ISO 27001 Kurumsal Bilgi Güvenliği Standardı

TÜRCERT

Bilgi Güvenliği Kavramı

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "süreklilik(erişilebilirlik)" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik zaafiyeti oluşur.

- Gizlilik (Confidentiality): Bilginin yetkisiz kişilerce erişilememesidir.
- Bütünlük (Integrity): Bilginin doğruluğunun ve tamlılığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır.
- Erişilebilirlik (Availability): Bilginin bilgiye erişim yetkisi olanlar tarafından istenildiği anda ulaşılabilir, kullanılabilir olmasıdır.

Kurumsal Bilgi Güvenliği

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

Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Yani, bilgi güvenliği sadece bir Bilgi Teknolojisi (BT) ya da yaygın söylemle Bilgi Sistemleri işi değildir; kurumun her bir çalışanının katkısını ve katılımını gerektiren bir süreçtir.

ISO 27001 Standardı ve Bilgi Güvenliği Yönetim Sistemi(BGYS)

ISO/IEC 27001:2005 *- Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler* standardı , bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) (ISMS – Information Security Management System) kurmak, geliştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak amacıyla hazırlanmıştır. ISO/IEC 27001, bilgi güvenlik yönetim standardıdır.

Bu standart ISO tarafından 14 Ekim 2005 tarihinde yayınlanmış ve ISO/IEC 27000 standart serisi altında yerini almıştır.

Türkiye'de ise, ISO tarafından kabul edilen, ISO/IEC 27001:2005 standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 2 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek, "**TS *ISO/IEC 27001*** *Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimleri* "adıyla yayınlanmıştır.

ISO 27001'in de içinde bulunduğu ISO 27000 ailesi kısaca şöyledir:

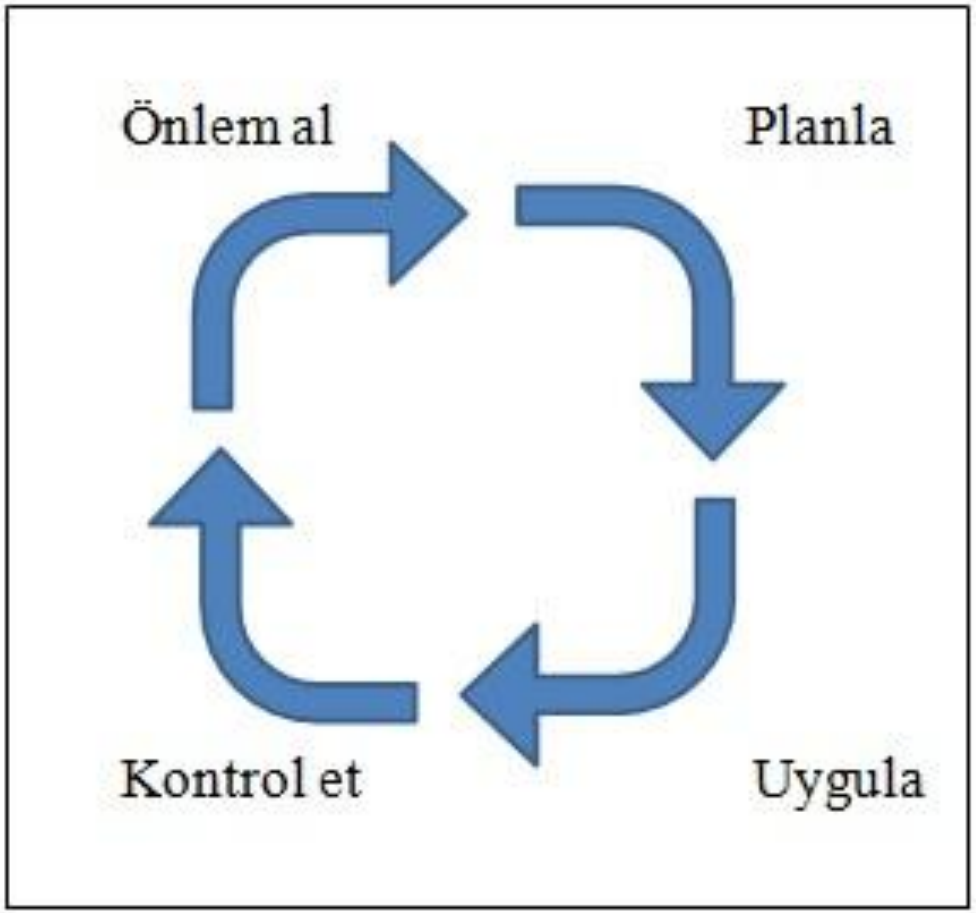
- ISO/IEC 27000 – BGYS Genel Bilgiler ve Tanımlar
- ISO/IEC 27001 – BGYS Gereksinimleri
- ISO/IEC 27002 – BGYS Uygulama Pratikleri ve Kontrolleri
- ISO/IEC 27003 – BGYS Risk Yönetimi Uygulama Rehberi
- ISO/IEC 27004 – BGYS Etkinlik Ölçüm Rehberi
- ISO/IEC 27005 – BGYS Risk Yönetimi Rehberi
- ISO/IEC 27006 – BGSY Belgelendirme Kurumları İçin Rehber
- ISO/IEC 27007 – BGYS Denetim Rehberi
- ISO/IEC 27011 – Telekominikasyon Kuruluşları için BGYS
- ISO/IEC 27799 – Sağlık Kuruluşları için BGYS Rehberi

ISO 27001 ve ISO 27002, BGYS'nin en temel standartlarıdır. BGSY'nin planlanmasının, gerçekleştirilmesini, iyileştirilmesini ve sürdürülmesi için uygulama işlemlerini ve kontrollerini ISO 27002 içerirken; BGYS'nin belgelendirilmesi için gereken standartlarsa ISO 27001'de yer almaktadır.

ISO 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler standardı kurumsal bilgi güvenliğinin sağlanmasına yönelik bir standarttır. Kurumsal bilgi güvenliğinin bir kurumda nasıl uygulanabileceğini açıklayan bir dokümandır. Sadece sistem güvenliğinden değil bilgi güvenliğinden bahsetmektedir.

Bu standart, bir BGYS kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır.

BGYS yaşayan bir süreç olmak zorundadır. Bu nedenle de Standard BGYS için, planla-uygula - kontrol et - önlem al (PUKÖ) döngüsünü benimsemiştir.



BGYS için PUKÖ döngüsü

Planlama; Kurumun BGYS politikası, amaçları, hedefleri, prosesleri ve prosedürlerinin oluşturulur.

Uygulama; BGYS'nin gerçekleştirilmesi ve işletilmesini yani, BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesini ifade etmektedir.

Kontrol et; BGYS'nin izlenmesi ve gözden geçirilmesi, BGYS politikası, amaçlar ve kullanım deneyimlerine göre süreç performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesini ifade etmektedir.

Önlem al; BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilerek BGYS'nin sürekliliğinin ve iyileştirilmesinin sağlanmasını ifade etmektedir.

Bilgi Güvenliği Yönetim Sistemi"ni uygulamak isteyen bir kurumda yapılması gereken aşamalar, 11 ana madde halinde aşağıda özetle anlatılmaya çalışılmıştır.

1.Güvenlik politikası: Üst yönetim tarafından onaylanmış bir bilgi güvenliği politikası oluşturulmalıdır. Bu politika üst yönetimin bilgi güvenliği yönetimi ile ilgili taahhüdünü ve kurumsal yaklaşımını yansıtmalıdır.

2.Bilgi güvenliği organizasyonu: Bu bölümde kurum içi ve üçüncü taraflarla olan erişim güvenliği organize edilmelidir. Yönetim kurum içinde uygulanacak güvenlik tedbirlerini aktif olarak desteklemeli, bilgi güvenliği ile ilgili hedefler belirlenmeli ve sorumluların atanması yapılmalıdır. Ayrıca organizasyon içerisindeki uygulama ile güvenlik politikası esaslarının aynı olduğu, güvenlik politikasının etkin ve uygulanabilir olduğu düzenli bir şekilde bağımsız bir kurum veya kuruluş tarafından denetlenmelidir.

3.Varlık yönetimi: Tüm bilgi varlıklarını içeren bir varlık envanteri tutulmalıdır. Bu envanter hazırlanırken aşağıda belirtilen varlık türlerinin tamamı göz önünde bulundurulmalıdır.

- Bilgi: Veri Tabanı, sözleşme ve anlaşmalar, sistem dokümantasyonu vb.
- Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları ve yazılım geliştirme araçları.
- Fiziksel varlıklar: Bilgisayarlar ve iletişim araçları.
- Hizmete dönük varlıklar: Bilgisayar ve iletişim hizmetleri, ısıtma, aydınlatma, güç vb.
- Personel: Nitelik ve tecrübeleri ile birlikte.
- Soyut varlıklar: Kuruluşun itibarı ve imajı gibi.

Varlık envanteri herhangi bir afetten sonra normal çalışma şartlarına dönmek için gereken (varlığın türü, formatı, konumu, değeri gibi) tüm bilgileri içermelidir.

4.İnsan kaynakları güvenliği: Kurumun bilgi güvenliği politikası uyarınca personele düşen güvenlik rol ve sorumlulukları belgelenmeli; işe alınacak personele yüklenecek rol ve sorumluluklar açıkça tanımlanmış ve işe alınmadan önce personel tarafından iyice anlaşılması sağlanmış olmalıdır. Kurum çalışanlarının gizlilik ve açığa çıkarmama anlaşmalarını işe alınma şartının bir parçası olarak imzalamaları istenmelidir. Kurum çalışanlarının güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin süreci olmalıdır.

5.Fiziksel ve çevresel güvenlik: Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği (kart kontrollü giriş, duvarlar, insanlı nizamiye vb.) tesis edilmelidir. Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalıdır. Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları oluşturulmalı ve ziyaretçilerin giriş-çıkış zamanları ve ziyaret sebepleri kaydedilmelidir. Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmış olmalı ve uygulanmalıdır.

6.İletişim ve işletme yönetimi: İşletme prosedürleri yazılmalı ve güncellenmelidir. Bilgi işlem ve iletişim ile ilgili sistem açma/kapama, yedekleme, cihazların bakımı, sistem odasının kullanılması, gibi sistem faaliyetleri prosedürlere bağlanmalıdır. İşletme prosedürlerine, ihtiyacı olan tüm kullanıcılar erişebilmeli ve bu prosedürler resmi belge gibi ciddiye alınmalıdır. Bilgi işlem sistemlerinde yapılan değişiklikler denetlenmeli ve yapılan değişiklikler için kayıtlar tutulmalıdır. Yedekleme politikası uyarınca bilgi ve yazılımların yedeklenmesi ve yedeklerin test edilmesi düzenli olarak yapılmalıdır.

7.Erişim kontrolü: Erişimle ilgili iş ve güvenlik ihtiyaçları göz önünde bulundurularak erişim denetimi politikası oluşturulmalı ve belgelenmelidir. Erişim denetimi hem fiziksel, hem işlevsel boyutları ile değerlendirilmeli ve erişim denetimi politikası bütün kullanıcılar veya kullanıcı grupları için erişim kurallarını ve haklarını açıkça belirtmelidir. Erişim haklarının "Yasaklanmadıkça her şey serbesttir" değil "İzin verilmedikçe her şey yasaktır" prensibine göre verilmesine dikkat edilmelidir.

8.Bilgi sistemleri tedariği, geliştirme ve bakımı: Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı; doğru girilmiş bilginin işlem sırasında hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır. Bilginin korunması için kriptografik kontrollerin kullanılmasını düzenleyen politika geliştirilmiş ve uygulamaya alınmış olmalıdır.

9.Bilgi güvenliği olayları yönetimi: Güvenlik olaylarını mümkün olduğunca hızlı bir şekilde raporlamak ve kurum çalışanlarının sistem ve servislerdeki güvenlik zafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulmalıdır. Personel ve üçüncü taraf çalışanları zafiyetlerin varlığını kanıtlamak için test ve girişimler yapmaktan kaçınmalıdır. Aksi halde sistemde hasar oluşabileceği gibi testi yapan personelin de suçlu durumuna düşebileceği personele anlatılmalıdır. Bilgi güvenliği olaylarını ortaya çıkarmak için sistemler, sistemlerin açıklıkları ve üretilen alarmlar izlenmelidir. Bilgi sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilgi sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanmalıdır.

10.İş sürekliliği yönetimi: Kurum bünyesinde bilgi güvenliği ihtiyaçlarına yer veren iş sürekliliği için geliştirilmiş bir süreç oluşturulmalı. Bu süreç iş sürekliliği ile ilgili olarak kuruluşun yüz yüze olduğu riskleri, kritik iş süreçleri ile ilgili varlıkları, bilgi güvenliği olayları yüzünden gerçekleşebilecek kesintilerin etkisini, ilave önleyici tedbirlerin belirlenmesi ve uygulanmasını, bilgi güvenliğini de içeren iş sürekliliği planlarının belgelenmesi konularını içermelidir.

11.Uyum: Her bir bilgi sistemi için ilgili bütün yasal, düzenleyici ve sözleşmeye bağlı gereksinimler ve gereksinimleri sağlamak için kullanılacak kurumsal yaklaşım açık şekilde tanımlanmış ve belgelenmiş olmalıdır. Yine bu gereksinimleri karşılamak amacıyla kontroller ve bireysel sorumluluklar tanımlanmalı ve belgelenmelidir.

Sonuç

ISO 27001'in öngördüğü bir BGYS kurmak kurumlara birçok yarar sağlayacaktır. BGYS kurma adımlarının izlenmesi sonucunda kurum her şeyden önce bilgi varlıklarının farkına varacaktır. Hangi varlıkları olduğunun ve bu varlıkların önemini anlayacaktır.

Risklerini belirleyip yöneterek en önemli unsur olan iş sürekliliğini sağlayabilecektir.

Bir kuruluşun ISO 27001 sertifikasına sahip olması, kurumun güvenlik risklerini bildiği, yönettiği, belli riskleri de ortadan kaldırmak için kaynak ayırdığı anlamına gelmektedir.

SORULAR

&

TEŞEKKÜRLER