Dr.M.Talat ŞİMDİ
ÖZEL

ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı

ISO27001:2005 Bilgi Güvenliği Yönetimi Sistemi Nedir? Bilgi güvenliği yönetim sistemi hakkında bilinçlendirme ve eğitim faaliyetlerini yoğunlaştırarak devam ettiren Gelişim Yönetim Sistemleri A.Ş. 2006 yılında tüm kamu kurumları, üniversiteler ile IT, finans, sağlık sektörleri başta olmak üzere tüm Türkiye'deki kurumlara danışmanlık ve eğitim hizmetleri sunmaktadır.

Türkiye için yeni bir standart olmasına ve Türkçe hemen hemen hiç kaynak bulunmamasına rağmen sektörünün öncü kurumları tarafından faydası tespit edilmiş ve çalışmaları yıllardır sürdürülen bilgi güvenliği yönetim sisteminin yaygınlaşması, doğru anlaşılması ve verimli bir şekilde uygulanabilmesi için seminer faaliyetlerinin yanı sıra hazırlanan Türkçe kılavuzlar ve kitaplar ile de kurumların işlerini kolaylaştıracak çözümler sunmaya devam etmekteyiz.

ISO 27001 bilgi güvenliği yönetim sistemi hakkında dikkat edilmesi gereken temel noktalar aşağıda özetlendiği gibidir.

Bilgi güvenliği standardı BS 7799-2'nin revize edilip 2005'in sonlarında ISO 27001:2005 olarak değiştirilmesiyle yürürlüğe giren bu standart kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır.
Bunun yanı sıra ISO 17799:2002 numaralı standart ISO 17799:2005 "bilgi teknolojileri güvenlik teknikleri en iyi uygulamalar rehberi" olarak revize edilip yayınlanmıştır ve ISO 27001'e göre kurulacak bir BGYS'nin nasıl gerçekleştirilebileceğine dair açıklamaları içerir.

Bilgi güvenliği yönetim sistemi , kurumunuzdaki tüm bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir. Kurum kendine bir risk yönetimi metodu seçmeli ve risk işleme için bir plan hazırlamalıdır.

Risk işleme için standartta öngörülen kontrol hedefleri ve kontrollerden seçimler yapılmalı ve uygulanmalıdır. Planla-uygula-kontrol et-önlem al (PUKÖ) çevrimi uyarınca risk yönetimi faaliyetlerini yürütmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye geriletilene kadar çalışmayı sürdürmelidir.

ISO 27001 Kurumların risk yönetimi ve risk işleme planlarını , görev ve sorumlulukları, iş devamlılığı planlarını , acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Kurum tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamalı ve personelini bilgi güvenliği ve tehditler hakkında bilinçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımcılığıyla başarılabilir.

Kurum içerisinde bu çalışmaları yürütecek BGYS takımının ve BGYS yöneticisinin bilgi güvenliği yönetimi konusunda iyi eğitimli olmaları gerekmektedir. Risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması aşamalarında uzman desteği ve danışmanlık almaları faydalı olacaktır.

ISO 27001'den bahsederken karıştırılan ve dikkatle ayrılması gereken şey ISO 27001'in YÖNETİM SİSTEMİ öngörmesidir. ISO 27001 size nasıl virüs bulaşmayacağını anlatmaz.

ADRES : Zeytinalan Mah.4163 Sokak No : 11 Urla-İZMİR
TLF : 0232 472 19 80 GSM 0532 316 26 63
E.Mail : talatsimdi@talatsimdi.com
www.talatsimdi.com

Bilgisayar ağınıza saldırganların nasıl sızabileceğini söylemez. Size toplam bilgi güvenliği ve "yaşayan bir süreç olarak" bilgi güvenliğinin nasıl "yönetileceğini" tanımlar.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi kurmanın yararları

• Bilgi varlıklarının farkına varma: Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır.
• Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metotlarını belirler ve uygulayarak korur.
• İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.
• İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.
• Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
• Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.
• Çalışanların motivasyonunu arttırır.
• Yasal takipleri önler
• Yüksek prestij sağlar

ISO 27001 Bilgi Güvenliği Sistemi Kurma Aşamaları :

• Varlıkların sınıflandırılması
• Gizlilik , bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi
• Risk analizi
• Risk analizi çıktılarına göre uygulanacak kontrolleri belirleme
• Dokümantasyon oluşturma
• Kontrolleri uygulama
• İç tetkik
• Kayıtları tutma
• Yönetimin gözden geçirmesi
• Belgelendirme

ADRES : Zeytinalan Mah.4163 Sokak No : 11 Urla-İZMİR
TLF : 0232 472 19 80 GSM 0532 316 26 63
E.Mail : talatsimdi@talatsimdi.com
www.talatsimdi.com