ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme

Vedat MARTTİN[1*], İhsan PEHLİVAN[2]

[1] Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, Bilecik Üniversitesi,Bilecik,Türkiye
[2]Elektrik-Elektronik Mühendisliği Bölümü, Sakarya Üniversitesi,Sakarya,Türkiye
vedat.marttin@bilecik.edu.tr, ipehlivan@sakarya.edu.tr

Özet- Günümüzde bilgiye ulaşmak kolaylaşmış, erişilen bilgilerin mekândan bağımsız olarak taşınmasında ve saklanmasında bilgi güvenliği önemli rol oynamaktadır. Bilgi Güvenliğinin daha sağlıklı yapılabilmesi için kullanılan standartlar vardır. Bu makalede Bilgi Güvenliği Yönetim Sistemi nedir? Kurulum aşamaları nelerdir? ISO 27001 BGYS kurma yararları nelerdir? Sistemle ilgili yanlış algılamalar ve olması gerekenler nelerdir? Türkiye'de Kamu Kurumlarında Bilgi Teknolojileri Güvenliği Yönetimi örnekleri ve TS ISO/IEC 17799 Uygulamaları nelerdir? Sorularına cevap olabilecek bilgiler sunulacaktır.

Anahtar Kelimeler- ISO 27001:2005,Bilgi Güvenliği Yönetim Sistemi, Bilgi Güvenliği.,PUKO.

ISO 27001:2005 Information Security Management Standards and Practices in Turkey, A Study of Some Public Institutions

Abstract- Today, access to information became easier to access the information regardless of location for transporting and storing of information security play an important role. Information Security used to be more healthy, there are standards. In this article What is Information Security Management System? What are the installation steps? What are the benefits of ISO 27001 ISMS up? System and must be related to those perceptions are wrong? Information Technology Management in Public Institutions in Turkey are examples of security and ISO / IEC 17799 Applications? Information that can answer the questions will be presented.

Keyword- ISO 27001:2005 ,ISMS,Information security,PDCA.

1. GİRİŞ

Günümüzde bilgiye ulaşmak kolaylaşmış, erişilen bilgilerin mekândan bağımsız olarak taşınmasında ve saklanmasında bilgi güvenliği önemli rol oynamaktadır. Kamu kurum ve kuruluşları ile özel kuruluşlarda pek çok bilginin, elektronik ortamlarda yedeklendiği düşünüldüğünde ve "Bilginin nasıl daha güvenli ve sürekli saklanabilir?"sorusuna cevap olabilecek standartlar incelendiğinde Bilgi Güvenliği Yönetim Sistemi Standartlarında ISO 27001:2005 Standardı akla gelmektedir. Bu makalede Bilgi Güvenliği Yönetim Sistemi Standartlarından ISO 27001:2005 Standardının ne olduğu, kimleri ilgilendirdiği, standardı kurma aşamaları, standardı kullanmanın ne gibi faydalar getireceği, risk grubu içinde olan sektörler ve ülkemizdeki bazı kamu kurumlarında yapılan bilgi güvenliği yönetimi uygulamalardan bahsedilecektir.

Bu çalışma ile yüksek risk grubu içinde bulunan sektörlerden kamu kurumlarının bilgi güvenliği konusunda bilinçlendirilmesi ve ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardıyla risk düzeyinin daha aşağıya çekileceği düşünülmektedir.

2. BİLGİ GÜVENLİĞİ

Bilgi birçok biçimde bulunabilir. Bilgi, kâğıt üzerinde yazılı olabilir, elektronik olarak saklanıyor olabilir, posta ya da elektronik posta yoluyla bir yerden bir yere iletilebilir ya da kişiler arasında sözlü olarak ifade edilebilir. Bilgi hangi formda olursa olsun, mutlaka uygun

bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin yeterli düzeylerde sağlanabilmesi ile mümkündür[1].

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:
• Gizlilik (Confidentiality)
• Bütünlük (Integrity)
• Kullanılabilirlik (Availability)

Kavramları açmak gerekirse gizlilik, bilginin yetkisiz kişilerin erişimine kapalı olması ya da bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

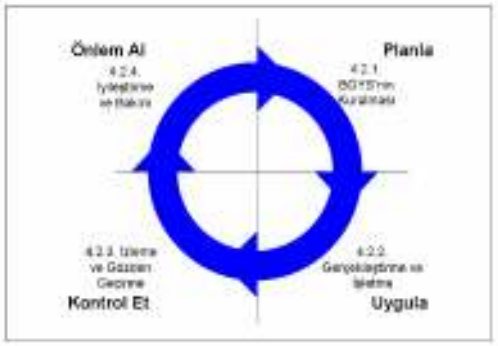
Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda problem çıkması durumunda bile bilginin erişilebilir olması, kullanıma hazır durumda olması demektir.
Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir[1].

3. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Bilgi Güvenliği Yönetim Sistemi kısaltılmış adıyla BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. BGYS'nin temel amacı hassas bilginin korunmasıdır.

Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Bu standart daha sonra Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından yayınlanan bir diğer standart BS 7799-1 ise bilgi güvenliğinin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Yine ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıştır. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu[1].

Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir. Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın belgelendirmesi konusunda TSE tarafından TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu standardı yayınlanmıştır. ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. BGYS standartları kapsamında PUKÖ (Planla – Uygula –Kontrol et – Önlem al) modeli kullanılmaktadır. PUKÖ modelini görsel olarak anlatan Şekil 1 de görülmektedir.



Şekil 1. PUKÖ adımları ve BGYS döngüsü [2]

a) Planla (BGYS'nin kurulması)
BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesidir.

b)Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi)
BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesidir.

c)Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi)
BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesidir.

d)Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)
Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesidir.
Bilgi güvenliği yönetimi, sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi bir döngü içinde durmaksızın sürekli devam etmelidir. PUKÖ modeli özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır.

Çizelge 1. PUKÖ adımlarının standart alt başlıkları ile ilişkisi [2]

Adım	Standardın ilgili başlığı
Planla	4.2.1-BGYS'nin kurulması
Uygula	4.2.2-BGYS'nin gerçekleştirilmesi ve işletilmesi
Kontrol Et	4.2.3-BGYS'nin izlenmesi ve gözden geçirilmesi
Önlem Al	4.2.4-BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi

3.1 Bilgi Güvenliği Yönetim Sistemi Kapsamı

BGYS kapsamında, güvenlik ile ilintili kontroller 11 ana çalışma alanı altında toplanmıştır. Bu alanlar ve kısa tanımları aşağıdaki gibidir:

a) Güvenlik Politikası : Bilgi güvenliğini arttırıcı kurallar ve yönetim tavsiyelerini içerir.

b)Organizasyonel Güvenlik: Kurum içindeki bilgi güvenliği yönetimini kolaylaştırır.

c)Varlık Sınıflandırması ve Denetim: Varlıkların envanterini çıkartılması ve bu varlıkları etkin bir şekilde korunmasını sağlar.

d)Personel Güvenliği: İnsan hatası, hırsızlık, dolandırıcılık ya da ekipmanın amacı dışında kullanılması gibi riskleri en aza indirmesini sağlar.

e)Fiziksel ve Çevresel Güvenlik: Saldırıyı, kalite kaybını ya da endüstriyel vasıtaların ve verinin bozulmasını engeller.

f)İletişim ve Operasyonel Yönetim: Bilgi işleme donanımlarının yeterli ve güvenilir olduğunun kontrolünü sağlar.

g)Erişim Kontrolü: Bilgiye erişimin kontrolünü sağlar.

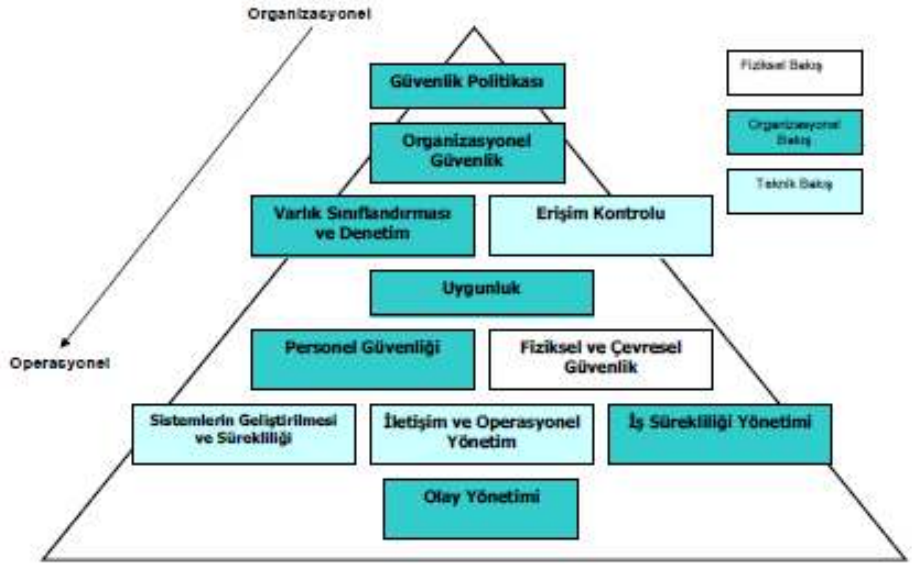
h)Sistemlerin Geliştirilmesi ve Sürekliliği: Güvenliğin bilgi sistemlerinin içine dâhil edilmesini sağlar.

ı)Olay yönetimi: Güvenlik ihlallerinin ne şekilde ele alınacağına yönelik tavsiyeler verir.

i)İş Sürekliliği Yönetimi: İş kesintilerini ve etkilerini azaltmak ve şirketin esas işlemlerini arıza ve büyük felaketlerden korunmasına yardımcı olur.

j)Uygunluk: Herhangi bir yasal ihlal ve güvenlik koşulları ile ilgili ihlallerden kaçınmasına yardımcı olur.

Aşağıdaki diyagram 11 ana başlığı gösterir. Her bir ana başlık; yönetimsel, teknik ve fiziksel ölçütler etrafında kurulmuş farklı konuları ele alır ve tepeden aşağıya doğru türetilir. Etkisi yönetim seviyesinden operasyonel seviyeye doğru hissedilir[3].



Şekil 2. BGYS kontrolleri şeması [3]

3.2 Bilgi Güvenliği Yönetim Sistemiyle İlgili Yanlış Algılamalar ve Olması Gerekenler

Bilgi güvenliği yönetişimi konusunda yasal bir düzenleme ve zorunluluk olmaması ülkemizde faaliyet gösteren kamu kurumları ve özel sektörde bilgi güvenliği yönetişiminin çok az sayıdaki kurumda uygulanmasına yol açmaktadır. Yasal eksiklik, bilgi güvenliği yönetiminin uygun bir şekilde yapılandırılmasına da engel olmaktadır. Bu durumda, Bilgi Güvenliği Yönetim Sistemi kurmak isteyen kurumlarda görev yapan yönetici ve personelde genellikle aşağıdaki yanlış algılamalar olmaktadır:

a) BGYS'nin kapsamı bilgi işlem birimidir.
b) BGYS'yi kurmaktan ve yürütmekten sorumlu üst düzey yönetici bilgi işlem birimi başkanıdır.
c) BGYS bir bilgi teknolojileri projesidir.
d) BGYS'nin sadece ve doğrudan bilgi işlem birimi ile bağlantısı vardır.

e) BGYS'nin sadece ve doğrudan güvenlik teknolojileri ile bağlantısı vardır.
f) BGYS bir yazılım/donanım/servis tedarik projesidir.
g) BGYS, tamamen başka bir kuruma yaptırılabilen bir projedir.

Bu cümlelerin doğrusu ise şu şekilde olmalıdır:

a) BGYS'nin kapsamı nihai olarak kurumun tamamıdır.
b) BGYS'yi kurmaktan ve yürütmekten sorumlu yönetici kurumun en üst düzey yöneticisidir.
c) BGYS bir bilgi teknolojileri projesi değildir. Bir bilgi güvenliği projesidir.
d) BGYS'nin kurumun tüm birimleri ve süreçleri ile ilişkisi vardır.
e) BGYS kapsamında güvenlik teknolojilerinden faydalanılır.
f) BGYS kapsamında yazılım/donanım/ servis tedariki yapılabilir.
g) BGYS kurulması için başka bir kurumdan danışmanlık hizmeti alınabilir. Ancak BGYS'yi asıl kurması gereken kurumun kendisidir [4].

3.3 ISO 27001 Bilgi Güvenliği Yönetim Sistemi Kurmanın Yararları

a)Bilgi varlıklarının farkına varma: Hangi bilgi varlıklarının olduğunu anlar, değerinin farkına varır.

b)Sahip olduğu varlıkları koruyabilme: Kuracağı kontroller ile koruma metotlarını belirler ve uygulayarak korur.

c)İş sürekliliği: Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.

d)İlgili taraflar ile barış halinde olma: Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.

*e)*Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
*f)*Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.
*g)*Çalışanların motivasyonunu arttırır.
h)Yasal takipleri önler.
*ı)*Yüksek itibar sağlar [1].

3.4 ISO 17799 Standardı Kimler İçindir?

BS 7799 / ISO 17799 / ISO 27001 kamu veya özel tüm şirket ve organizasyonların ihtiyaçlarını karşılamaktadır. Şirketin büyüklüğüne ve birincil öncelik durumlarına göre standardın hangi bölümlerini kullanması gerektiği aşağıda Çizelge 2 de görülmektedir.

Çizelge 2. Standartların kullanımı [3]

Şirket Tipi	Büyüklük	Birincil Öncelik	Standardın Kullanımı
Küçük İşletme ve Organizasyon	200 çalışandan az	Yönetimin ilgisini bilgi güvenliğine çekmek	Güvenlik konularını kapsayan ISO 17799 yönetim temel olarak alınmalıdır.
Orta Boy İşletmeler	5000 çalışandan az	Uygulanabilir kollektif güvenlik kültürü oluşturmak	Bilgi güvenliği politikası oluşturmak için uygulanma içeren bir standart kullanılmalı.
Büyük İşletmeler	5000 çalışandan çok	Süreç sonunda güvenlik sertifikası almak	Şirket içi güvenlik referans belgesi için BS 7799-2 kullanılmalı.

Sektörel olarak firmaların risk durumlarına bakıldığında tarım, inşaat, gıda gibi alanlarda çalışan firmaların düşük ölçekli; otomotiv, kimya, enerji gibi alanda çalışan firmaların orta ölçekli; kamu kurumları, savunma sanayi, biyomedikal, elektronik gibi çalışma alanlarındaki firmaların yüksek ölçekli olduğu Şekil 3 de görülmektedir.

Düşük	Orta	Yüksek
▪Tarım	▪Otomotiv	▪Kamu Kurumları
▪İnşaat ve Emlak	▪Kimya	▪Uzay, Havacılık ve Savunma
▪Gıda ve Tütün	▪Enerji	▪Biyomedikal
▪Endüstriyel Ekipman	▪Nakliyat	▪Elektronik
▪Maden	▪Toptan Satış	▪Finans ve Banka
		▪Sağlık
		▪Bilgi
		▪Perakende Satış
		▪İlaç

Şekil 3. Sektörel risk grupları [3]

3.5 Kurulum Adımları

BGYS konusunda temel başvuru kaynakları ISO/IEC 27001 ve ISO/IEC 27002 standartlarıdır. BGYS kurulumu öncesinde bu standartların mutlaka anlaşılması gerekmektedir. BGYS kurulumu TS ISO/IEC 27001:2005'teki "4.2.1 BGYS'nin Kurulması" ve TS 13268-1 "4.3 BGYS'nin kurulması" başlıkları altında detaylı olarak açıklanmaktadır [1].
BGYS kurulumunda sırasıyla izlenmesi gereken adımlar şöyledir:

a)Kapsam Belirleme

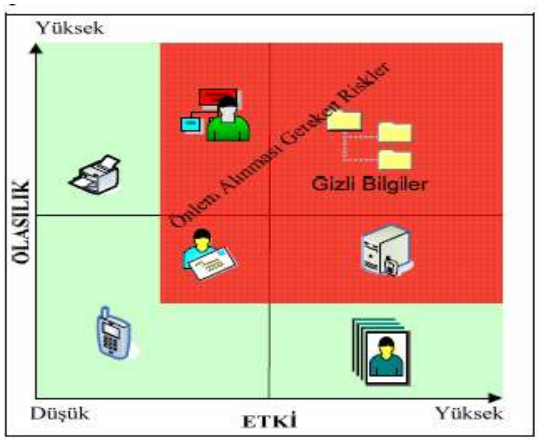
BGYS'nin kapsamı ve sınırları belirlenmelidir. BGYS'nin kapsamı kurumun belli bir kısmı olabileceği gibi, kurumun bütünü de olabilir. Her iki durumda da, kurumun BGYS kapsamını ve sınırlarını eksiksiz ve doğru bir biçimde tanımlaması gerekmektedir. Mesela kurum içindeki bir bölüm ya da bir bölümün verdiği tek bir hizmet için BGYS hayata geçirilebilir. BGYS kapsamı, üst yönetimin niyeti ve kurumun bilgi güvenliği hedefleri dikkate alınarak belirlenir. ISO/IEC 27001 ve ISO/IEC 27002 standartlarının bu konuda belli bir yönlendirmesi veya zorlaması söz konusu değildir. Kapsam belirlenirken BGYS dışında bırakılan varlıklarla, bu söz konusu varlıkların hangi sebeplerle dışarıda bırakıldıklarını kurumun gerekçeleriyle açıklayabilmesi gerekmektedir. Bu adımın sonunda bir kapsam dokümanı yayınlanmalı ve üst yönetim tarafından onaylanmalıdır.

b)BGYS Politikası

BGYS politikası, hedefleri ortaya koyan, yönetime yön veren ve harekete geçiren, hangi riskin değerlendirmeye alınacağına ilişkin risk yönetim kapsamı ve kriterini belirleyen bir çerçeve sunmalıdır. Politikanın amacına ulaşmasında yönetim, politika içerik maddelerin uygulamaya geçirilmesinde kararlı olmalı ve bunu çalışanlara hissettirmelidir.

c)Risk Değerlendirme Yaklaşımı

Bilgi güvenliği politikası temel alınarak sistematik bir risk değerlendirme yaklaşımı belirlenmelidir. Seçilen risk değerlendirme metodu kıyaslanabilir ve tekrarlanabilir sonuçlar üretmelidir. Bu adımda kabul edilebilecek risk seviyeleri belirlenmeli ve bunlar için ölçütler geliştirilmelidir. Örneğin Şekil 4 deki risk değerlendirme haritasında önlem alınması gereken bilgiler etki derecesine ve risk olasılığına göre seçilmiştir. Her kurum kendine uygun bir metot seçmekte serbesttir.



Şekil 4. Risk değerlendirme haritası [5]

d)Risk Belirleme

Korunması gereken varlıkları tehdit eden riskler, bir önceki basamak olan Risk Değerlendirme Yaklaşımında belirlenen yöntem kullanılarak tespit edilmelidir. Risk değerlendirme işinin esasını BGYS içerisindeki tüm varlıkların tanımlanması, yani varlık envanterinin çıkarılması oluşturur. Kurum BGYS kapsamına dâhil edeceği tüm varlıkların sahiplerini, türünü ve önem

derecesini bir döküm listesi şeklinde belgelemelidir. Bir varlığın önem derecesini belirlemek için bu varlığın

gizliliğine, bütünlüğüne ve kullanılabilirliğine gelecek zararın kuruma yapacağı etkinin derecesini baştan ortaya koymak gerekmektedir. Örnek olarak, çok gizli bir bilginin açığa çıkması kuruma büyük zararlar verebilecekken aynı gizli bilginin kullanılamaz hale gelmesi ilkine nazaran büyük zarar vermeyebilir.

e)Risk Analizi ve Derecelendirilmesi

Kurum/şirketlerde risk analizleri yapılırken çoğunlukla karşılaşılan riskler:

1. Yazılımlar için uygulama geliştirme ve test ortamlarının ayrı olarak bulunmaması, canlı sistemle birlikte olması,
2. Bilgi güvenliği sorumluluklarının atanmamış olması,
3. Varlık envanteri eksiklikleri,
4. Güvenlik olaylarını, zayıflıklarını ve yazılım arızalarını raporlama süreçlerinin olmaması,
5. Personel eksikliği,
6. Personel eksikliğine bağlı olarak görevlerin ayrılığı prensibinin uygulanamamasıdır [6].

Risk analizi yaparken bu risklere neden olan tehdit ve açıklıklardan yola çıkılmalıdır. Risk, açıklığın bir tehdit tarafından kullanılmasıyla oluşur. Riskin derecelendirilmesi veya değerinin belirlenebilmesi için öncelikle tehdidin gerçekleşme olasılığı ile etki derecesi hesaplanmalıdır. Bunlar sayısal değerler kullanılarak hesaplanabileceği gibi rakamlarla ifadenin zor olduğu durumlarda düşük, orta, yüksek gibi sözel değerlerle belirlenebilir.

Tüm bu hesaplama ve değerlemeler uygulanmakta olan mevcut kontroller de dikkate alınarak yapılmalıdır. Kontroller risk değerini azaltabilir. Sonunda bir risk değerlendirme sonuç raporu yayınlanmalıdır.

f)Risk İşleme

Bu adımda risk değerlendirme sonuç raporundan yola çıkılarak uygun risk işleme (*risk treatment*) yöntemleri belirlenmelidir. Belli bir risk karşısında dört farklı tavır alınabilir:

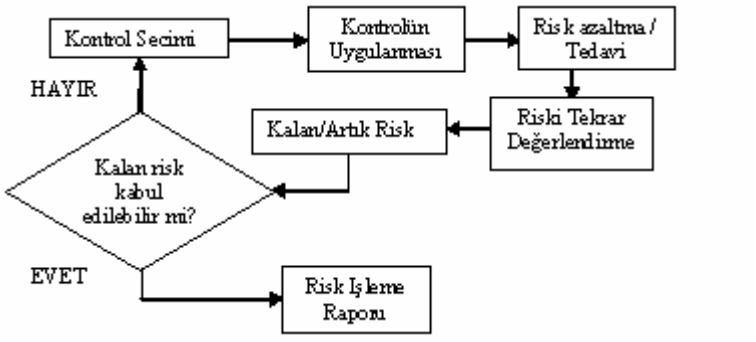
1. Uygun kontroller uygulanarak riskin ortadan kaldırılması veya kabul edilebilir seviyeye düşürülmesi,
2. Riskin oluşmasına neden olan faktörleri ortadan kaldırarak riskten kaçınılması,
3. Riskin sigorta şirketleri veya tedarikçiler gibi kurum dışındaki taraflara aktarılması,
4. Kurum politikalarına ve risk kabul ölçütlerine uyması şartıyla riskin objektif bir biçimde ve bilerek kabul edilmesidir.

g)Kontrol Seçimi

Risk işleme süreci sonuçlarına uygun kontrol ve kontrol hedeflerinin seçilmesi gerekir. TS ISO/IEC 17799:2005'te bu kontrollerden detaylı bir biçimde bahsedilmektedir. Kurum kendisine ek olarak başka kontroller de seçmekte serbesttir. TS ISO/IEC 17799:2005'te bulunan kontroller, sektör tecrübelerinden faydalanmak suretiyle, standart etki alanlarında olabildiğince geniş kapsamlı olarak belirlenmiş olsa da dış kaynaklı kontrollere ihtiyaç olabilmektedir.

h)Artık Risk Onayı

Risk işleme süreci sonrasında geriye kalan ve artık risk (*residual risk*) olarak adlandırılan riskler, kabul edilen riskler veya tamamen ortadan kaldırılamayan risklerdir. Kurum üst yönetimi artık riskler için onay vermelidir. Bu adım sonunda artık risk onay belgesi oluşturulmalıdır. Risk yönetim sürecinde yapılan kontrol seçimi sonucunda artık riski azaltmaya yönelik bir akış diyagramı Şekil 5 de görülmektedir.



Şekil 5.Risk yönetimi süreci [7]

ı)Yönetim Onayı

Risk yönetimi adımlarını geçtikten sonra BGYS işletimi ve uygulamasını yapmak için yönetimden onay almak gerekmektedir.

i)Uygulanabilirlik Bildirgesi

Son olarak risklere karşı seçilen kontrolleri içeren bir Uygulanabilirlik Bildirgesi hazırlanarak BGYS kurulum işi tamamlanır. Uygulanabilirlik Bildirgesi Kontrol Seçimi basamağında seçilen kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatmalıdır. TS ISO/IEC 27001 EK-A'dan seçilmeyen kontrollerin neler olduğu ile bunların seçilmeme gerekçeleri de Uygulanabilirlik Bildirgesinde verilmelidir.

3.6 ISO 27001 sertifikası nasıl alınabilir?

ISO 27001 standardının tüm gereklerinin yerine getirilmesini takiben dış denetim için başvurulabilir. Bu denetimin akredite bir sertifikalandırma kurumu tarafından gerçekleştirilmesi gerekir. Denetimi gerçekleştirecek kurum önce dokümantasyonu gözden geçirir. Bu dokümantasyon güvenlik politikasını, risk değerlendirmesi dokümanlarını, risk eylem planını, uygunluk beyanı ve güvenlik prosedürlerini içermelidir. Bu incelemeyi takiben, ileriki bir tarihte denetçiler tarafından yerinde denetim gerçekleştirilir. Bu denetimde, kuruluşunuzun büyüklüğüne ve işinizin tipine uygun kontrollerin, tarafınızca hazırlanmış bulunan prosedürlerde tanımladığınız şekilde yapılıp yapılmadığı gözden geçirilir. Başarılı bir denetimi takiben ISO 27001 sertifikası alınır. Alınan sertifikadan sonra yılda bir ya da iki kez, firmanın belirleyeceği periyotlara göre yenilemeye yönelik gözden geçirme tetkikleri gerçekleştirilir. Alınan belge 3 yıl geçerlidir ve 3. yılın sonunda yeniden belgelendirme tetkiki yapılarak süreç içerisindeki gelişmeleriniz gözden geçirilir[9].

Bulgular

4- BAZI KAMU KURUMLARINDA BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ YÖNETİMİ ÖRNEKLERİ VE TS ISO/IEC 17799 UYGULAMALARI

"E-dönüşüm Türkiye" projesi Başbakanlığa ait 2003/12 sayılı genelgesi ile başlamış, 2003/48 sayılı genelge ile de DPT projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile görevlendirilmiştir. Bu bağlamda çalışmalarına başlayan DPT Bilgi Toplumu Dairesi, "E-dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi"ni yayınlamıştır. Rehber'de kamu kurumlarında bilgi güvenliği yönetim sistemlerinin kurulmasının önemi anlatılmıştır. Kamu kurumlarını bağlayıcı nitelikteki bu dokümanla, kamu kurumlarında uygulamalar başlanmış ama tüm kurumların entegresi gerçekleşmemiştir. Kurumlar kendi iletişim ağlarını kullanarak e-dönüşüme kısmen başlamıştır[8].

a)MERNİS Projesi

Ülkemizde İçişleri Bakanlığı, Nüfus ve Vatandaşlık Genel Müdürlüğü tarafından yürütülen, Merkezi Nüfus İdaresi (MERNİS) ve Kimlik Paylaşımı Sistemi (KPS) internetten gelebilecek saldırılara karşı firewall ile korunurken Atak Tespit ve Önleme Sistemi URL filtreleme,Anti virüs, Gateway ve Antispam özelliklerini barındırmaktadır. Taşra bağlantısı ise Telekom'dan kiralanan özel hatlar ile sağlanıyor ve bu hatların internet ile hiçbir bağlantısı bulunmamaktadır. Tamamıyla kapalı bir ağ olan MERNİS yazılımına kullanıcı adı ve parola ile girilebilmektedir. Bütün yapılan işlemlerin geri izleme bilgisi tutulurken bir sorun çıkması halinde sistemin devamlılığı için veriler Felaket Yedekleme Merkezinde (FYM) güncellenmektedir. İki ayrı veri tabanı olan MERNİS ve KPS arasında IP tabanlı bir erişim bulunmamaktadır. KPS'ye kötü amaçlı bir erişim olsa bile MERNİS'e KPS üzerinde ulaşmak mümkün değildir. Sunulan web servislerinde Web Servis Güvenliği (WS-Web Security) alt yapısı kullanılmaktadır[8].

b)UYAP Projesi

Adalet Bakanlığı'nın kullandığı intranet içinde çalışan bir sistem olan Ulusal Yargı Ağı projesinde (UYAP), uygulama katmanı erişimi birden fazla güvenlik duvarı ve saldırı tespit sistemleri tarafından denetlenmektedir. Sistemin güvenliği dışarıdan gelebilecek saldırılara karşı donanım (Güvenlik Duvarı, Anahtar, Yönlendirici, Saldırı Tespit Sistemi (IDS)) ve yazılımlar (Güvenlik Duvarı yazılımı, Saldırı Önleme Sistemi Yazılımı, Anti virüs Yazılımı, EPO yazılımı) ile sağlanmaktadır[8].

c)POLNET Projesi

Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı'nın geliştirdiği Polis Bilgisayar Ağı (PolNet) projesinde hassas olarak nitelendirilen veriler, dış dünyadan tamamen yalıtılmış olup, gerekli işlemler için daha önceden belirlenmiş sistem kullanıcılarının kullanımın sunulmaktadır. Sistemin güvenliği, oluşturulan belirli standartlar ve talimatlar doğrultusunda sağlanırken noktadan noktaya erişim şifreli olarak gerçekleştirilmektedir[8].

d)SAĞLIK BAKANLIĞI Projesi

Sağlık Bakanlığı, bilgi sistemlerinde bilgi sistemlerinde paylaşılan idari, mali ve klinik verilerin güvenliğinin ve iş devamlılığının sağlanması, güvenlik ihlalinden kaynaklanabilecek kanuni risklerin en aza indirilmesi, yatırımların ve kurumun itibarının korunması için bütün kurumlarında bilgi sistemlerinin güvenliğinin sağlanması konusunda standartlar belirlenmiştir. Bakanlığın Bilgi Güvenliği Politikası, genel olarak; e-posta güvenliği, anti

virüs sistemleri, şifreleme gibi 23 ana başlık altında toplanan metot ve kurallardan oluşmaktadır[8]. Sağlık Bakanlığının ISO 27001:2005 BGYS sertifikası alma çalışmaları devam etmektedir.

5- TARTIŞMA VE SONUÇ

Yapılan bu çalışma, BGYS'nin kurulum aşamaları uzun bir süreç olsa da önemli olduğu ve kurumlar bazında bilgi güvenliği ve bilginin daha iyi nasıl korunacağı konusunda standartlaşmanın olması gerektiği fakat TS ISO/IEC 17799:2005'nin kamu ya da özel kurumların bu standartlaşma konusunda serbest bıraktığı görülmektedir.

ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı planlanması ve kurulum aşamaları zaman ve emek kaybı gibi gözükse de uzun vadede fayda sağlar. Sistemin yaygınlaşmasında özel ve kamu sektöründe sistemi kurmak isteyen idarecilere ve sistemin sağlıklı işleyebilmesi için çalışanların da özverili davranması gerektiği anlaşılmaktadır.

Ülkemizde ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardına sahip kamu kuruluşu bulunmadığı ama Sağlık Bakanlığının sertifika alma çabalarının devam ettiği görülmektedir. Bu standardın kurumsal bazda faydalarının anlaşılması ve kurum yöneticilerinin konu hakkında bilinçlendirilmesiyle birlikte sertifika almaya çalışan ve bu sertifikayı almaya hak kazanan kurumların sayısının artacağı düşünülmektedir.

KAYNAKLAR

[1]http://www.bilgiguvenligi.gov.tr (2009.10.10)
D.Önel, A.Dinçkan,"Bilgi Güvenliği Yönetim Sistemi Kurulumu",Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(TÜBİTAK UEKAE),2007.

[2]http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/cok-katmanli-iso-27001sureci.html?Itemid=6 (2009.10.15)
F.Ottekin,"ÇokKatmanlı ISO 27001 Süreci", Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(TÜBİTAK-UEKAE),2008.

[3] http://www.tbd.org.tr/webler/kamubiby/raporlarPDF/RP4-2006.pdf (2010.01.04),
M.Tora,A.Ş.Ohri,A.Coşkunsakarya,A.Yazıcı,B.Uyukçuoğlu,B.DayıoğluD.Soyer,E.Ersoy,E.Demirbağ,M.Erdoğan,M.S.Uçum,N.Özalp, S.Altınsoy,Ü.Ayçiçeği,"E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları",TBD Kamu-BİB Bilişim Platformu VIII 4. Çalışma Grubu Sonuç Raporu,2004.

[4] http://www.bilgiguvenligi.gov.tr/teknikyazilar-kategorisi/iso-iec-27001-2005-ve-bilgi-guvenligi-yonetisimi-turkiye-analizi.html (2009.10.16)
B.Karabacak, "ISO/IEC 27001:2005 ve Bilgi Güvenliği Yönetişimi – Türkiye Analizi". Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(TÜBİTAK-UEKAE), 2008.

[5] Y.Vural, Ş.Sağıroğlu. "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme",Gazi Üniv. Müh. Mim. Fak. Dergisi ,23-(2), 507-522, 2008.

[6] M.Çetinkaya, **Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi**, Yüksek Lisans Tezi ,İstanbul Kültür Üniversitesi,Fen Bilimleri Enstitüsü,2008.

[7] http://www.itmsdays.com/sunumlar.php (2010.01.04)
K.Atsan,"ISO/ IEC 27001 Bilgi Güvenliği Yönetim Sistemi& Belgelendirme Semineri",2009 .

[8] B.Yıldız,**Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması**,Yüksek Lisans Tezi, GYTE.Gebze Yüksek Teknoloji Enstitüsü, 2007.

[9] http://www.cio-club.net/page_1215526874265.html (2009.12.28)
C.İ. Alpar ,"Bilgi Güvenliği Yönetim Sistemi ISO 27001", Kalite Yolculuğu ,CIO Club Der.26-30, 2009.