BM TRADA

Bilgi Güvenliği Yönetim Sistemi ISO 27001: 2013

Bilgi güvenliği; iş devamlılığı, kaçınılmaz felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin, ulaşılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır.

Günümüzde, sadece çalışanlarıyla değil, müşterileri, iş ortakları ve hissedarlarıyla birlikte tanımlanan kurumlarda, bilginin korunmasına ve gizliliğine ilişkin güven ortamının yaratılması stratejik bir önem taşımaktadır.
Yaşanan güvenlik sorunları, iş devamlılığını engellemenin yanı sıra, kurumların; pazar kaybına, müşteriler, iş ortakları ve hissedarlar karşısında güven yitirmesine neden olmaktadır.
Bunların geri kazanılması, bunların yitirilmemesi için alınacak önlemlerden her zaman daha pahalıdır.

Bilgi Nedir?

Bilgi, diğer önemli ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi, kuruluşunuzun faaliyetleri ve devamı için büyük bir önem taşır.

Bilgi Güvenliği Nedir?

Bir kurumun bilgi varlıklarının gizliliğinin (bilginin yetkisi olmayan kişiler, kurumlar ya da süreçler için kullanılabilir olmamasını ya da ifşa edilmemesini temin etme özelliği), bütünlüğünün (varlıkların doğruluğunun ve eksiksizliğinin teminat altına alınması özelliği) ve kullanılabilirliğinin (yetkili bir kurumun talebi üzerine kullanılabilir olma özelliği) korunmasıdır.

Bilgi Güvenliği Nedir?

ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (ISMS) gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Ülkelere göre özel tanımlar içermeyen, genel tanımların bulunduğu bir standarttır. Yeterli ve orantılı güvenlik denetimleri seçilmesini sağlamak için tasarlanmıştır.

Bilgi güvenliği standardı BS 7799-2'nin revize edilip 2005'in sonlarında ISO 27001:2005 olarakdeğiştirilmesiyle 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 tekniklerien iyi uygulamalar rehberi" olarak revize edilip yayınlanmıştır ve ISO 27001'e göre kurulacak bir BGYS'nin nasıl gerçekleştirilebileceğine dair açıklamaları içerir.

ISO 27001 Kimi ilgilendirir?

ISO/IEC 27001, dünyanın hangi Ülkesinden veya hangi sektörden olursa olsun büyük küçük tüm kuruluşlara uygundur.

Bu standart, finans, sağlık, kamu ve BT sektörleri gibi bilginin korunmasının büyük öneme sahip olduğu alanlarda özellikle gereklidir.ISO/IEC 27001, BT taşeron şirketleri gibi bilgiyi başkaları adına yöneten kuruluşlar için de oldukça önemlidir, müşterilere bilgilerinin koruma altında olduğu güvencesini vermek için kullanılabilir.

ISO 27001 Standart Ailesi

ISO 27001 BGY Sistemi Şartları

- 27000 Tanım ve Tarifler
- 27002 Uygulama Kuralları
- 27003 BGYS Uygulama Klavuzu
- 27004 BGYS Ölçümü
- 27005 Bilgi Güvenliği Risk Yönetimi

ISO/IEC 27001 İle ilgili Terim ve Kavramlar

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası.

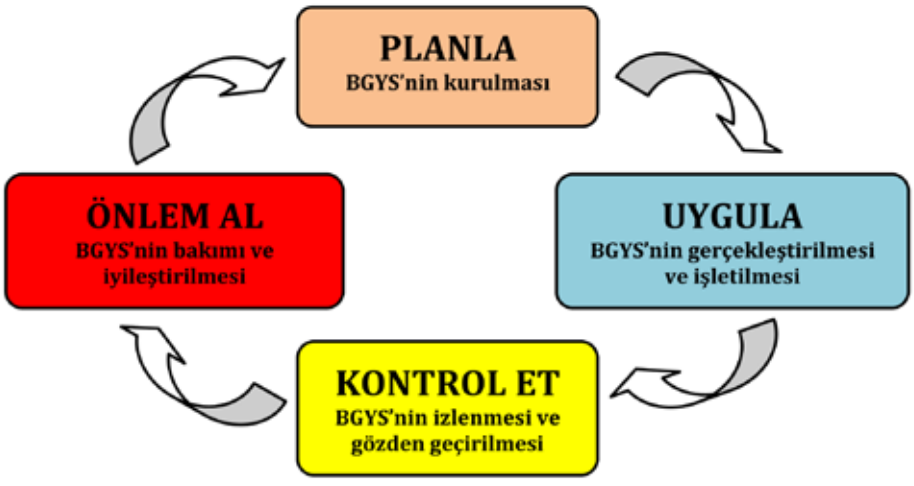
Risk analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı

Risk değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi.

Risk yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler.

ISO 27001 Bilgi Güvenliği Yönetim Sisteminin Kurulmasının Planlaması

- Organizasyondaki altyapıyla ilgili bilgilerin toplanması
  - yapılan işin niteliği
  - misyon
  - yerleşim noktaları
- BGYS'nin kurulumda görev alacak anahtar oyuncular
  Risk yönetimini gerçekleştirecek sorumlular ve BGYS'nin kurulma nedeni
- Mevcut durumda organizasyonun güvenlik durumu
- BGYS'nin kapsamını belirleyecek bilgiler; lokasyonlar, işlemler, iş fonksiyonları, bilgi, bilgi teknolojileri
- BGYS'nin hedefi
- BGYS'nin kapsamının belirlenmesi
- BGYS'nin kurulması için çalışma programının oluşturulması
- BGYS'nin kurulması ve sürekliliği için gerekli olan süreçlerin belirlenmesi



ISO 27001 Bilgi Güvenliği Yönetim Sistemi Kurmanın Yararları

- Bilgi varlıklarının farkına varılır, kuruluş hangi bilgi varlıklarının olduğunu ve bunların değerinin farkına varır.
- Sahip olduğu varlıkları, kuracağı kontroller ile koruma metodlarını belirleyerek ve uygulayarak korur.
- İş sürekliliği sağlar, uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.
- Tedarikçi ve müşterilerin bilgileri korunacağından ilgili tarafların güvenini kazanır.
- Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
- Müşterileri değerlendirirken, rakiplerine göre daha iyi değerlendirilir.
- Çalışanların motivasyonunu arttırır.
- Yasal takipleri önler.
- Yüksek prestij sağlar.
- Rekabet avantajı kazandırır.
- Düzenli değerlendirme işlemi performansınızı sürekli izlemenize ve geliştirmenize yardımcı olur.

ISO 27001 Bilgi Güvenliği Sistemi Kurma Aşamaları

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 Yönetim Sistemi öngörmesidir. ISO 27001 size nasıl virüs bulaşmayacağını anlatmaz. Bilgisayar ağınıza saldırganların nasıl sızabileceğini söylemez. Size toplam bilgi güvenliği ve "yaşayan bir süreç olarak" bilgi güvenliğinin nasıl "yönetileceğini" tanımlar.

Kurma aşamalarını maddeler halinde sıralayacak olursak aşağıda belirtildiği şekilde bir sıralama uygundur.

- 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.

Standartla İlgili Yasal Şartlar

- 5651 Sayılı Kanun İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 5809 Sayılı Kanun Elektronik Haberleşme Kanunu
- 26942 Sayılı Elektronik Haberleşme Güvenliği Yönetmeliği

Kanun kapsamında yapılması gerekenler;

- Bilgisayarların aldığı IP loglarını kayıt altına almak
- Geçmişe yönelik hangi kullanıcının hangi IP adresine sahip olduğunu kayıt altına almak
- Kullanıcının web üzerindeki yaptığı gezintilerin loglarını kayıt altına almak
- Atılan e-mail loglarını kayıt altına almak
- Geçmişe yönelik hangi kullanıcının web üzerinde hangi sayfalara gittiği ve ne kadar zaman geçirdiğini kayıt altına almak
- Web erişimlerini içerik bazlı filtreleyerek kısıtlı erişimler sağlamak
- Toplanan tüm kayıtların bütünlüğünü sağlayarak değiştirilmediğini kanıtlamak

Elektronik haberleşmeye ilişkin başlıca tehditler;

a) Yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi,

b) Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması,

c) Donanım-yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi,

d) Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,

e) Elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve/veya dinlenmesi,

f) Doğru olmayan bir bilgi üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafa gönderilmesi,

g) Elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez hale getirilmesi veya altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesidir.

Elektronik haberleşmeye ilişkin başlıca zayıflıklar;

a) Gelecekte gerçekleşmesi muhtemel tehditlerin öngörülememesi,

b) Bir sistem veya protokolün tasarımında yapılan yanlışlıklar,

c) Bir sistem veya protokolün kurulumu sırasında oluşan problemler,

ç) Geliştiricilerin hataları,

d) Uygulayıcıların hataları,

e) Sistemin işletimi sırasında oluşan uygunsuzluklar veya yetersizliklerdir.

Neden BM TRADA?

Standart BM TRADA Belgelendirme A.Ş., uluslararası BM TRADA Group'un Türkiye'deki ortak teşebbüsü olup UKAS ve TÜRKAK akreditasyonları ile denetim ve sertifikasyon hizmetleri vermektedir. BM TRADA Group ürün testleri, belgelendirme ve fabrika üretim kontrolü denetimlerinde 80 yıllık tecrübesi ile dünya liderleri arasındadır.

Grup kuruluşumuz olan Standart Yapı Laboratuvarı ise Türkiye'de TÜRKAK'tan akredite ve T.C. Çevre ve Şehircilik Bakanlığı'nın atadığı AB onaylı cam laboratuvarıdır. Uluslararası laboratuvar akreditasyon standardı ISO 17025'e göre faaliyet göstermektedir. Laboratuvarımız, tüm gerekli testleri tam donanımlı bir ortamda, ilgili uluslararası, AB ve yerel standart ve yönetmeliklere göre yapmaktadır. Standart Yapı Laboratuvarı kurulduğu 2009 yılından bu yana temperli ve yalıtım camlarının ilk tip ve periyodik testlerini yaparak Türkiye'de 700'ün üzerinde cam üreticisine test hizmeti vermiştir.

info@bmtrada.com.tr

www.bmtrada.com.tr

+90 (0) 216 574 88 01