

ISO 27001 Kurumsal Bilgi Güvenliği Standardı

Şenol Şen¹, Tarık Yerlikaya²

¹ Trakya Üniversitesi, Bilgi İşlem Daire Başkanlığı, Edirne

² Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne
senolsen@trakya.edu.tr, tarikyer@trakya.edu.tr

Özet: Bilgi Güvenliği bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci olarak tanımlanmaktadır. ISO 27001 dünya üzerinde geçerliliği olan ve gitgide birçok alanda zorunlu hale getirilmeye ç alışılan bir Bilgi Güvenliği Yönetim Sistemleri (BGYS) standardıdır. Bu standart, kurumlara genel anlamda bilgi güvenliğini nasıl yapabileceklerini anlatmaktadır. Kurumların, bilgi sistemleri süreçlerini inceleyerek tehditleri ve riskleri belirlemesi ve bu riskleri kabul edilebilir bir seviyeye indirebilmesi için alınacak önlemleri tespit etmesi gerekmektedir. Bu bildiriye, bu önlemlerin ISO/IEC 27001 Kurumsal Bilgi Güvenliği Standardı çerçevesinde bir kuruma uygulanabilmesi için yapılması gereken aşamalar verilmeye çalışılmıştır.

Anahtar Sözcükler: Bilgi güvenliği, Kurumsal Bilgi Güvenliği, ISO/IEC 27001 Kurumsal Bilgi Güvenliği Standardı

ISO 27001 Enterprise Information Security Standard

Abstract: Information Security, accessibility of the information provided in an environment constantly, until the recipient of the sender of information, in confidence intact, unchanged and ensure the integrity of passed over by others, and is defined as the process of delivering a safe way. ISO 27001 becomes mandatory in many areas around the world and increasingly tried to be valid an Information Security Management Systems (ISMS) standard. This standard describes to institutions how to provide information security in general. Organizations have to examine their information system processes to find out threats and risks and then countermeasures against these risks must be determined to be able to reduce the risks to an acceptable level. In this article, it is aimed to provide some clues on how these methods could be applied to organizations within the framework of ISO/IEC 27001 Information Security Management Systems standard.

Keywords: Information Security, Enterprise Information Security, ISO/IEC 27001 Information Security Management Systems Standard1.

1. Giriş

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri "olmazsa olmaz" bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir.

2. 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. [1]

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.



Şekil 1. Temel Güvenlik Prensipleri

Bu üç temel unsur birbirinden bağımsız olarak düşünülememektedir. Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de sağlanması önemlidir. Eğer bir bilgi için sadece

gizlilik sağlanıyor ve bilgiye erişim engelleniyor ise kullanılamaz durumda olan bu bilgi bir değer ifade etmeyecektir. Eğer erişimi sağlanıyor ancak bütünlüğü sağlanmıyor ise kurumlar ve kişiler için yanlış veya eksik bilgi söz konusu olacak ve olumsuz sonuçlara neden olabilecektir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanması demektir. [2]

3. Kurumsal Bilgi Güvenliği

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanmaktaydı. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zaafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir. [3]

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 çalışanın katkısını ve katılımını gerektirir. Ciddi boyutta bir kurum kültürü değişimi gerektirdiği için, en başta yönetimin onayı, katılımı ve desteği şarttır. BT'nin teknik olarak gerekli olduğunu saptadığı ve uyguladığı teknik güvenlik çözümleri, iş süreçleri ve politikalarla desteklenmemiş ve kurum kültürüne yansıtılmamışsa etkisiz kalacaklardır. Gerekli inanç ve motivasyon yaratılamamışsa, çalışanlar şifrelerini korumakta özensiz, hassas alanlarda gördükleri yabancı kişilere karşı aldırılmaz, kağıt çöpüne gerekli imha işlemini yapmadan atacakları bilgilerin değeri konusunda dikkatsiz olabilecekler ve yapılan güvenlik yatırımlarına karşın büyük bir açık oluşturmaya devam edebileceklerdir. [4]

Kişiler ve kurumların bilgi güvenliğini sağlamadaki eksikliklerinin yanında saldırganların saldırı yapabilmeleri için ihtiyaç duydukları yazılımlara internet üzerinden kolaylıkla erişebilmeleri fazla bilgi birikimine ihtiyaç duyulmaması ve en önemlisi ise kişisel ve kurumsal bilgi arlıklarına yapılan saldırılardaki artışlar, gerek kişisel gerekse kurumsal bilgi güvenliğine daha fazla önem verilmesine yeni yaklaşımların ve standartların kurumlar bünyesinde uygulanması zorunluluğunu ortaya çıkarmıştır. [5]

4. ISO 27001 Standardı ve Bilgi Güvenliği Yönetim Sistemi (BGYS)

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda bilgi güvenliğinin sağlanması

ihtiyacı her geçen gün katlanarak artmıştır. Sadece teknik önlemlerle (güvenlik duvarları, saldırı tespit sistemleri, antivirüs yazılımları, şifreleme, vb.) kurumsal bilgi güvenliğinin sağlanmasının mümkün olmadığı görülmüştür. Bu nedenle teknik önlemlerin ötesinde, insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sisteminin gerekliliği ortaya çıkmıştır.

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için, teknik önlemlerin yanında teknik olmayan (insan faktörü, prosedürel faktörler, vb.) önlemlerin ve denetimlerin alınması, tüm bu süreçlerin devamlılığının sağlanması ve bilgi güvenliği standartlarına uygun olarak yönetilebilmesi amacıyla yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini kapsayan bilgi güvenliği standartlarına uygun olarak Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları gerekmektedir. Bilgi güvenliği standartları kurumların kendi iş süreçlerini bilgi güvenliğine yönelik risklerden korumaları ve önleyici tedbirleri sistematik biçimde işletebilmeleri ve standartların gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir. [5]

Bilgi varlıklarının korunabilmesi, kurumların karşılaşılabileceği risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması BGYS'nin kurumlarda üst yönetim desteğiyle hayata geçirilmesiyle mümkün olmaktadır. BGYS, ISO 27001 standardının öngördüğü bir yapıdır.

Standardın tanımına göre BGYS, "Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası" olarak tanımlanmaktadır. Kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içermektedir.

ISO 27001'in de içinde bulunduğu ISO 27000 ailesi aşağıda kısaca verilmiştir.

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 – Telekomünikasyon Kuruluşları için BGYS

ISO/IEC 27799 – Sağlık Kuruluşları için BGYS Rehberi [7]

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 standartlara ISO 27001'de yer almaktadır. [7]

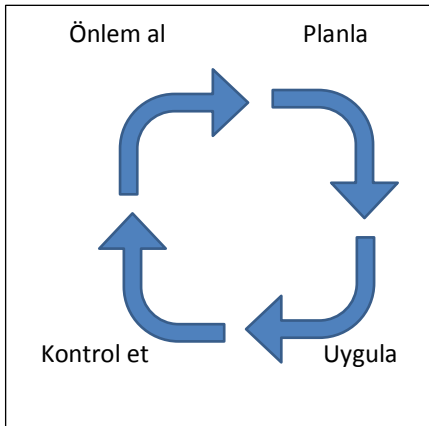
ISO 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler standardı kurumsal bilgi güvenliğinin sağlanmasına yönelik bir standarttır. Kurumsal bilgi güvenliğinin bir kurumda nasıl uygulanabileceğini açıklayan bir dokümandır. Sadece sistem güvenliğinden değil bilgi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

Bu standart, bir BGYS kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. Bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan süreçler ve kuruluşun büyüklüğü ve yapısından etkilenir. Bir BGYS gerçekleştirmesinin kuruluşun ihtiyaçlarına göre ölçeklenmesi beklenir.[6]

Standard, sunulan bilgi güvenliği süreç yaklaşımının, kullanıcılarını aşağıdakilerin önemini anlamalarına yardımcı olmaktadır.

- İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için politika ve amaçların belirlenmesi ihtiyacını anlamak,
- Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
- BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,
- Nesnel ölçmeye dayalı olarak sürekli iyileştirmek.

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



Şekil 2. BGYS için PUKÖ döngüsü

BGYS süreçlerine uygulanan PUKÖ modeli aşamaları şu şekilde özetlenebilir:

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.

Bu aşamalar sürekli bir biçimde birbirini izleyerek yaşayan bir sistem oluşturmaktadır.

Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, varlıkların yönetimi, risk yönetimi, dokümantasyon oluşturma, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri ve yönetimin gözden geçirmesi BGYS'nin kurulum adımlarıdır.[2]

BGYS'nin kurulması; varlık envanterinin yapılması, bu varlıklara karşı olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun çözümlerin geliştirilerek sistemin iyileştirilmesi gibi birbirini izleyen ve tamamlayan denetimlerin gerçekleştirilmiş olması demektir.

Bilgi Güvenliği Yönetim Sistemi'ni uygulamak isteyen bir kurumda yapılması gereken aşamalar aşağıda özetle anlatılmaya çalışılmıştır.

4.1 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.

4.2 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. Yine bilgi sistemlerine üçüncü tarafların erişiminden kaynaklanacak riskler belirlenmeli ve erişim hakkı verilmeden önce bununla ilgili tedbirler alınmalıdır.

4.3 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.

4.4 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. İşten ayrılma, kontratın veya anlaşmanın sona ermesi halinde veya görev değişikliği halinde kurum çalışanlarının veya üçüncü parti kullanıcılarının kuruluşun bilgi varlıklarına veya bilgi işlem araçlarına erişim hakları kaldırılmalı veya gerektiği şekilde yeniden düzenlenmelidir.

4.5 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.

4.6 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. Bir felaket veya sistem hatasından sonra gerekli tüm bilgilerin ve yazılımların kurtarılmasını sağlayacak yedekleme kabiliyetleri kuruma kazandırılmalıdır.

4.7 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.

4.8 Bilgi sistemleri tedarigi, 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. Çalışan sistemlere yazılım yüklenmesini -bozulma riskini asgariye indirmek için- düzenleyen prosedürler olmalı ve bilgi sistemleri üzerinde yapılacak değişiklikler resmi kontrol prosedürleri aracılığı ile denetlenmelidir.

4.9 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 kaçınılmalıdır. 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. Açığı kapatmak ve hataları düzeltmek için gereken çalışmalar yapılırken canlı sisteme sadece yetkili personelin erişmesine, acil düzeltme çalışmalarının dokümanite edilmesine, çalışmaların düzenli olarak yönetime bildirilmesi ve yönetim tarafından gözden geçirilmesine ve bilgi sistemlerinin bütünlüğünün asgari gecikme ile sağlanmasına dikkat edilmelidir.

4.10 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.

4.11 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 olmalı ve bu gereksinimleri karşılamak amacıyla kontroller ve bireysel sorumluluklar tanımlanmalı ve belgelenmelidir. Kullanılmakta olan yazılım ve diğer her türlü materyal ile ilgili olarak yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasını güvence altına alan prosedürler yürürlüğe sokulmalıdır.

5.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. İş sürekliliğinin sağlanması kurumun faaliyetlerine devam edebilmesi anlamına gelmektedir.

Bilgilerin korunacağından, kurumun iç ve dış paydaşlarında bir güven duygusu oluşturur, motivasyon sağlar. Daha iyi bir çalışma ortamı yaratılmasına katkı sağlar.

Kurum, kuruluş ve işletmelerin belirli güvenlik standartları çerçevesinde bilgi güvenliğini sağlayarak iç ve dış tehditler karşısında zarar görmeden veya en az zararla iş sürekliliklerini devam ettirebilmeleri için bilgi güvenliği standartlarını kendi kuruluşlarında uygulamaları artık neredeyse bir zorunluluk haline gelmiştir.[8]

6. Kaynaklar

- [1] Bilişim Güvenliği Sürüm 1.1, [Http://Www.Pro-G.Com.Tr](http://Www.Pro-G.Com.Tr)
- [2] Doğantimur F., Iso 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, 2009
- [3] Vural Y., Sağıroğlu Ş., Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme, Gazi Üniv. Müh. Mim. Fak. Der. Cilt :23 No: 2, 2008.
- [4] Küçükoğlu Ş., Uygun Güvenlik Çözümüne Yolculuk, [Http://Www.İnfosecurenet.Com/Macroscop/Macroscop6.Pdf](http://Www.İnfosecurenet.Com/Macroscop/Macroscop6.Pdf).
- [5] Vural Y., Sağıroğlu Ş., Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği Ve Kriptoloji Konferansı, 2007.
- [6] Ts Iso/Iec 27001, Mart 2006.
- [7] [Http://Www.CozumPark.Com/Blogs/Cobit-İtil/Archive/2012/06/02/Ts-_3101_So-_3101_Ec-27001-2005-Bilgi-G-Venli-I-Y-Netim-Sistemi-Ve-Puk-Modeli-B-L-M-2.AspX](http://Www.CozumPark.Com/Blogs/Cobit-İtil/Archive/2012/06/02/Ts-_3101_So-_3101_Ec-27001-2005-Bilgi-G-Venli-I-Y-Netim-Sistemi-Ve-Puk-Modeli-B-L-M-2.AspX)
- [8] Sağıroğlu Ş., Ersoy E. Ve Alkan M., Bilgi Güvenliğinin Kurumsal Bazda Uygulanması, Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği Ve Kriptoloji Konferansı, 2007.
- [9] Ottekin F., Ts Iso/Iec 27001 Denetim Listesi, Tubitak- Uekae, 2008