TS ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİMİ STANDARDI KAPSAMINDA BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN KURULMASI VE BİLGİ GÜVENLİĞİ RİSK ANALİZİ

Kurumsal bilgi güvenliğinde en önemli ve etkili önlem kurum çalışanlarının bilgi güvenliği konusunda farkındalıklarının ve bilinç düzeyinin arttırılmasıdır. Bu nedenle kurumsal bilgi güvenliğinin sağlanmasında yapılacak olan teknolojik yatırımlar yanında kurum çalışanlarının da bu konuda eğitilmesi önem taşımaktadır.

Hasan YILMAZ
İç Denetçi,
İstanbul Üniversitesi

ÖZET: *Makalede bilgi güvenliğinin önemine vurgu yapmak, kurumlarda bilgi güvenliğini tehdit eden unsurlar ve buna karşı alınabilecek önlemlerin ortaya konulması, bu itibarla TS ISO/IEC 27001 Standardı kapsamında Bilgi Güvenliği Yönetim Sisteminin (BGYS) kurulmasına ve son olarak süreç tabanlı bir model üzerinden bilgi güvenliğini tehdit eden risklerin analizine yönelik bir çalışmaya yer verilmesi amaçlanmıştır.*

Makalenin I inci bölümünde Bilgi güvenliği kavramsal çerçevesi, II nci bölümünde Kurumsal bilgi güvenliğinin önemi, III üncü bölümünde TS ISO/IEC 27001 Standardı kapsamında Bilgi Güvenliği Yönetim Sisteminin kurulması, Bilgi güvenliği yönetim sistemi için risk analizi başlığını taşıyan IV üncü bölüm altında ise modellenmiş olan bir süreç üzerinden risk analizi çalışmasına yer verilmiştir.

ANAHTAR KELİMELER: *Veri, enformasyon, bilgi, bilgi güvenliği, siber saldırı, sosyal mühendislik, mahremiyet artırıcı teknolojiler, elektronik imza, akıllı kartlar, bilgi güvenliği yönetim sistemi, TS ISO/IEC 27001, PUKÖ döngüsü, bilgi güvenliği risk analizi,*

GİRİŞ

İçinde bulunduğumuz 21 inci yüzyılın ilk çeyreğinde bilişim sistemlerinin, ağ teknolojilerinin kullanım alanlarının hızla artması ve özellikle bulut bilişimin birçok işletmede, kamu kurum ve kuruluşunda kullanılıyor olması, üretilen ve işletilen bilginin *güvenliğinin sağlanmasını da zorunlu* hale getirmiştir. Kurum ve işletmelerde bilgi güvenliğinin önemi ve tüm paydaşların bu yöndeki bilinç düzeyi de her geçen gün atmakla birlikte, "Kurumuma/şirketime ait bilgiyi nasıl korumalıyım, bilgi güvenliğimi nasıl sağlayabilirim?" vb. gibi sorular halâ güncelliğini korumaktadır. Makalemizde bu sorulara cevap olabilmek amacıyla, TS ISO/IEC 27001, etkili bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulması ve yönetilmesi için gerekli adım-

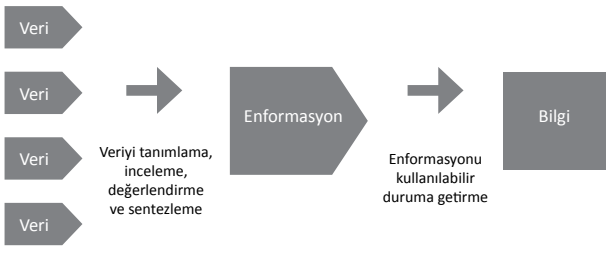
lara ve özellikle atılması gereken en önemli adım olan risk analizi yapılmasına yönelik olarak bir risk analiz modeli önerilmektedir.

I. BİLGİ GÜVENLİĞİ KAVRAMSAL ÇERÇEVE

A. Bilgi ve Bilgi Güvenliği Tanım

Bilgi güvenliğinin tanımını yapmadan önce 'Bilgi' kavramının önemli olduğu ve hızla arttığı gerçeğinden yola çıkarak, bilginin tanımının açık ve anlaşılır bir şekilde verilmesi gerekir. Bilgi, kağıt veya başka ortamlar üzerine kaydedilmiş, anlaşılabilen ve iletilebilen veriler topluluğudur veya zihinde herhangi bir biçimde resmi veya gayri resmi olarak iletilen, kaydedilen, yayınlanan fikirlerin gerçek ve hayali ürünleridir.[1]

Bilgi, enformasyon ve verinin üst seviyesidir. Bilgi kısaca "anlamlandırılmış enformasyon" olarak tanımlanmaktadır. Enformasyonu kullanılabilir ve işe yarar bir faaliyete dönüştürme işlemi yaptığımız takdirde enformasyon bilgi halini almaktadır. Örnek olarak, telefon numaralarını veri olarak düşünürsek, bu telefon numaralarından oluşturulmuş anlamlı bir telefon rehberi bir enformasyondur. Bu telefon rehberinde gördüğümüz bir numarayı tanıyarak, bu numaranın bir arkadaşımıza ait olduğunu ve bu kişiyi uzun zamandır aramadığımız gerektiğini düşünmemiz ise bir bilgidir. Enformasyonu tanımlayıp, inceleme, değerlendirme, sentezleme ve sonunda bir karar verme sürecinden geçirip uygulayarak bilgiye ulaşılmış olunur.[2]



Şekil 1. Verilerin bilgiye dönüşmesi (Kaynak: Yazar)

Bilgi güvenliği ise, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.[3] Bir diğer tanıma göre bilgi güvenliği, diskte, iletişim ağında, yedekleme ünitelerinde ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasıdır.[4] Bilgi güvenliği ile ilgili tanımları çoğaltmak mümkün olmakla birlikte bu tanımların bir kaçını aşağıdaki gibi sıralayabiliriz.

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.[5]

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 tanımlanabilir.[6]

Bilgi güvenliği; kurumdaki işlerin sürekliliğinin sağlanması, işlerde meydana gelebilecek aksaklıkların azaltılması ve yatırımlardan gelecek faydanın artırılması için bilginin geniş çaplı tehditlerden korunmasını sağlar. 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 SAĞSAN, Mustafa, Gelişmişliğin Vazgeçilmez Unsuru: Ulusal Bilgi Politikası,http://www.baskent.edu.tr/~msagsan/ downloads/UBP.pdf, Erişim tarihi:24/05/2014

2 OK, Kerem, Bilgi ve Bilgi Yönetimine Giriş, 1. Baskı, Papatya Yayıncılık Eğitim, İstanbul, Ekim 2013, s.21

3 CANBEK Gürol, SAĞIROĞLU Şeref, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt: 9, Sayı:3, 2006, s.165

4 Türkiye Bilişim Derneği, Bilişim Sistemleri Güvenliği El Kitabı, Sürüm 1.0, Ankara, Mayıs 2006, s.3

5 ÇETİNKAYA, Mehtap, Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması, Akademik Bilişim 2008, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak- 01 Şubat 2008, s.511

6 VURAL Yılmaz, SAĞIROĞLU Şeref, Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt 23, No 2, Ankara, 2008, s.509

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

- Gizlilik (Confidentiality)
- Bütünlük (Integrity)
- Kullanılabilirlik (Availability)

Bu kavramları biraz daha açacak olursak;

Gizlilik; bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanabilir. Bir diğer tarif ile gizlilik bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir. Bütünlük; bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük; Bilginin doğruluğunun ve tamlığının sağlanmasıdır. Bilginin içeriğinin değiştirilmemiş ve hiçbir bölümünün silinmemiş ya da yok edilmemiş olmasıdır. Kullanılabilirlik; bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.[7]

Bunun dışında sorumluluk, erişim denetimi, güvenilirlik ve emniyet etkenleri de bilgi güvenliğini destekleyen unsurlardır. Sorumluluk; belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirleme yeteneğidir. Erişim denetimi; bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir. Güvenilirlik; bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir. Emniyet; bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda, kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları önleme tedbirleridir. [8]

Bilgi güvenliğinin sağlanması için bilgi varlıklarının korunması gerekmektedir. Bir kurum veya kuruluşun kâr etmek, katma değer sağlamak, rekabet oluşturmak ve kurumsal sürdürülebilirliğini sağlamak amacıyla sahip olduğu veya sahip olması gereken ürün, pazar, teknoloji ve organizasyona ait bilgilerin tümü bilgi varlıkları olarak tanımlanabilir. Bu bilgi varlıklarının fiziksel olarak korunması için, fiziksel güvenliğin, transfer edilmesi gereken bilgilerin sağlanması için iletişim güvenliğinin, bilgisayar sistemlerine erişimlerin kontrol edilmesi için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir.[9]

B. Kişisel ve Kurumsal Veri (Bilgi) Güvenliği ve Tehditlere Karşı Alınabilecek Önlemler

Kişisel veri, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilgili her türlü veri olarak tanımlanmaktadır. Bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, cihaz kimlikleri, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri kapsamındadır.

Kişisel verilerin korunması hakkı, temel insan hak ve özgürlükleri arasında yer almakta olup, insanın şahsiyetinin korunması, hukuk devleti ilkesi ve demokrasinin derinlik kazanması açısından hayati öneme sahiptir. Kişisel veriler dâhil, özel hayatın anayasal güvence ile koruma altına alınmasında temel amaç, insan kişiliğinin serbestçe gelişmesine imkân vermek, kişiye kendisi ve yakınları ile baş başa kalabileceği, devlet veya başkaları tarafından rahatsız edilemeyeceği özerk bir alan sağlamaktır.

Kişisel verilerin korunması hakkı son kırk yılda büyük önem kazanmıştır. Bunda, bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte veri toplama ve bunları otomatik olarak işleme kapasitelerindeki artış ile bu artışa dayalı olarak kişilerin özel hayat mahremiyet

7 http://www.belgelendirme.com.tr/belgelendirme-standartlari/iso-27001-standart/175-bilgi-guvenligi-nedir, Erişim tarihi: 14/05/2014

8 CANBEK Gürol, SAĞIROĞLU Şeref, a.g.e., s.170

9 BAYKARA Muhammet, DAŞ Resul, KARADOĞAN İsmail, Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensicsand Security (ISDFS'13), Elazığ, 20-21 May 2013, s.238

alanının daha savunmasız hale gelmesi önemli bir etkendir. Özellikle, bilişim teknolojilerindeki gelişmeler sonucunda;

- Geleneksel yöntemlerle mümkün olmayan çok sayıda verinin toplanabilmesi,
- Daha önce dağınık yapılarca toplanan ve birbirinden ilişkisiz şekilde tutulan pek çok verinin merkezi olarak bir araya getirilmesi,
- Verilerin ileri teknolojik imkânlarla ve veri eşleştirme (data matching) ve veri madenciliği (data mining) gibi tekniklerle analize tabi tutulmak suretiyle, veriden yeni veriler üretme kapasitesinin artması,
- Verilere erişim, paylaşım ve transferin kolaylaşması ve maliyetinin düşmesi,
- Kişisel verilerin ticari işletmeler için kıymetli bir varlık ve ticari meta niteliği kazanması neticesinde özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşmış olması,
- Yabancı ülke istihbarat birimlerinin, terör ve suç örgütlerinin kişisel verileri ele geçirme veya bu sistemlere zarar verme yönündeki faaliyet ve saldırılarının artması,
- Banka ve kredi kartı dolandırıcılıkları başta olmak üzere, kişisel verileri hedef alan veya bunlar kullanılmak suretiyle işlenen suç olaylarının artması gibi hususlar kişilerin mahremiyet alanını önemli derecede daraltmış ve kişisel verilerin korunması ihtiyacını en üst noktaya taşımıştır.[10]

Kişisel bilgi güvenliği önlemi olarak aşağıda maddeler halinde verilen siber saldırı türlerine karşı çeşitli güvenlik önlemlerinin alınması tavsiye edilebilir:

- Program manipülasyonu,
- Sahtekârlık ve taklit,
- Erişim araçlarının çalınması,
- Kimlik çalma,
- Ticari bilgi çalma,
- İstihbarat amaçlı faaliyetler,
- Takip ve gözetleme,
- Hackleme,
- Virüsler, solucanlar (worms), truva atları (Slammer, MsBlaster, Sobig vb.),
- Ajan yazılım (spyware),
- Spam,
- Hizmeti durduran saldırılar

Tüm bu siber saldırı türleri bilinmeli, kişisel farkındalık ve bilgi güvenliği bilinci geliştirilmeli ve bu gibi saldırılar için gerekli korumayı sağlayan yazılımsal ve donanımsal destek üniteleriyle kişisel bilgi güvenliği sağlanmalıdır.[11]

Yukarıdaki siber saldırı türleri dışında kişisel ve kurumsal bilgi güvenliğini tehdit eden "Sosyal mühendislik saldırıları" ciddiye alınması gereken önemli bir tehdittir. Bir kurumdaki güvenlik seviyesini belirlemek için en zayıf halkaya bakılır. Bilgi güvenliği konusunda en zayıf halka ise insan faktörüdür. Teknik olarak ne kadar önlem alınırsa alınsın, bilinçsiz bir kullanıcının bulunduğu bir ortamda güvenlik sağlamak pek kolay olmayacaktır. İnsan faktörünü kullanan saldırı tekniklerinden ya da kişiyi etkileme ve ikna yöntemlerinden faydalanarak normal koşullarda bireylerin gizlemeleri / paylaşmamaları gereken bilgileri bir şekilde ele geçirme sanatı Sosyal mühendislik olarak ifade edilir.[12]

Kişisel veri hırsızlıkları, fiziksel ve bilgi işlem güvenliğine yeterince önem verilmemesi, dizüstü bilgisayar hırsızlıkları, korsan faaliyetler, şirket çalışanlarının veri sızdırması gibi farklı şekillerde gerçekleşebilmektedir. Siber suç ve veri hırsızlıklarında farkındalığı artırmaya yönelik olarak son yıllarda önleyici, caydırıcılığı artırıcı ve koruyucu birtakım önlemler alınmaktadır. Bu tedbirlerden önleyici nitelikte olanların başarısı, yalnızca bilgi teknolojileri okuryazarlığının artırılması ile mümkün değildir. Bireyin farklı ortamlardaki davranışlarının mahremiyete yönelik etkilerinin farkında olabilmesi ve tehlikeleri öngörebilmesi oldukça önemlidir. Bu sebeple, kişilerin mağduriyete uğramadan önce neler yapmaları gerektiği konusunda bilgilendirilmeleri ve bilinçlendirilmeleri faaliyetleri önleyici niteliktedir.

Mahremiyet artıcı teknolojiler, kimlik doğrulamada sağladığı avantaj nedeniyle mahremiyetin korunmasında *elektronik imza* ve güvenlik ve veri gizliliğinin

10 T.C. Cumhurbaşkanlığı, Devlet Denetleme Kurulu, 27/11/2013, 2013/3 sayılı Denetim Raporu, s.778,779

11 BAYKARA Muhammet, DAŞ Resul, KARADOĞAN İsmail, a.g.e., s.238

12 http://www.bilgimikoruyorum.org.tr/?b321_sosyal_muhendislik_giris, Erişim tarihi:11/06/2014

sağlanmasında akıllı kartlar koruma ve özellikle maddi zararın azaltılmasında günümüzde yaygınlaşmaya başlayan tedbirlerdendir. Koruyucu nitelikteki bu tedbirler aşağıda incelenmektedir.

Mahremiyet artırıcı teknolojiler: Temel amacı, mahremiyet kanunlarının ya da ilkelerinin uygulanmasına yardımcı olmak, kişiyi belirlenebilir kılan verilerin toplanması veya bu verilerin daha ileri düzeylerde işlenmesini mümkün olduğunca aza indirgemek olan teknolojik çözüm araçlarına mahremiyet artırıcı teknolojiler denilmektedir. Bu teknolojiler, kullanıcıya verilerinin çevrimiçi ortamda ifşa edilmesi, yayılması ve kullanılması riskine karşı kontrol imkânı sağlamaktadır. Bu kontrol, herhangi bir ağ üzerindeki tarayıcılarda veya e-postalarda kişisel verilerin belirli durum ve şartlarda anonim hale getirilmesi, çerezlerin veya diğer izleme teknolojilerinin filtrelenmesi, verinin yayılması şartlarının belirlenmesi, verilerin şifrelenmesi vb. seçenekler ile gerçekleşmektedir.

Elektronik imza (e-İmza): Kimlik doğrulama, neredeyse bütün hukuki işlemlerin gerçekleştirilmesinde ilk adımı oluşturmaktadır. Bu nedenle elektronik hizmet sunumunda kimlik doğrulama araçlarından sağlıklı olanlar tercih edilmelidir. Elektronik imza; bilginin, orijinalliği bozulmadan, tarafların kimliğini de belirleyebilecek şekilde elektronik ortamda karşı tarafa aktarılmasını garanti eden bir teknolojidir.

Akıllı kartlar: Akıllı kartlar, elektronik imza altyapılarında ve gizliliğinin korunması gereken bilgilerin taşınmasında sıklıkla kullanılan donanımlardır. Bu kartlar, gizli bilgilerin taşınması amacıyla kullanılabileceği gibi, şifreli yayınlara erişim gibi elektronik şifreleme vb. bazı özel fonksiyonları yerine getirmede veya GSM telefonları veya kredi kartlarında kullanılabilir. Akıllı kartlar, gizli bilgilerin korunması ve bu bilgilerle işlem yapılması konusunda güvenli yapılardır. Bu nedenle söz konusu kartlar, elektronik imzanın gizliliğinin korunması gereken bazı uygulamalarında (örneğin, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verilerin korunmasında) yaygın olarak kullanılmaktadır. Bu kartlar, kimlik tespiti gerektiren hizmetlerin sunumunda da oldukça güvenli araçlar olarak kabul edilmektedir.[13]

Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir. Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Kurumsal bilgi güvenliği insan faktörü, eğitim, teknoloji gibi birçok faktörün etki ettiği tek bir çatı altında yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. [14]

Bilgi güvenliğinin sağlanması için bilgi varlıklarının korunması gerekmektedir. Bir kurum veya kuruluşun kâr etmek, katma değer sağlamak, rekabet oluşturmak ve kurumsal sürdürülebilirliğini sağlamak amacıyla sahip olduğu veya sahip olması gereken ürün, pazar, teknoloji ve organizasyona ait bilgilerin tümü bilgi varlıkları olarak tanımlanabilir. Bu bilgi varlıklarının fiziksel olarak korunması için, fiziksel güvenliğin, transfer edilmesi gereken bilgilerin sağlanması için iletişim güvenliğinin, bilgisayar sistemlerine erişimlerin kontrol edilmesi için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir.

Bilgisayar güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için duruma uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir. Bu politikalar;

- Etkinliklerin sorgulanması,
- Erişimlerin izlenmesi,
- Değişikliklerin kayıtlarının tutulup değerlendirilmesi,
- Silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir.

13 KARİMİ Oldouz, KORKMAZ Adem, Kişisel Verilerin Korunması, inet-tr.org.tr/inetconf18/bildiri/63.doc, , s.6-7, Erişim tarihi: 14/05/2014

14 VURAL Yılmaz, SAĞIROĞLU Şeref, a.g.e., s.509

Bilgisayar teknolojilerinde yer alan bilgisayar güvenliğinin amacı ise: «Kişi ve kurumların bu teknolojileri kullanırken karşılaşabilecekleri tehdit ve tehlikelerin incelemelerinin yapılarak gerekli önlemlerin önceden alınmasıdır». Bilgi ve bilgisayar güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan «Güvenlik Mühendisliği»nin bir alt alanı olarak görülmektedir. Bilgisayar güvenliği geniş anlamda bir koruyucu mekanizma olarak düşünüldüğünde, kişisel veya kurumsal bilgisayarlar için genel olarak aşağıdaki maddelerin hepsinin veya bazılarının uygulanması gerekmektedir:

- Kötücül yazılım (virüs, backdoors vb.) koruma yazılımlarının kurulu olması
- Bu yazılımların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması
- Bilgisayarda şifre korumalı ekran koruyucu kullanılması
- Kurmuş olduğunuz yazılımların paylaşıma açık olup olmadığının kontrol edilmesi
- Bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması
- Kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi
- Bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi
- Disk paylaşımlarında dikkatli olunması
- İnternet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi
- Önemli belgelerin parola ile korunması veya şifreli olarak saklanması
- Gizli veya önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi
- Kullanılmadığı zaman internet erişiminin kapatılması
- Önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması
- İşletim sistemi güncelleştirmelerinin yapılması gibi önlemler, basit gibi gözükebilecek ama hayat kurtaracak önlemlerden bazılarıdır. [15]

15 BAYKARA Muhammet, DAŞ Resul, KARADOĞAN İsmail, a.g.e., s.238

II. KURUMSAL BİLGİ GÜVENLİĞİNİN ÖNEMİ

Bilgisayar ağlarının ve internetin yaygın olarak kullanılmaya başlanmasıyla Bilgi Güvenliği oldukça önemli hale gelmiştir. Kurumların çoğunlukla bilgiye, teknolojiye ve sistemlere bağımlı olmasından dolayı bilgi güvenliği yaşamsal önemdedir ve bilgi varlıklarının zarar görmekten korunması gereksinimi de bundan kaynaklanmaktadır. Ayrıca bilgi güvenliğinin bir kurumsal yönetim unsuru olması ve bilgi teknolojileri güvenliği, fiziksel güvenlik, risk yönetimi, iş sürekliliği ile yasa ve yönetmeliklere uyum gibi unsurlarla yakından ilgili olması ve böylece çalışanlara, iş ortaklarına, müşterilere ve topluma yönelik çeşitli yükümlülükleri desteklemesi nedeniyle de önceliğinin yüksek olması gerektiği daha net anlaşılabilir. Bilgi güvenliği bazen riskli olabilecek durumlara, iş ilişkilerine ve pazarlara adım atarken ve bunları sürdürürken de daha güvenli olmamızı olanak tanır. Bilgi güvenliği kaynaklı olaylardan doğan kayıpların minimum seviyeye indirilmesi mali sonuçları olumlu yönde etkiler. Ayrıca güvenilir, açık ve dürüst kurum imajını da destekler.[16]

Uluslararası denetim ve danışmanlık firması Ernst & Young'ın 2008 yılında yaptığı Küresel Bilgi Güvenliği anketine, Türkiye'nin de içinde bulunduğu 50 ülke ve 1.400 kuruluş katıldı ankette, bilgi güvenliğinin doğru uygulanmasının kurum itibarını doğrudan etkilediği sonucu ortaya çıkmıştır. Katılımcıların yüzde 85'i bir bilgi güvenliği ihlali durumunda ortaya çıkan durumun, marka kimliği ve itibarına zarar verdiğini savunurken, yüzde 72'si gelir kaybına neden olduğuna değinmiştir.[17]

Bilgi güvenliği konusundaki en yakın örnek ise Sony Play Station ağına sızan hackerların uç güvenlik duvarlarını da aşıp 77 milyon kullanıcının, kullanıcı adını ve şifrelerini çalmasıdır. Yaşanan bu olayın zararının 170 milyon dolar olduğu bildirilmiştir.

16 SÜDERBAY, Gökhan, Bilgi Güvenliği Neden Bu kadar Önemli ve Gerekli, http://www.tubiyad.org/ PublicationsDetail.aspx?PublicationID=56, Erişim tarihi:27/05/2014

17 CAN, Murat,ISO ve Standartlara Genel Bakış, ISO 27001'ye göre Bilgi ve Bilgi Güvenliği-Bölüm 1http://www.cozumpark.com/blogs/cobit-itil/archive/2012/06/02/ts-iso-iec-27001-2005-bilgi-guvenligi-yonetim-sistemi-ve-puko-modeli-bolum-2.aspx, Erişim tarihi:28/05/2014

Ernst & Young›ın yıllık anket sonuçlarına göre, şirketler bilgi güvenliği hakkındaki risk ortamının değiştiğinin farkında. Ankete yanıt verenlerin yüzde 80'i dış tehditlerin artmasıyla risk faktörünün de yükseldiği konusunda hemfikir. Buna ek olarak katılımcıların yüzde 31'i bilgi güvenliklerini tehdit eden vakaların geçen yıla göre artış gösterdiğini, yüzde 59'u aynı oranda kaldığını, yüzde 10'u da düşüş gösterdiğini belirtti. Bilgi güvenliğine yönelik tehditlerin sıklığı ve güvenlik vakalarının artması bu konuda şirketlerin görebileceği potansiyel zararın da arttığına işaret ediyor. ABD›nin resmi rakamları da kişisel tanımlanabilir bilgilerin izinsiz paylaşımı, 2011 yılında yüzde 19 arttığını belirterek bilgi sızıntısının vardığı boyutu ortaya koymaktadır. [18]

Yukarıda verilen anket ve örnekler, bilgi güvenliği zafiyetinin ortaya çıkardığı itibar ve gelir kaybının düzeyini ortaya koyması ve bilgi güvenliğinin önemini vurgulaması açısından son derece çarpıcı veriler sunmaktadır.

III. TS ISO/IEC 27001 STANDARDI KAPSAMINDA BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN KURULMASI

1.TS ISO/IEC 27001 Standardı Nedir?

ISO[19] 27000 ailesinden olan ve ISO/IEC[20] 17799'un yerine geçen ISO/IEC 270001Standardı, bilgi güvenliği standardı, bilgi güvenliği yönetiminin daha verimli hale getirilmesi için tasarlanmıştır. Orijinal ismi "Information Technology - Security Technigues - Information Security Nanagement Systems - Requirements" olan bu standardın Türk Standartları Enstitüsü (TSE) tarafından Türkçeye çevirisi "Bilgi Teknolojisi- Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler" olarak yapılmıştır.[21] Teknik bir standart olmayan ISO/IEC 27001 kurum, kuruluş ve işletmelerin güvenlik gereksinimlerini tanımlar, ancak gerçekleştirme şeklini onlara bırakır. Başka bir deyişle, kurum içi veya dışı yanlış ve kötü amaçlı kullanıma karşı bilginin korunması için gerekli beklentileri tanımlar. TSE'nin yayınlamış olduğu TS ISO/IEC 270001 adlı kitapçıkta bu standardın hazırlanış amacı; Bilgi Güvenliği Yönetim Sistemini (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak olarak açıklanmıştır.[22]

2. Bilgi Güvenliği Yönetim Sistemi Tanım

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

18 ERNST&YOUNG, 27/12/2012 tarihli Basın Bülteni, http://www.ey.com/Publication/vwLUAssets$FILE/Bilgi Guvenligi%20BB_EB.pdf, Erişim tarihi:28/05/2014, s.1

19 ISO: (International Organization for Standardization); Uluslararası Standartlar Teşkilâtı, Uluslararası Elektroteknik Komisyonu'nun çalışma sahasına giren elektrik ve elektronik mühendisliği konuları dışında, bütün teknik ve teknik dışı dallardaki standartların belirlenmesi çalışmalarını yürütmek gayesiyle 1946'da Cenevre'de kurulan uluslararası teşkilât. (Kaynak:http://tr.wikipedia.org/wiki/ISO_standart, Erişim tarihi:03/06/2014)

20 IEC:(International Electrotechnical Commission);1906 yılında elektrik, elektronik ve ilgili teknolojiler konusunda uluslararası standard hazırlama çalışmalarına başlayan ve halen 51 üyesi bulunan IEC (www.iec.ch)'ye TSE 1956 yılında üye olmuştur.(Kaynak:http://inndustry.blogcu.com/iso-ve-iec-nedir/5279272 (Erişim tarihi:03/06/2014)

21 ISO/IEC 27001 Uluslararası gösterim şeklidir. TS ISO/IEC 27001 ise TSE'nin resmi olarak kabul edip yayınladığı Türkçe versiyonu belirtir. İkisi arasında içerik farkı yoktur. 27001, ISO/IEC 27001 ve TS ISO/IEC 27001 aynı standardı ifade eder. ISO/IEC 27001:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir. Makalemizde bu yazım çeşitleri birbirinin yerine kullanılmıştır.

22 ERSOY, Eren Veysel, ISO/IEC 27001 Bilgi Güvenliği Standardı, ODTÜ Yayıncılık, Ankara, Şubat 2012, s.14,15

ve standartların gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir.[23]

Bilgi Güvenliği Yönetim Sistemi (BGYS); Bilginin gizliliğini, bütünlüğünü ve kesintisiz kullanılabilirliğini (erişilebilirliğini) sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetimce kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünüdür.[24]

BGYS kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar. Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart 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. Bu da 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. Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, en iyi uygulamaları temel alan bir dizi standarttır ve organizasyonlara bilgi güvenliği programlarını uygularken ve yönetirken uymaları gereken kuralları temin eder.[25]

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.[26]

Tüm dünyada kabul edilen standart yaklaşımla bilgi güvenliğinin sağlanabilmesi için üç ana şartın yerine getirilmesi gerekmektedir. Bu şartlar; gizlilik (confidentiality), bütünlük (Integrity), kullanılabilirlik/erişilebilirlik (Availability) olarak sıralanabilir.

Gizlilik (confidentiality): Önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesi önlenmelidir ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınmalıdır.

Bütünlük (Integrity): Bilginin bir kısmının veya tümünün yetkili olmayan kişilerce değiştirilmesinin, silinmesinin ve bozulmasının önlenmesi gerekmektedir.

Kullanılabilirlik/erişilebilirlik (Availability): Bilgi veya bilgi sistemleri sürekli kullanıma hazır ve erişilebilir olmalıdır.[27]

TS ISO 27001 BGYS teknik bir süreçten daha çok bir yönetim sürecidir. BT Risklerinin mümkünse ortadan kaldırılmasını, değilse etkisinin düşürülmesini hedefler ve sürekli iyileştirme metodu olarak Planla, Uygula, Kontrol et, Önlem al (PUKÖ) döngüsünü temel alır.[28] Döngünün her bir bileşeninin ne anlam geldiği aşağıdaki gibi açıklanmaktadır.

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.

23 VURAL Yılmaz, SAĞIROĞLU Şeref,Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 2007,s.196

24 ERSOY, Eren Veysel, a.g.e., s.8

25 ÖZBEK, Çetin, Kurumsal Yönetim-Risk Yönetimi-İç Kontrol, Türkiye İç Denetim Enstitüsü Yayınları, Yayın no:3, Cilt no:2, 1. Baskı, İstanbul, Ekim 2012, s.1071

26 http://www.belgelendirme.com.tr/belgelendirme-standartlari/iso-27001-standart/182-iso-27001-nedir:, Erişim tarihi:28/05/2014

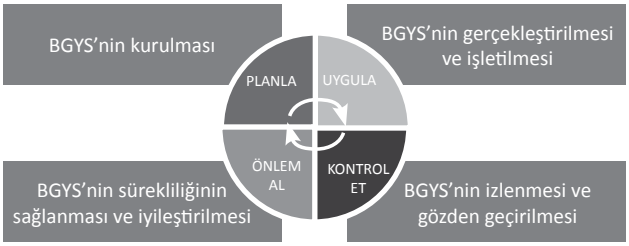
27 ERSOY, Eren Veysel, a.g.e. s.10

28 http://www.boydakbilisim.com/2014/05/ts-iso-iec-270012005-bilgi-güvenligi-yönetim-sistemi-denetimi-basari-ile-tamamlandi/, Erişim tarihi: 29/05/2014

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.[29]



Şekil 2. PUKÖ döngüsü modeli (Kaynak: Yazar)

3. Bilgi Güvenliği Yönetim Sisteminin Kurulumu Aşamaları

Bilgi Güvenliği Yönetim Sistemini uygulamak isteyen bir kurumda yapılması gerekenleri, aşamalar halinde aşağıdaki gibi özetleyebiliriz:

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

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.

29 MARTTİN Vedat, PEHLİVANİhsan, ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir inceleme, Mühendislik Bilimleri ve Tasarım DergisiCilt:1 Sayı:1,2010, s.50

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

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.

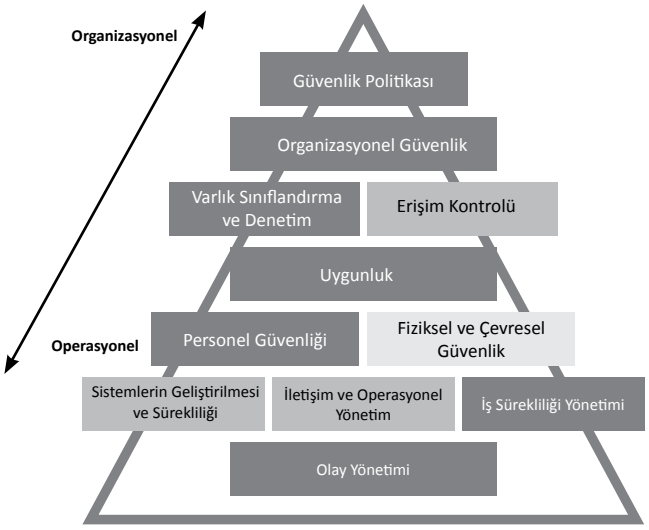
8) Bilgi sistemleri tedariki, geliştirme ve bakımı: Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı; doğru girilmiş 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.

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

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 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.[30]

BGYS'nin kurulma (kontrolleri) aşamalarını organizasyonel ve operasyonel boyutları aşağıdaki gibi şematize edilebilir.



Şekil 3. BGYS Kontrolleri Şeması
(Kaynak: MARTTİN Vedat, PEHLİVAN İhsan, a.g.e, s.51)

4. ISO/IEC 27001 BGYS'nin Kuruma Katkıları

- Kurum güvenlik politikalarını ve buna bağlı olarak bilgi güvenliğini yönetir.
- Bilgi varlıklarının farkına varılıp korunmasını sağlar.
- Kurumsal bilgi varlıklarının uygun bir şekilde korunmasını sağlar ve bu sayede, şirketin iş, zaman, para ve itibar kayıplarının önüne geçer.
- Bilgi kaynakları denetimiyle bilginin, gizlilik, erişilebilirlik ve bütünlüğünün korunması sayesinde bilgi güvenliğini sağlar.
- Tehdit ve riskleri yöneterek iş sürekliliğini sağlar.
- Yasa ve yönetmeliklere uyum sayesinde yasal takipleri önler.
- Kurumun, çalışanlarının ve birlikte iş yapılan 3. taraflarının güvenlik risklerini minimuma indirir.
- Eğitim ve sözleşmeler ile personel, yönetici ve üçüncü kişilerin bilgi güvenliği farkındalıklarını arttırır.
- Kurumum prestijini yükseltip rekabet avantajı sağlar.
- Güvenlik politikaları sayesinde, sistemlerin kötü amaçlar için kullanımını ve suistimalleri engeller.
- İş sürekliliğini sağlamak için geliştirilen kontroller ile kurumun iş ve finans kaybını minimize eder.
- Bilgi güvenliği ihlal olaylarını etkili bir şekilde yönetip kurumun iç-dış tehditlerden zarar görme risklerini minimize eder.
- Her türlü hukuka ve yasal düzenlemelere uyum sayesinde, kurumu olası hukuki yaptırımlara karşı korur.[31]

Bilgi Güvenliği Yönetim Sisteminin (BGYS) 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.[32]

5. 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 Yöne-

30 ŞEN Şenol, YERLİKAYA Tarık,ISO 27001 Kurumsal Bilgi Güvenliği Standardı, ab.org.tr/ab13/bildiri/216.doc, Erişim tarihi:02/06/2014

31 http://www.boydakbilisim.com/2014/05/ts-iso-iec-270012005-bilgi-guvenligi-yonetim-sistemi-denetimi-basari-ile-tamamlandi/, Erişim tarihi:29/05/2014

32 ŞEN Şenol, YERLİKAYA Tarık, a.g.e.

tim Sistemi kurmak isteyen kurumlarda görev yapan yönetici ve personelde genellikle aşağıdaki yanlış algılamalar olmaktadır: [33]

Yanlış Algılamalar	Olması Gerekenler
BGYS'nin kapsamı bilgi işlem birimidir.	BGYS'nin kapsamı nihai olarak kurumun tamamıdır.
BGYS'yi kurmaktan ve yürütmekten sorumlu üst düzey yönetici bilgi işlem birimi başkanıdır.	BGYS'yi kurmaktan ve yürütmekten sorumlu yönetici kurumun en üst düzey yöneticisidir.
BGYS bir bilgi teknolojileri projesidir.	BGYS bir bilgi teknolojileri projesi değildir. Bir bilgi güvenliği projesidir.
BGYS'nin sadece ve doğrudan bilgi işlem birimi ile bağlantısı vardır.	BGYS'nin kurumun tüm birimleri ve süreçleri ile ilişkisi vardır.
BGYS'nin sadece ve doğrudan güvenlik teknolojileri ile bağlantısı vardır.	BGYS kapsamında güvenlik teknolojilerinden faydalanılır.
BGYS bir yazılım/donanım/servis tedarik projesidir.	BGYS kapsamında yazılım/ donanım/ servis tedariki yapılabilir.
BGYS, tamamen başka bir kuruma yaptırılabilen bir projedir.	BGYS kurulması için başka bir kurumdan danışmanlık hizmeti alınabilir. Ancak BGYS'yi asıl kurması gereken kurumun kendisidir.

IV. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ İÇİN RİSK ANALİZİ

Risk önceden bilinen somut bir değer değil, bir olasılık değeridir. Bu nedenle risk analizi bir olasılık hesabıdır ve karmaşık bir süreç olabilmektedir. Bilgi teknolojileri söz konusu olduğunda, risk analizi sürecinin karmaşıklığı daha da artmaktadır. [34]

Temel olarak, nitel ve nicel olmak üzere iki tür risk analizi yöntemi vardır. Nitel yöntemlerde analiz; riski düşük, orta, yüksek şeklinde sıfatlar kullanarak sınıflandırmayla yapılır. Nicel yöntemlerde ise, matematiksel ve istatistiki ifadeler kullanılır ve sayısal değerler ortaya konur. Risk analizinde bu iki temel tür üzerinde geliştirilmiş çeşitli yöntemler kullanılır. Ayrıca bazı yöntemler, karma yapıdadır, yani iki yapıyı bir arada kullanmaktadır. Karma yapıdaki yöntemlerde bile, nitel veya nicel özelliklerden bir tanesi daha ağırlıklı olmakta, yöntem bu özelliğiyle daha nicel veya daha nitel olarak sınıflandırılabilmektedir. Kullandığı yöntem ister nitel, ister nicel olsun, genel olarak bütün risk analiz yöntemlerinin ana hedefi, toplam risk değerini tahmin etmektir. Birçok risk analizi ve yönetimi yöntemi olmasına karşın bunların genel anlamda birbirlerine üstünlükleri bulunmamakta ancak uygulayan organizasyonun ihtiyaçları çerçevesinde o organizasyon için en iyi olan yöntemin bulunması (önem taşımaktadır.) [35]

Bu makalemizde modellenmiş olan bir süreç üzerinden risk analizi yapılmaya çalışılacaktır. Bilgi teknolojileri açısından risk, basit bir olasılık değeri değildir. Risk, bir varlıktaki bir açıklığın bir tehdit tarafından kullanılma olasılığıdır. Böylece risk; varlık, açıklık ve tehdit olmak üzere üç adet girdiye bağımlıdır.
Risk = f (Varlık, Açıklık, Tehdit)

Formüldeki f fonksiyonu, risk modelini ifade etmektedir. Bu modelin üç adet temel girdisi vardır ve bu fonksiyonun (modelin) çıktısı da risk değeridir.

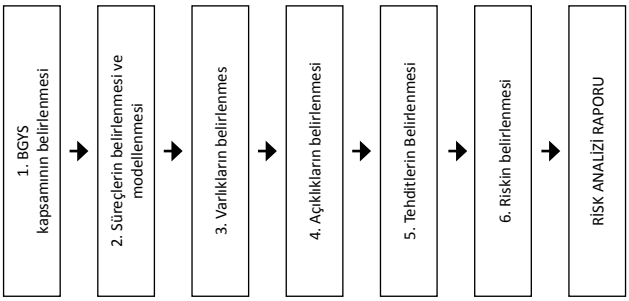
Risk analizi çalışmaları belirlenmiş olan BGYS kapsamı dâhilinde gerçekleştirilir. BGYS'nin kapsamı aynı zamanda risk analizinin de kapsamıdır. Aynı kapsamın, varlık envanterinin oluşturulması esnasında da dikkate alınması gerekir. Birçok BGYS çalışmasında kapsamın belirlenmesinin ardından, varlık envanteri oluşturulmasına geçilmektedir. Önerilen metotta, BGYS kapsamının belirlenmesinin ardından, varlık envanterine geçilmeden önce bu kapsam içerisinde yer alan süreçlerin ortaya konulması ve modellenmesi önerilmektedir. Süreçleri oluşturan yapıtaşları varlıklardır. Bu nedenle, süreçlerin belirlenmesi ve yazılı hale getirilmesi varlıkların daha sağlıklı ve eksiksiz bir şekilde belirlenmesini de sağlayacaktır. BGYS kapsamının belirlenmesinin ardından doğrudan varlık envanterinin oluşturulması aşamasına geçilmesi, bilgi işlem personelinin sadece donanım ve yazılımlara odaklanmasına yol açmaktadır. Önerilen metotta ise,

33 MARTTİN Vedat, PEHLİVAN İhsan, a.g.e., s.51,52

34 KARABACAK Bilge, ÖZKAN Dr. Sevgi, Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi, http://www.emo.org.tr/ekler/fa22e-2c8eca438e_ek.pdf, Erişim tarihi 03/06/2014

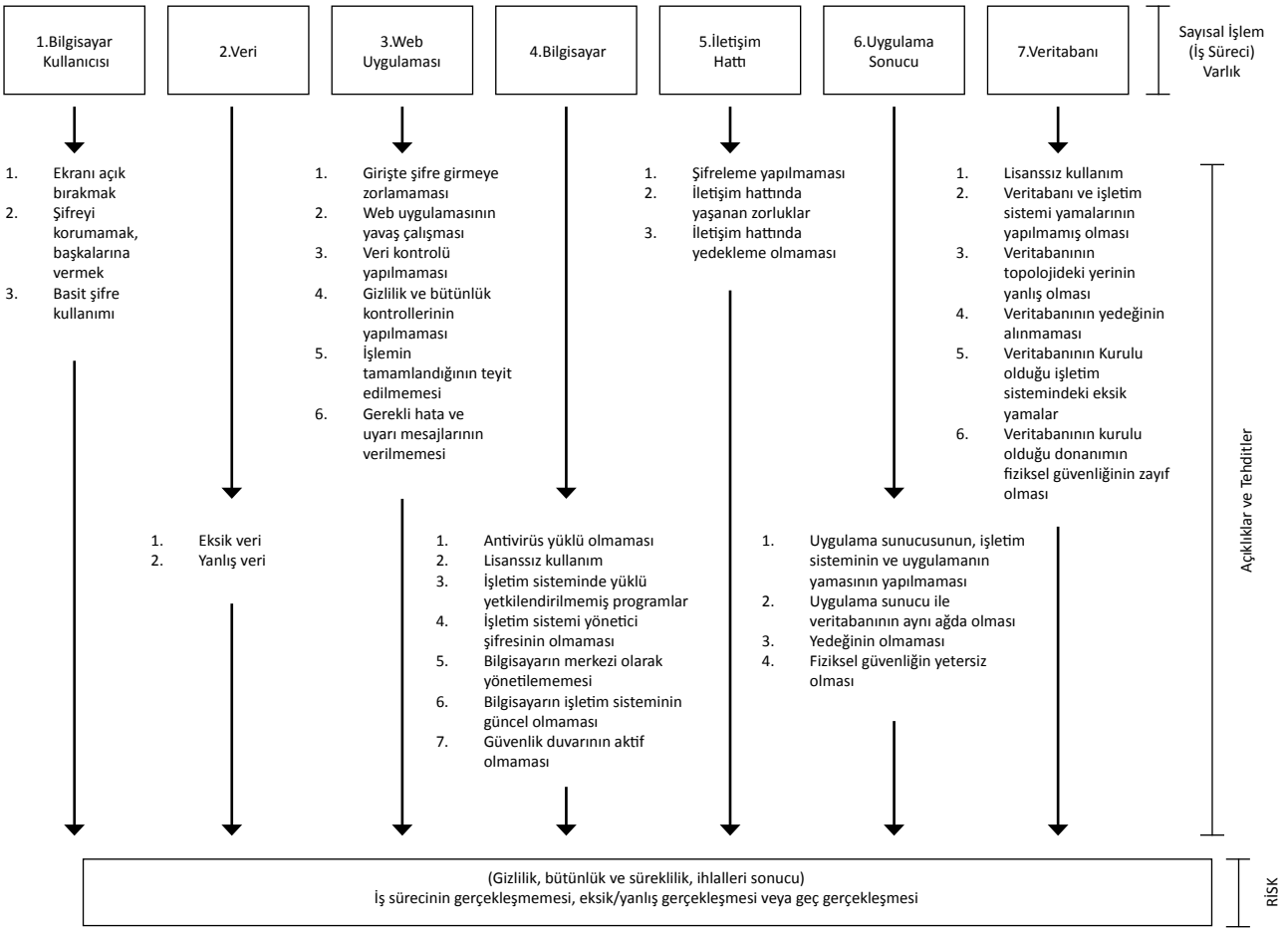
35 AKTAŞ F. Özden, SOĞUKPINAR İbrahim, Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım, http://eski.tbd.org.tr,Erişim tarihi:10/06/2014

modellenmiş süreçlerden yola çıkılarak belirlenmiş olan varlıklardaki açıklıklar ve bu açıklıklar kullanan tehditler ortaya konmaktadır. Risk analizinin son adımında ise, belirlenmiş olan varlık, açıklık ve tehditlere değerler verilerek risk hesaplanmakta ve risk analizi süreci tamamlanmaktadır. Önerilen risk analizi metodunun genel akış diyagramı Şekil 4'de verilmiştir.



Şekil 4. Öngörülen yöntemin genel akışı

Bir bilgi işlem aktivitesini veya bilgi işlem altyapısını kullanan bir bilgisayar kullanıcısının yaptığı işlemi modellemek akış diyagramları ile oldukça kolay olmaktadır. Akış diyagramları en çok bilinen ve uygulama kolaylığı olan süreç modelleme yöntemidir. Sistemin bütüncül yapısını göstermede ve bu yapı içerisinde işlerin ve bilginin akışını izlemede faydalıdır. Şekil-2'de bir bilgisayar kullanıcısının veri girişi modellenmiştir. Birçok kurumda, kurumun kritik bilgisini içerdiğinden dolayı veritabanları en kritik varlıklardır. Veritabanlarına veri girişi genellikle kurum personeli tarafından yapılan günlük bir iş sürecidir. Şekil 5'de bu kritik işlem yedi adet süreç kutusu kullanılarak akış diyagramı metodu ile basit bir şekilde modellenmiştir. Bu basit modelleme, veri giriş sürecinde hangi bilgi işlem elemanlarının kullanıldığını ortaya koymuştur.



Şekil 5. Örnek bir süreç modeli ve modelin kullanılarak risk analizi yapılması

Akış diyagramındaki her bir süreç kutusu aslında bir varlığa işaret etmektedir. Böylece akış diyagramı kullanarak hem varlıklar listelenmiş hem de bu varlıkların birbirleri ile olan ilişkileri ortaya konulmuştur. Özetlemek gerekirse, bilgisayar kullanıcısı, evraktaki veriyi bilgisayarındaki web uygulamasını kullanarak sayısallaştırır, bu aşamada, veri iletişim hattından geçerek uygulama sunucusuna gelir, uygulama sunucusu da yine iletişim hattını kullanarak veritabanına verinin yazılmasını sağlar. Bu işlemde bilgisayar kullanıcısı da dahil olmak üzere adı geçen her şey birer varlıktır. Varlıkların süreç içerisinde gösterilmesi ve listelenmesinin ardından ikinci aşama olarak bu varlıklardaki açıklıklar ve bu açıklıkları kullanabilecek tehditler ortaya konur. Bu da yine akış diyagramı kullanılarak yapılır. Makalenin başında bahsedildiği gibi klasik varlık envanteri oluşturulurken yapılan önemli hatalardan birisi olan, varlık envanterinde sadece teknik bileşenlerin geçmesi hatası tekrarlanmadığı için bilgisayar kullanıcısından, girilen verinin doğruluğuna ve kullanıcının bilgisayarına kadar birçok alanda açıklık ve tehditler saptanmış olur. Belirlenmiş olan her bir açıklık ve tehdit Şekil 5'de de gösterildiği gibi akış diyagramı kullanılarak modellenmiş olan sürecin gerçekleşmemesi, eksik/yanlış gerçekleşmesi veya geç gerçekleşmesi gibi birer sebep olacaktır. O halde, iş sürecinin her aşamasında varlıkları etkileyen tehditleri ve bu varlıklardaki açıklıkları engellemek gereklidir.

Şekil 5'de gösterilen adımların kapsam dahilindeki tüm süreçler için tamamlanması ile beraber, Şekil 4'deki genel akış diyagramındaki 2, 3, 4 ve 5 numaralı adımlar da gerçekleştirilmiş olacaktır. Bu aşamadan sonra, birçok kaynakta önerilen ve standart olarak kullanılan aşağıdaki formül ile risk değeri hesaplanır ve risk analizi tamamlanır.

Risk = Tehdidin etki derecesi x tehdidin gerçekleşme ihtimali

Risk analizi sürecinin bu son aşamasının da tamamlanması ile birlikte Şekil 5'deki 6 ve 7 numaralı adımlar tamamlanmış olacaktır. [36]

36 KARABACAK Bilge, ÖZKAN Dr., a.g.e

ISO 27001 standardı BGYS kurmak isteyen kuruluşun risk analizi çalışmasının ardından çeşitli kontrolleri devreye sokarak mevcut riskleri tedavi etmesini ve kabul edilebilir risk seviyesinin altına indirmesini şart koşmaktadır.[37]

IV- SONUÇ

Bilişim teknolojilerindeki baş döndürücü gelişmeler, bilginin bu teknolojiler sayesinde üretilmesi, işlenmesi, kullanılması ve paylaşılmasının saniyeler içerisinde gerçekleşebilmesi, buna paralel olarak bilgi güvenliğinin kontrolünün ve güvenliğinin sağlanmasını da zorunlu kılmaktadır. Bilgi güvenliği risklerinin tespit edilerek bilgi güvenliğinin sağlanmasında, bilgi teknolojileri alanında yatırım yapmak, korunma amaçlı birçok teknolojileri, yöntemlerinin kullanılması, TS ISO/IEC 27001 vb. gibi standartlar kapsamında Bilgi güvenliği yönetim sisteminin (BGYS) kurulması önem taşımaktadır.

Bunun yanında bilinmesi gereken bir husus var ki, o da Kurumsal bilgi güvenliğinde en önemli ve etkili önlem kurum çalışanlarının bilgi güvenliği konusunda farkındalıklarının ve bilinç düzeyinin arttırılmasıdır. Bu nedenle kurumsal bilgi güvenliğinin sağlanmasında yapılacak olan teknolojik yatırımlar yanında kurum çalışanlarının da bu konuda eğitilmesi önem taşımaktadır. Ancak bu sayede güvenlik teknolojileri yerinde ve zamanında kullanılabilecek ve bilgi güvenliğine ilişkin artık riskler kabul edilebilir düzeye çekilebilecektir.

37 ÇALIKUŞU Faruk, KARAMEHMET Bilge, DENİZCİ Dr.Ömer Mert, Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetimi Modeli, http://www.farukcalikusu.com/Bilgi-Guvenligi-Yonetim-Sistemi_BGYS.pdf, Erişim tarihi:10/06/2014

Kaynaklar

Kitaplar

1. OK, Kerem, Bilgi ve Bilgi Yönetimine Giriş, 1. Baskı, Papatya Yayıncılık Eğitim, İstanbul, Ekim 2013
2. ÖZBEK, Çetin, Kurumsal Yönetim-Risk Yönetimi-İç Kontrol, Türkiye İç Denetim Enstitüsü Yayınları, Yayın no:3, Cilt no:2, 1. Baskı, İstanbul, Ekim 2012
3. ERSOY, Eren Veysel, ISO/IEC 27001 Bilgi Güvenliği Standardı, ODTÜ Yayıncılık, Ankara, Şubat 2012
4. Türkiye Bilişim Derneği, Bilişim Sistemleri Güvenliği El Kitabı, Sürüm 1.0, Ankara, Mayıs 2006
5. VURAL Yılmaz, SAĞIROĞLU Şeref,, Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, Bildiriler Kitabı Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 2007

Makaleler

1. SAĞSAN, Mustafa, Gelişmişliğin Vazgeçilmez Unsuru: Ulusal Bilgi Politikası, http://www.baskent.edu.tr/~msagsan/downloads/UBP.pdf, Erişim tarihi:24/05/2014
2. CANBEK Gürol, SAĞIROĞLU Şeref, Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt: 9, Sayı:3, 2006
3. ÇETİNKAYA, Mehtap, Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması, Akademik Bilişim 2008, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak- 01 Şubat 2008
4. VURAL Yılmaz, SAĞIROĞLU Şeref, Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt 23, No 2, Ankara, 2008
5. BAYKARA Muhammet, DAŞ Resul, KARADOĞAN İsmail, Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensicsand Security (ISDFS'13), Elazığ, 20-21 May 2013
6. KARİMİ Oldouz, KORKMAZ Adem, Kişisel Verilerin Korunması, inet-tr.org.tr/inetconf18/bildiri/63.doc, , s.6-7, Erişim tarihi: 14/05/2014
7. SÜDERBAY, Gökhan, Bilgi Güvenliği Neden Bu kadar Önemli ve Gerekli, http://www.tubiyad.org/PublicationsDetail.aspx?PublicationID=56, Erişim tarihi:27/05/2014
8. CAN, Murat, ISO ve Standartlara Genel Bakış, ISO 27001'ye göre Bilgi ve Bilgi Güvenliği-Bölüm 1 http://www.cozumpark.com/blogs/cobit-itil/archive/2012/06/02/ts-iso-iec-27001-2005-bilgi-guvenligi-yonetim-sistemi-ve-puko-modeli-bolum-2.aspx, Erişim tarihi:28/05/2014
9. ŞEN Şenol, YERLİKAYA Tarık, ISO 27001 Kurumsal Bilgi Güvenliği Standardı, ab.org.tr/ab13/bildiri/216.doc, Erişim tarihi:02/06/2014
10. MARTTİN Vedat, PEHLİVAN İhsan, ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir inceleme, Mühendislik Bilimleri ve Tasarım Dergisi, Cilt:1 Sayı:1, 2010
11. KARABACAK Bilge, ÖZKAN Dr. Sevgi, Bilgi Güvenliği Yönetim Sistemi için Süreç Tabanlı Risk Analizi, http://www.emo.org.tr/ekler/fa22e2c8eca438e_ek.pdf, Erişim tarihi 03/06/2014
12. AKTAŞ F. Özden, SOĞUKPINAR İbrahim, Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım, http://eski.tbd.org.tr, Erişim tarihi:10/06/2014
13. ÇALIKUŞU Faruk, KARAMEHMET Bilge, DENİZCİ Dr.Ömer Mert, Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetimi Modeli, http://www.farukcalikusu.com/Bilgi-Guvenligi-Yonetim-Sistemi_BGYS.pdf, Erişim tarihi:10/06/2014

Rapor

T.C. Cumhurbaşkanlığı, Devlet Denetleme Kurulu, 27/11/2013, 2013/3 sayılı Denetim Raporu

Elektronik Kaynaklar

1. http://www.belgelendirme.com.tr/belgelendirme-standartlari/iso-27001-standart/175-bilgi-guvenligi-nedir, Erişim tarihi: 14/05/2014
2. http://www.bilgimikoruyorum.org.tr/?b321_sosyal_muhendislik_giris, Erişim tarihi: 11/06/2014
3. ERNST&YOUNG,27/12/2012 tarihli Basın Bülteni,http://www.ey.com/Publication/vwLUAssets$FILE/BilgiGuvenligi%20BB_EB.pdf, Erişim tarihi: 28/05/2014
4. http://www.belgelendirme.com.tr/belgelendirme-standartlari/iso-27001-standart/182-iso-27001-nedir:, Erişim tarihi:28/05/2014
5. http://www.boydakbilisim.com/2014/05/ts-iso-iec-270012005-bilgi-güvenligi-yönetim-sistemi-denetimi-basari-ile-tamamlandi/, Erişim tarihi: 29/05/2014