetim Sistemi Risk Yönetim Standardı 2008 yılında yayınlanmıştır. Kurumların risklerini değerlendirmek amacı ile bir çerçeve sunar. Genel bir kapsamda hazırlanmıştır. Özel, adlandırılmış, zorunlulukları belirlenmiş bir yaklaşıma sahip değildir. ISO 27001 Standardına göre sistem kurarken risk değerlendirmelerinde ISO 27005 standardından yararlanılabilir.

# Bilgi Güvenliği Standartları

**TS ISO/IEC 27006 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemlerin Denetim ve Belgelendirilmesi için Şartlar Standardı**

**(Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems) ?**

- TS ISO / IEC 27006 Bilgi Güvenliği Denetim ve Belgelendirme için Şartlar Standardı
- Genel olarak ISO 27001 standardına göre sistem kuran veya sürekliliğini sağlayan firmalar şirketlerin dışında ISO 27001 standardına göre akrediteli olarak Belgelendirme denetim gözetim hizmeti veren ISO 27001 Belgelendirme kuruluşlarını ilgilendiren ve kapsam belirleme, denetim adam gün , vb aşağıdaki konuları içeren bir standarttır.

# ISO 27001 standardı

- Belgelendirme kapsamı
- Geçerli referanslar
- Terimler ve tanımlar
- İlkeler
- Genel gereksinimler
- Yapısal gereksinimler
- Kaynak gereksinimleri
- Bilgi gereksinimleri
- Süreç gereksinimleri
- Sertifikasyon kuruluşları için yönetim sistem gereksinimleri

# Bilgi Güvenliği Standartları

**TS ISO/IEC 27799 Sağlık Bilişimi Bilgi Güvenliği Yönetim Sistemi Sağlık Kuruluşları için ISO 27002 ( Health informatics - Information security management in health using ISO/IEC 27002) ?**

- TS ISO / IEC 27799 Sağlık Bilişimi Bilgi Güvenliği Yönetim Sistemi Sağlık Kuruluşları için ISO 27002 Standardı ISO 27002 standardının sağlık sektörü ile ilgili uygulamalarına yardımcı olması için hazırlanmış genel bir standarttır ve zorunlu değildir.

# Bilgi Güvenliği Standartları

**TSE GUIDE 13268-1 TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) belgelendirmesi için gereksinimler ve hazırlık kılavuzu ?**

- ISO 27001 standardına göre akrediteli olarak Belgelendirme denetim gözetim hizmeti veren ISO 27001 Belgelendirme kuruluşlarını ilgilendiren belgelendirme denetimine hazırlık ve belgelendirme gerekliliklerini ortaya koyan zorunlu olmayan bir standarttır. PLANLA - UYGULA - KONTROL ET - ÖNLEM AL birinci, ikinci veya üçüncü taraf denetçiler veya denetim dışında uygulamak isteyenler için hazırlanan BGYS için kullanılabilen ve bir BGYS'nin tesis edilmesi, gerçekleştirilmesi, izlenmesi, gözden geçirilmesi ve geliştirilmesi için kılavuz standarttır.

# Bilgi Güvenliği Standartları

**TSE GUIDE 13268-2 TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) gerçekleştirmelerinin etkinliğinin ölçülmesi kılavuzu ?**

**TSE GUIDE 13268-2 kılavuz standardı**

- ISO 27001 standardına göre akrediteli olarak Belgelendirme denetim gözetim hizmeti veren ISO 27001 Belgelendirme kuruluşlarını ilgilendiren Bilgi Güvenliği Yönetim Sisteminin gerçekleştirilmesinin etkinliğinin ölçülmesi için kılavuzluk eden zorunlu olmayan bir standarttır. TSE GUIDE 13268-2 Standardı UYGULA - ÖNLEM AL KONTROLÜ GERÇEKLEŞTİRME TAVSİYESİ TS ISO/IEC 17799'daki denetimlerin gerçekleştirilmesi konusunda tavsiye ve yorum yapılması; bu tavsiye denetimleri gerçekleştirirken ya da gerçekleştirmeyi denetlerken herhangi birisi tarafından kullanılabilir.

# Bilgi Güvenliği Standartları

**TSE Guide 13268-3: TS ISO/IEC 27001 e Göre Bilgi Güvenliği Yönetim Sistemi (BGYS) Denetimine Hazırlık Kılavuzu ?**

**TSE GUIDE 13268-3 kılavuz standardı**

- ISO 27001 standardına göre akrediteli olarak Belgelendirme denetim gözetim hizmeti veren ISO 27001 Belgelendirme kuruluşlarını ilgilendiren Hangi prosesleri koymalıyım ve Hangi denetimleri yapmalıyım gibi soruların cevabının aranması gereken zorunlu olmayan bir standarttır TSE GUIDE 13268-2 standardı PLANLA - UYGULA - KONTROL ET - ÖNLEM AL BOŞLUK ANALİZİ BGYS prosesleri ve TS ISO/IEC 17799 denetimleri için "Denetim için hazırlık" uyum kontrolü ve boşluk analizi standardıdır.

# Bilgi Güvenliği Standartları

**TSE GUIDE 13268-4 (BIP 0073) TS ISO/IEC 27001'i esas alan bilgi güvenliği yönetim sistemi (BGYS) kontrollerinin gerçekleştirilmesi ve denetlenmesi kılavuzu?**

**TSE GUIDE 13268-3 kılavuz standardı**

- ISO 27001 standardına göre akrediteli olarak Belgelendirme denetim gözetim hizmeti veren ISO 27001 Belgelendirme kuruluşlarını ilgilendiren Bilgi Güvenliği Yönetim Sistemi kontrollerinin gerçekleşmesi ve denetlenmesi için yardımcı olan bir kılavuz standarttır. ETKİNLİĞİNİN ÖLÇÜLMESİ Güvenlik düzenlemelerinin ölçülmesinde kullanılan farklı metotları bir araya getirir, BGYS proseslerinin ve denetimlerinin başarısını ölçmek için ölçü araçlarının ve metotlarının geliştirilmesi konusunda bilgi verir ve kılavuzluk eder.

# Bilgi Güvenliği Standartları

**TS ISO/IEC TR 18044 Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği ihlal olayı yönetimi Standardı**

**(Information technology -- Security techniques -- Information security incident management) ?**

## TS ISO/IEC TR 18044 standardı

- ISO 27001 standardına göre Bilgi güvenliği yönetim sistemlerinin işletildiği kurumlarda ortaya çıkan ihlal olaylarının tespiti, kayıt altına alınması, raporlanması, değerlendirilmesi ve azaltılması için bir çerçeveye ihtiyaç vardır. TS ISO/IEC 18044 standardı bu konularda destek sağlamak amacı ile yayınlanmıştır.

# Kaynak:

https://www.isokalitebelgesi.com/iso-27001-standartlari-nelerdir-iso-27000-standart-ailesi-iso-27001-standardi-nedir