T.C.

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ

KURUMSAL BİLGİ GÜVENLİĞİ & COBIT

YÜKSEK LİSANS TEZİ

Hazırlayan

BİLAL ÖZCAN

Tez Danışmanı

Prof. Dr. ALİ OKATAN

Haziran 2009

İSTANBUL

T.C.

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bilgisayar Mühendisliği Anabilim Dalı Yönetim Bilişim Sistemleri Programı Yüksek Lisans öğrencisi **Bilal ÖZCAN** tarafından hazırlanan **"Kurumsal Bilgi Güvenliği & Cobit"** adlı bu çalışma jürimizce Yüksek Lisans Tezi olarak kabul edilmiştir.

Sınav Tarihi : 08.07.2009

(Jüri Üyesinin Ünvanı , Adı , Soyadı ve Kurumu) : İmzası :

Jüri Üyesi: Prof.Dr.Ali OKATAN
Danışman–HAL.Üni.Bilgisayar Müh.ABD Öğr.Üyesi .....

Jüri Üyesi : Prof.Dr.Bekir KARLIK
HAL.Üni.Bilgisayar Müh.ABD Öğr.Üyesi .....

Jüri Üyesi : Prof.Dr.Avni Y.ERYILMAZ
HAL.Üni.Endüstri Müh.ABD Öğr.Üyesi .....

Jüri Üyesi : Prof.Dr.Oya KALIPSIZ
Yeditepe Üniv.Öğr.Üyesi (Yedek) .....

ÖNSÖZ

Tez çalışmalarım boyunca değerli bilgileri ile bana destek olan tez danışmanım Prof. Dr. Ali OKATAN'a, beni yönlendiren dokümanlar sunan Bilgi Güvenlik Yöneticisi, Ender ŞAHİNARSLAN'a, tez çalışmalarım boyunca yardımlarını esirgemeyen Bilgisayar Mühendisi, Orhan TANRIKULU'na, zaman yönetimi ve motivasyon konusunda maddi manevi bana destek olan sevgili eşim Tuba ÖZCAN'a, kızım Sare ÖZCAN'a ve aileme teşekkür etmeyi borç bilirim.

Bilal ÖZCAN

Haziran/2009

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

KISALTMALAR

AC : Authorization Control
AI : Acquire and Implement
AICPA : The American Institute of Certified Public Accounts
BDDK : Bankacılık Düzenleme ve Denetleme Kurumu
BGYS : Bilgi Güvenliği Yönetim Sistemi
BSI : British Standards Institute
BT : Bilişim Teknolojileri
BTY : Bilişim Teknolojileri Yönetişimi
CBK : Common Body of Knowledge
CISSP : Certified Information Security Systems Professional
COBIT : Control Objectives for Information and Related Technologies
COSO : The Committee of Sponsoring Organizations of the Treadway Commission
DMZ : De Militarized Zone
DOM : Document Object Model
DS : Deliver and Support
GAO : The US General Accounting Office
HTML : Hyper Text Transfer Protocol
IEC : The International Electro Technical Organization
ISACA : Information Systems Audit and Control Association
ISO : International Organization for Standardization: Uluslararası Standartlar Teşkilâtı
IT : Information Technology
ITGI : The IT Governance Institute
JTC : Joint Technical Committee
ME : Monitor and Evaluate
OODA : Observe Orient Decide Act
OSI : Open Systems Interconnection, Birbirine Bağlı Açık Sistemler
OWASP : The Open Web Application Security Project
PO : Plan and Organize
PUKÖ : Planla Uygula Kontrol et Önlem al
TCB : Trusted Computing Base
TSE : Türk Standartları Enstitüsü
WASC : The Web Application Security Consortium
XML : Extensible Mark up Language
XSS : Cross Site Scripting

T.C.

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ

YÜKSEK LİSANS TEZİ

KURUMSAL BİLGİ GÜVENLİĞİ & COBIT

Hazırlayan: Bilal ÖZCAN

Tez Danışmanı: Prof. Dr. Ali OKATAN

Haziran 2009,İSTANBUL

ÖZET

Bu tez çalışmasında bilgi güvenliği kavramlarını genel olarak incelenmekle birlikte, bilgi güvenliğini zaafa uğratan güncel tehtidler açıklanmıştır. Kurumsal bilgi güvenliği ve standartları değerlendirilmiş olup kurumlarda bilgi güvenliğine yönelik risklerin önlenmesinde, bilgi güvenliği farkındalığının önemi ve oluşturma yöntemleri ile ilgili tavsiyeler sıralanmaktadır.

Günümüz iş dünyasında uygulanması kaçınılmaz hale gelen BGYS (Bilgi güvenliği yönetim sistemi) ve kurulum adımları detaylı bir şekilde açıklanmıştır. BGYS için gerekli faaliyetlerinin neler olduğu, nasıl uygulandığı, uygulamalar sırasında karşılaşılan sorunlar ve iş sürekliliğinin sağlanmasında izlenen yöntemler açıklanmaktadır.

Kurumlarda tüm departmanların bilgi teknolojilerine bağlı hale geldiği günümüzde, bilişim teknolojileri ekseninde kurumların vizyon ve stratejisini belirleyip yöneten Bilgi Teknolojileri İçin Kontrol Hedefleri, Türkiye'de son yıllarda gelişim göstermektedir. Ülkemizde yeni bir alan olan Bilgi Teknolojileri İçin Kontrol Hedefleri ve sağladığı faydalar hakkında değerlendirmeler yapılmaktadır.

Anahtar Kelimeler: Bilgi güvenliği, Kurumsal bilgi güvenliği, Bilgi güvenliği yönetim sistemi, Bilgi Teknolojileri İçin Kontrol Hedefleri

T.C.

HALİC UNIVERSITY

INSTITUTE OF NATURAL SCIENCES
MANAGEMENT OF INFORMATION SYSTEMS

MASTER THESIS

CORPORATE INFORMATION SECURITY & COBIT

Bilal ÖZCAN

Supervisor: Prof. Dr. Ali OKATAN

June 2009, İSTANBUL

ABSTRACT

In this thesis the information security concepts were investigated in general however current threats which will be damaged the information security were explained. Institutional information security and standards were appreciated, the recommendations in connection with the importance of the information security awareness and building up methods were arranged to prevent risks about the information security of the corporations.

It was given full particulars that the information security controls system which is in evitable in current business world and its installation steps. It was explained what required activities for the information security control system have been how they have carried out, the problems in the field of application and the methods for continuity of business.

At the present day, all departments of corporations have been depending on information Technologies. COBIT which has been managing vision and strategy of the corporations in the field of information technologies has developed in recent years in Turkey. It was assessed about COBIT and its advantages that is a new field in our country.

Keywords: Information security, corporate information security, Information Security Management System, Control Objectives for Information and Related Technology

1. GİRİŞ

Günümüzde ticari şirketler ve devlet kurumları işlerini sürdürebilmek için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin önemi artmış, sadece güvenli bir şekilde saklanması ve depolanması gelişen ihtiyaçlara cevap verememiş aynı zamanda bir yerden bir yere nakil edilmesi de kaçınılmaz bir ihtiyaç haline gelmiştir. Bilgiye olan bu bağımlılık bilginin korunması ihtiyacını gündeme getirmiştir. Bu anlamda bilgi, kurumun sahip olduğu varlıklar arasında çok önemli bir yere sahiptir. Bilgiye yönelik olası saldırılar, tahrip edilmesi, silinmesi, bütünlüğünün ve/veya gizliliğinin zarar görmesi, bilgi altyapısının bozulmasına ve bu da beraberinde işlerin aksamasına neden olmaktadır.

Bilgi, kurumdaki diğer varlıklar gibi, kurum için önem taşıyan ve bu nedenle de en iyi şekilde korunması gereken bir varlıktır. 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.

Kurumlarda BGYS (Bilgi Güvenliği Yönetim Sistemi) uygulanabilmesi için bilgi güvenliği kavramlarından önce bilgi teknolojileri sistemlerinin yönetim stratejilerinin neler olacağının belirlenmesi gerekmektedir. "Bilgi Teknolojileri Yönetim Sistemleri" olarak anılan COBIT, ISO ve COSO gibi standartların amacı, bilgi teknoloji hizmetlerinin müşterilere arzu edilen seviyede ulaşmasını sağlamak, bilgi teknolojileri sistemlerinin denetimini, gözlemlenebilirliğini, ölçeklenebilirliğini, işlevselliğini, verimliliğini, güvenilirliğini ve sürekliliğini sağlamaktır. Bilgi Güvenliği Yönetim Sistemi ise temel olarak aynı hedeflere atıflar yapsa da bilginin gizliliği, bütünlüğü ve kullanılabilirliği ile ilgilidir.

Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler:

- Gizlilik
- Bütünlük
- Kullanılabilirlik

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 için kısaca kazara veya kasıtlı olarak bilginin bozulmamasıdır.

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. (Önel ve Dinçkan, 2007, s:6)

Bilgi teknolojilerinin yaygınlaşması ile beraber bilgi üretimi de ciddi boyutlarda artış göstermiştir. Bilgi teknolojileri yaygınlaşmadan önce, bilginin büyük bir çoğunluğu basılı dokümanlarda iken, günümüzde bilgi teknolojileri tarafından işlenir duruma gelmiştir. Bu nedenle günümüzde bilgiye erişme imkânları geçmiş ile karşılaştırılamayacak seviyede artmıştır. Bu durum, birçok dezavantajı beraberinde getirmektedir. Bilgi teknolojileri üzerinde bilinçli veya bilinçsiz yapılan hataların çok ciddi sonuçlar doğurması olasıdır. Bilgi teknolojilerindeki açıklıklar ve dikkatsiz yapılandırmalar bilgiye yetkisiz erişime yol açabilir. Bu durumda bilginin yetkisiz imhası, değiştirilmesi ve görülmesi söz konusu olabilir. Geçmişte sadece fiziksel güvenliğin tesis edilmesi ile sağlanan bilgi güvenliği, günümüzde kurumların en çok zorlandıkları ihtiyaçların başında gelmektedir.

Birçok akademik kaynakta, bilgi güvenliğinin teknik ve teknolojik bir kavram olmadığı vurgulanmakta, bilgi güvenliğinin sağlanması için kurum kültürünün değiştirilmesi, kurum üst yöneticilerinin bilgi güvenliği ile ilgili süreçlerde rol alması gibi sosyal çalışmalara değinilmektedir.

Sosyal boyut içerisinde yer alan önemli parametrelerden birisi de bilgi güvenliğinin yasal boyutudur. Gelişmiş ülkelerde ülke çapında tüm kurumları bağlayan düzenleyici bilgi güvenliği yasaları mevcuttur. Ülkemizde, düzenleyici mevzuat konusunda çalışmalar devam etmektedir.

Ülkemizde doğrudan bilgi güvenliğini konu alan bir mevzuat altyapısı henüz bulunmamaktadır. Bankacılık ve haberleşme sektörlerini düzenleyen mevzuatta bilgi güvenliği bir unsur olarak geçmektedir. Ancak bu durum Ulusal Bilgi Güvenliği ile ilgili hususları düzenlemek için yeterli düzeyde değildir. Günümüzde, bilgi güvenliği ile ilgili hususları içeren genelgeler yürürlükteki kanun ve yönetmeliklere göre bilgi güvenliğine daha çok vurgu yapmaktadır. Ancak, bu genelgelerin dayanak olabileceği yönetmelik, tüzük ve kanun olmadığından dolayı genelgeler etkili olamamaktadır. Ülkemizde, bilgi güvenliği mevzuatı ile ilgili çalışmalar Bilgi Toplumu Stratejisi Eylem Planı içerisinde yer alan 87 numaralı eylem maddesi çerçevesinde ve Başbakanlık tarafından yürütülen e-devlet mevzuat çalışmaları kapsamında gerçekleştirilmektedir. (Karabacak, 2009)

Kurumlarda bilgi güvenliğinin sağlanması kurumun imajı, güvenilirliği ve faaliyetlerinin devamı açısından oldukça önemli bir hale gelmiştir. Bir kurum, maliyetine bakmaksızın paranın alabileceği en ileri güvenlik teknolojilerini kullanabilir, sistemleri tasarlayabilir ve adeta kendisini bir güvenlik çemberinden geçirebilir. Bu şekilde sadece en son teknolojiyi kullanarak üst seviyede güvenlik önlemleri alabilen bir kurumda bilgi güvenliğinin tamamen (%100) sağlanmış olduğundan bahsedilememektedir.

Güvenlik teknolojileri geliştirildikçe, olası teknik açıkları kullanmak/sömürmek zorlaşacağı için saldırganlar insan unsurunun zayıflıklarından faydalanma yoluna yönelmişlerdir. Bundan dolayı kurumlarda güvenliğin en zayıf halkasını insan unsuru oluşturmaktadır.

Güvenlik; teknolojiden önce insana yatırım yapılmasıyla, kurum çalışanların/bireylerin en üstten en alt çalışanına, hatta bilgi alış verişinde yaptığı varsa tedarikçileri, müşteri ve ziyaretçilerini bilgilendirmesi, onlar üzerinde bir bilgi güvenlik farkındalığı oluşturması, kendini geliştirmesi, bilgi güvenlik faaliyetlerinin benimsenmesi, önemsenmesi ve desteklemesi ile anlamlı hale gelebilir.

Bilgi güvenliği risklerinden korunmanın en iyi yolu bilgi teknolojilerine çok para harcamak ve korunma amaçlı teknolojileri daha çok kullanmaktan önce insanların bilinçlenmesi ve ihtiyaç duyulan güvenlik teknolojisinin doğru yer ve zamanda kullanmakla mümkün olabilir.

İnsan faktörüne bağlı bilgi güvenlik riskleri hiçbir zaman tamamen ortadan kaldırmak mümkün olmasa da iyi planlanmış bir farkındalık faaliyeti ile güvenlik risklerinin kabul edilebilir bir seviyeye çekilmesini sağlanabilir.

Türkiye'de son yıllarda yayılmakta olan COBIT, iş ihtiyaçlarına göre Bilgi Sistemleri'nin ne kadar hizmet verdiğinden emin olunmasını sağlayan öneriler bütününden oluşan bir çerçevedir. Türkiye'de Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından yayınlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" uyarınca bankalara COBIT'te yer alan usul ve esaslar uygulanmalıdır. (Artinyan, 2008, s:1)

Bankacılık sektöründe BDDK ana düzenleyicidir ve halen bu konuda ISACA 'nın Bilgi Teknolojileri İçin Kontrol Hedefleri'nin (COBIT) esas alınacağını Bilgi Sistemleri Denetimine İlişkin Yönetmelik 'te belirtmiş durumdadır. ISACA tarafından geliştirilen ve güncellenen Bilgi Teknolojileri İçin Kontrol Hedefleri (COBIT), "bilgi" denilen çağımızın son derece değerli olan varlığından en iyi ölçüde yararlanmak ve bilgi teknolojilerinin getiri/ risklerinin anlaşılması ve yönlendirilmesi için kullanışlı ve standart bir çerçeve işlevi görmektedir. Halen çok sayıda banka ve denetim kuruluşu bu konudaki çalışmalarını yürütmektedir. Bu kapsamda Bilgi Teknolojileri İçin Kontrol Hedefleri Türkiye'de son zamanlarda çok yaygınlaşmakta ve önem kazanmaktadır.

Bilgi Teknolojileri İçin Kontrol Hedefleri; bir kurumda farklı seviyelerde görev alan farklı yöneticiler ve çalışanların farklı gereksinimlerine yanıt bulmaya çalışır. Öncelikle üst yönetimi dikkate alırsak; Bilgi Teknolojileri İçin Kontrol Hedefleri bir BT organizasyonunun, en basta hizmet vermiş olduğu iş birimleriyle stratejik olarak aynı yönde ilerlemelerini güvence altına almaya ve stratejik uyum sağlamaya çalışır.

Bunun dışında, kurum içerisinde BT' nin özellikle yatırım amaçlı tercihler yapması ve çözümlerin oluşturularak uygulanmasında değer yaratma unsurunu fayda / maliyet ve iş odaklı olarak gerçekleştirmesi gibi isler yer alır.

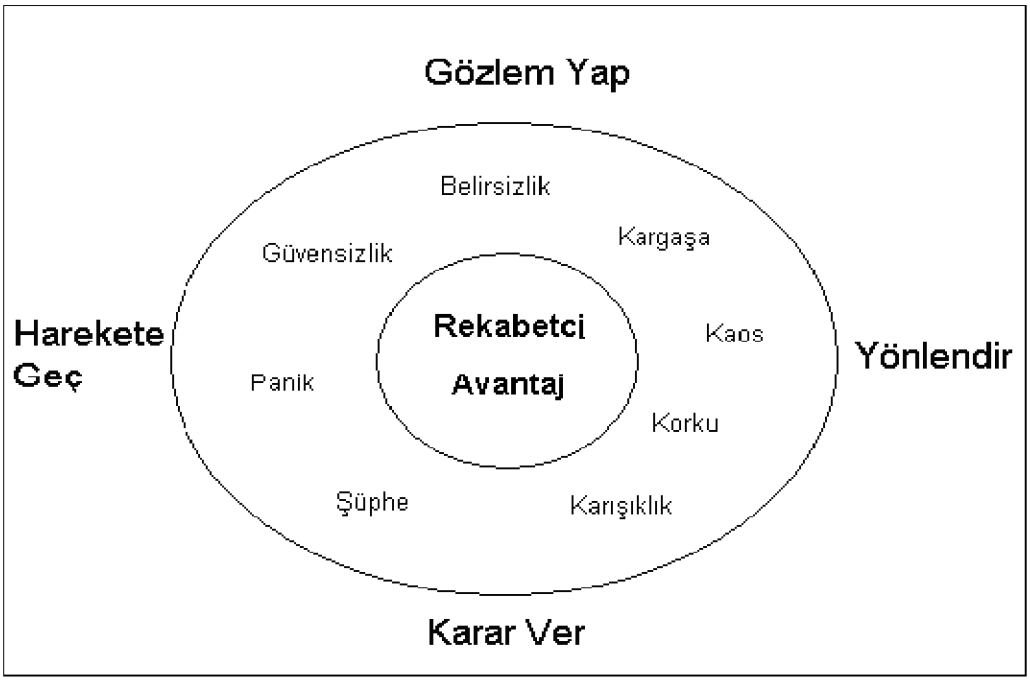
Orta kademe yöneticiler; BT Risk Yöneticileri, BT Denetçileri, Bilgi güvenliği yöneticileri gibi yöneticiler ise, yöntemin tümünü dikkate alarak çalıştıkları alana ait bakış açısı ile Bilgi Teknolojileri İçin Kontrol Hedefleri'ni kullanarak riskleri analiz ve takip ederler. Denetim faaliyetlerini gerçekleştirirler, bilgi güvenliği ile ilgili yönetsel ve operasyonel düzenlemeleri yaparlar. İzleme ve değerlendirmeye yönelik süreçler bütününün "sürekli iyileştirme" bacağına katkıda bulunurlar.

Bilgi Teknolojileri İçin Kontrol Hedefleri; kullanmasını bilen her BT çalışanının elinde bir rehberdir. BT ile ilgili beklentileri olan iş tarafındaki paydaşların, "Teknolojik işler nasıl yürütülüyor?" gibi soru bulutlarının içerisindeki işleyişi görebilmeleri için kullanabilecekleri bir sis dağıtma aracı; BT yöneticileri için "kaptanın seyir defteri ve pusulası"; denetçilerin iyileştirme fırsatları yaratabilmek için karşılaştırma yapmak amaçlı kullanılabilecek bir mihenk taşı özelliklerini taşıyan bir rehberdir. İş ve BT birimleri arasında "Ortak Dil" oluşmasında bir kılavuz görevindedir. Gelişmiş kurumlarda ise "büyük resmin" görülmesinde kullanılabilecek ve kurumsal gelişmeyi izleyebilecek bir yol haritası diyebiliriz. (Üvey, 2009, s:57)

2. BİLGİ GÜVENLİĞİ

Bilgi güvenliğine olan ihtiyacın neden ortaya çıktığını anlamak için zamanında ve doğru bilgi almanın önemini anlamak gereklidir. Bilgi güvenliğinin temel amacı doğru kişinin kısa zamanda doğruluğundan emin olunan bilgiye ulaşımını garanti altına almaktır. Bu ihtiyacı basitçe göz önüne sermek için Albay John R. BOYD' un OODA (Observe-Orient-Decide-Act, Gözle-Yönlendir-Karar Ver-Harekete Geç) döngüsü dediği gösterime bakmak gereklidir. OODA döngüsü ismini ingilizce Observe-Orient-Decide-Act (Gözle-Yönlendir-Karar Ver-Harekete Geç) kelimelerinden alır. (Kovacich, 2003, s:4)

Şekil 2.1: Gözle-Yönlendir-Karar Ver-Harekete Geç Döngüsü



Kaynak: Kovacich, 2003, s:4

Model, idari olarak doğru verilmiş kararların kurumları, aradaki belirsizlikler, kargaşa, kaos, korku, şüphe, panik ve güvensizlik ortamından rekabetçi avantaja götürdüğünü anlatmaktadır. Bu kararları verebilmek için de doğru bilgiye, doğru zamanda, doğru kişilerin ulaşması gerekmektedir.

Kurumların bilgi teknolojisi yatırımlarından hangi sonuçları bekledikleri konusunda yapılan bir araştırma güvenlik gereksinimlerine olan ihtiyacı açıklamaktadır. Tablo 2.1'de verilen çalışma ITGI (Information Technologies Governance Institude – Bilgi Teknolojileri Yönetim Enstitüsü) tarafından 2003 yılında "PriceWaterhouseCoopers" firmasına yaptırılmıştır. Örneklemi dünya çapında yaygın büyük kurumların genel yöneticileri ve bilgi teknolojileri yöneticileridir.

2003 yılında 276 şirket ile yapılmış olan araştırma 2005 yılında 695 şirket örneklemi kullanılarak yeniden gerçekleştirilmiştir.

Tablo 2.1: Şirketlerin BT yatırımlarından beklentileri (konuların önemine 5 üzerinden verilen notlar)

	BEKLENTİLER	2003	2005
1	Kurumun Stratejik Hedeflerine Ulaşması	4,18	4,21
2	İşe Faydalı Sonuçların Çıkması	4,24	4,18
3	İş-Kritik Bilgilerin Sürekli Erişilebilir Olması	4,06	4,17
4	İş Kritik Bilgilerin Güvenilir Olması	3,95	4,16
5	İş Kritik Bilginin Kesin ve Tam Olması	3,93	4,03
6	İş Kritik Bilginin Yasa ve Antlaşmalar ile Uyumlu Olması	3,82	4,00
7	Önemli Verimlilik Artışlarının Olması	4,12	3,91
8	İş Kritik Bilgilerin Gizli Kalması	3,8	3,81

Kaynak: ITGI, 2006

Geleceğe yönelik bilgi teknolojileri iş planlaması ve güvenlik çalışmalarında Tablo 2.1'de verilen veriler, beklentilerin önem derecesini göstermesi açısından önemlidir. Sekize ayrılan beklentilerde güvenlik bakış açısından önemli sayılan beklentilerden olan 3. sıradaki erişilebilirlik, 4. ve 5. sıradaki bütünlük ve nihayet 8. sıradaki gizliliktir. Anketlerin arasından geçen 2 yılda verim artışı beklentileri, yerini diğer öğelere bıraksa da bilişim güvenliği en önemli sıraya gelmemiştir. Bu ankette örneklem kurum/şirket yöneticileri olduğu için beklentiler

sonuç odaklı görülmektedir. Hızlanan piyasa koşullarında hayati önemde olan şirket hedeflerine ulaşmak, diğer öğeleri göreceli olarak önemsiz bırakmıştır. (ITGI, 2006)

2.1. Bilgi Güvenliği Tanımı ve Kavramları

Bilgi güvenliği çerçevesi belirlenirken ve sınıflamalar yapılırken genellikle (ISC)2 kuruluşunun CBK bilgi havuzu denen sektörün en uzman sayılan profesyonellerinin, CISSP (Certified Information Security Systems Professional – Profesyonel Sertifikalı Bilgi Güvenliği Sistemleri) girdi yaptığı en iyi uygulamalar kütüphanesinden oluşan veritabanı kullanılır. Buna göre bilgi güvenliği konularını incelerken üç kavram bakış açısından ele alınır. Bu üç kavrama başka kurumlar iki kavram bakış açısı daha eklemektedirler. Bu beş kavram, CBK dâhilindeki üçü olan gizlilik, bütünlük ve erişilebilirlik ile bu üçü kadar sık dile getirilmeyen diğer iki öğe olan hesap verebilirlik ve yetkilendirmedir. Bütün güvenlik konuları bu kavramlardan yola çıkılarak değerlendirilir, bilgi güvenliğinin tam tanımı bu kavramlar anlatıldıktan sonra ancak yapılabilir.

2.1.1. Gizlilik

Gizlilik Uluslararası Standartlar Örgütü (ISO) tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" olarak nitelenir. Bugün şifreleme altyapılarının olmasının sebebi temel olarak gizlilik ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için farklı önem taşıyabilir. Gizlilik özellikle kamu kurumları ve bankalar gibi kuruluşlar için çok önemlidir.

2.1.2. Bütünlük

Bütünlük (veri bütünlüğü) dar güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır. Verinin bozulması kasten yahut kaza ile olabilir ve bu bütünlüğün bozulmuş olduğu gerçeğini değiştirmez. Güvenlik önlemi alanların iki tür riske karşı da tedbir almaları gerekmektedir. Bilginin bütünlüğü aşağıdaki üç kıstası sağlamalıdır.

1. Kesinlik 2. Doğruluk 3. Geçerlilik

2.1.3. Erişilebilirlik

Erişilebilirlik herhangi bir sistemin yapılış amaçlarına göre işlev gördüğü zamanın, işlev gördüğü ve görmediği toplam zamana oranıdır. Daha yalın bir anlatımla, doğru yetkilendirilmiş bir kişinin ihtiyacı olduğu anda ihtiyacı olan hizmetin orada olma oranına erişilebilirlik denir. Verilen hizmetin ne kadar güvenilir olduğunun bir ölçütüdür. Kurumlar hizmetin ne kadar önemli olduğunun ölçümünü yapıp sistemleri ve verileri bu ihtiyaca göre yedekli hale getirirler.

2.1.4. Hesap Verebilirlik

Hesap verebilirliğin en kısa tanımı, kişilerin yaptıkları hareketlerden ve görevi olduğu halde yapmadıklarından sorumlu olmalarıdır. Hesap verebilirliğin alt kavramları olan sorumluluk, suçlanabilirlik, cevap verebilirlik gibi konular büyük tartışmaların merkez noktaları olduğundan hesap verebilirlik diğer üç kavramın yanında değil, biraz uzağında değerlendirmeye tabi tutulur.

2.1.5. Yetkilendirme

Bilgi güvenliği bakış açısından yetkilendirme kimlik doğrulama sistemidir. Bilgiye erişim sürecinde yetkilendirme, bilgiye doğru kişinin ulaşıp ulaşmadığını kontrol eden alt sistemdir. Gündelik işlerimizde hemen her bilgisayar ağ kaynağına eriştiğimizde yetkilendirme çözümlerini kullanmaktayız. Microsoft Windows işletim sistemine her şifre girildiğinde, şifre alan kontrolcüsünün Kerberos sisteminde kontrol edilip, cevap geriye yollanır. Bu aşamadan sonra kişi her ağ kaynağı kullanmak istediğinde, bağlanılan sistem kişinin kimliğini gene "alan sunucusundan" teyit eder. Yetkilendirme konusunda dikkat edilmesi gereken, bilgi sistemlerinde geçerli olan "en az bilgi" kuralıdır. Bu kural kişilerin işlerini yapmaları için gereken en az bilgiyi bilmeleri gerektiği prensibini kurumlara benimsetmektedir.

2.2. Bilgi Güvenliği Tanımı

Bilgi güvenliği, kurumların bilgi envanterindeki varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini tehdit eden risklerin tanımlanıp, bu konuda risk

yönetimi gereklerinin yapılmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olabilirliğine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir;

Riskin azaltılması,
Riskin kabul edilmesi,
Tamamen üçüncü bir tarafa devredilmesi (sigorta etmek gibi) veya
Risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir.

Risklerin tanımlanması ISO 13335-115 standardında da gösterilmektedir. Bu standardın tanımı itibariyle bilgi güvenliği, bilginin risk yönetimini yapmaktır.(Yıldız, 2007, s:25)

2.3. Bilgi Güvenliği İnceleme Alanları

Bilgi güvenliği kavramları CBK' da tanımlanan 10 alanda incelenir; (Yıldız, 2007,s:28)

1. Bilgi Güvenliği Yönetimi
2. Erişim Kontrol Sistemleri ve Yöntemleri
3. Telekomünikasyon, Bilgisayar Ağları ve internet Güvenliği
4. Uygulama Yazılımı Güvenliği
5. Şifreleme
6. Kurumsal Güvenlik Mimarisi
7. Operasyon Güvenliği
8. İş Sürekliliği Planı
9. Mevzuat, İnceleme ve Değerler
10. Fiziksel Güvenlik

2.3.1. Bilgi Güvenliği Yönetimi

Bilgi güvenliği yönetimi başlığından da anlaşılacağı gibi temel kavramlar üzerinde durur. Yukarıda açıklanan gizlilik, bütünlük ve erişilebilirlik kavramlarını derinlemesine irdeleyen bu başlıkta, konuya güvenliğin kurumda kimin sorumluluğu olduğu ile başlanır. Bilgi güvenliği, bilgi teknolojileri çalışanlarının değil, üst

yönetimin temel işidir ve kurumlarda güvenliğin gereklerinin yerine getirilip getirilmediğini bizzat üst yönetim sorgular. Strateji ve güvenlik gibi kavramlar merkezi ve askeri kökenli kavramlardır. Bu kavramların merkezi ve dayatıcı olmasından başka bir yol yoktur. Güvenlik aşağıdan yukarı uygulanamaz, bilişim çalışanları kurum çalışanlarını güvenlik kurallarına uymaya zorlayamaz, bunu her kurumda üst yönetimin yapması gereklidir.

İlk aşama, kurumun güvenlik önlemleri almak için örgütlenmesidir. Üst yönetimin başkanlık ettiği bir kurul, kurumun uzun vadeli stratejik bilgi teknolojileri ve güvenlik hedeflerini belirlemek ile işe başlar. Kurulda sadece bilgi teknolojileri çalışanları ya da bilgi teknolojilerine yakınlık duyan insanların olması hata olacaktır. Elden geldiğince çok birimden, değişik alışkanlık ve görüşten insanın olması, çalışmaları olumlu yönde etkileyecektir. Çalışmalar sırasında anonim girdilere de ihtiyaç olabilir. Güvenlik çalışmalarına katılım ne kadar yüksek olursa o kadar faydalı olacaktır. Stratejik hedefler belirlendikten sonraki aşama taktik hedeflerin belirlenmesidir. Taktik hedefler ile kurumun sunduğu ürün veya hizmetlerde nasıl bir değişikliğin kurumu stratejik hedeflerine ulaştıracağı ve bunların nasıl güvenlik ihtiyaçları doğuracağı belirlenir.

İkinci aşama ise operasyonel hedeflerin belirlenmesidir. Bu aşamada ise daha detaylı olarak günlük çalışmalarda yukarıdaki hedeflere nasıl ulaşılacağı kararlaştırılır.

Üçüncü aşamada kurum kültürü ve kurum yapısına göre ne gibi güvenlik önlemleri alınması gerektiği tartışılır. Örneğin bir özel şirketin öncelikli güvenlik hedefi yüksek erişilebilirlik iken, kamu kurumlarının hedefi gizliliktir. Bu hedefler belirlenirken kurum kültürünün ön planda tutulması çok önemlidir. Çünkü bu konuda ortaya çıkacak bir aksama veya çalışanların işlerini yapamamalarından dolayı güvenlik kurallarını toplu olarak hiçe saymaları, güvenlik çalışmalarına büyük darbe vuracaktır.

Dördüncü aşamada ise kurumun bilgi varlıklarını ve verileri sınıflaması gerekmektedir. Veriler gizlilik derecelerine, önemlerine, tarihlerine göre çıkarılıp sınıflanırlar.

Beşinci aşama riskleri belirlemektir. Riskleri belirlemeye fiziksel risklerden başlanmalıdır. Kurumun teyp yedekleme disklerinden, bilgisayarlara, sunuculara ve bağlantılarına kadar tüm varlıklarının bir listesi çıkarılıp bunların maruz kalabileceği

tehlikeler ve tehditler belirlenir. Neyin nerede tutulması gerektiği, bakım ve garantilerin hepsi bu çalışmada göz önünde tutulmalıdır.

Altıncı aşamada insanlardan kaynaklanabilecek riskler incelenmelidir. Burada kurumun iş yapma tarzları, çalışanların görev tanımları ve bu tanımlara göre erişim yetkilendirmelerinin belirlenmesi gerekir. Olası bilgi hırsızlıkları ve kuruma yapılabilecek sanal saldırılar bu aşamada değerlendirilir. Burada riskler belirlenirken bu risklere karşı alınacak önlemler de tartışılır. Burada önemli olan sadece alınacak önlemler değildir, bunların birbirlerine göre önem sırasına da karar verilmelidir. Bu aşamada risk yönetimi kavramlarını açıklamak gereklidir. Kurum bilişim varlıklarını tanımladıktan sonra bu varlıklara herhangi bir şekilde zarar verebilecek tehditleri de belirler. Bu tehditlerin varlıklara zarar vermesine yol açabilecek güvenlik açıklarına "zafiyet" denir. Tehditlerin varlıklara zarar verebilmelerinin olasılığı hesaplanarak belli bir tehdidin yılda kaç defa olabileceği ve oluştuğunda verebileceği zarar yüzde olarak ifade edilir. Böylece riskler ve potansiyel tehditler tanımlandıktan sonra bunlara karşı alınabilecek önlemler serisine karar verilir. Bir risk hakkında verilebilecek temel üç karar vardır; risk azaltılabilir, üçüncü bir tarafa devredilebilir ya da kabul edilir. Risk hesaplaması yapılırken her varlığa bir parasal değer atanmaya çalışılır. Böylece risk gerçekleştiğinde verebileceği zarar objektif olarak ortaya konmuş olur. Eğer riske karşı alınabilecek önlemler riskin kendisinden fazla maliyete yol açacak ise risk kabul edilir. Tüm bu çalışmalar yapılırken her aşamanın dokümante edilmesi önemlidir.

Güvenlik çalışmalarının aynen kalite çalışmaları gibi bir sonuç üretmeye çalışmadığı, kalite çalışmaları gibi her asli sürecin altında çalışan bir alt fonksiyon olduğu akılda tutularak, her adım yazılır. Böylece ileride çalışmalar yeniden gözden geçirildiğinde hangi kararın neden verildiği ortaya konabilecektir. Bu çalışmalardan sonra kurum, güvenlik politikası dokümanını ortaya koymalıdır. Güvenlik politikası dokümanı uzun olmayan, temel güvenlik gereksinimlerini ve kurallarını açıklayan, kurallara uyulmaması halinde verilebilecek cezaları da içeren bir kurallar bütünüdür. Bu politika içinde kurumun bağlı olduğu kanuni ve ikili antlaşmalara dayalı kurallar da ortaya konmalıdır. Politikalar içerisinde tavsiye niteliğinde, kurum stratejisine uygun bulunan ya da karşı olan davranışlar da belirtilir. Bu politikalar kurumun en yüksek yöneticileri tarafından onaylanır.(Hansche, 2003, S.3)

2.3.2. Erişim Kontrol Sistemleri ve Yöntemleri

Erişim kontrol sistemleri, isminden de anlaşılabileceği gibi, kimin hangi kaynaklara erişebileceği konusunda yetkilendirileceği ve bu yetkilendirmenin nasıl kontrol edileceği ile ilgilenen güvenlik alanıdır. Bu alanın kapsamına hesap verebilirlik de girer. Her çalışan kaynaklara erişim isteklerinden ve eriştiği kaynakların bütünlüğünden sorumludur. Bunu sağlamak üzere ise mümkün olduğu kadar çok alanda kimin hangi kaynaklara eriştiği kayıt altına alınmalıdır. En az yetki kavramı da gene bu başlık altında incelenir. Kişilere işini yapması gerekenden daha fazla kaynağa erişim vermek güvenlik bakış açısından kabul gören bir yaklaşım değildir. Üç tip erişimden bahsedilebilir.

Birincisi fiziksel erişim kontrolleridir. Çitler, duvarlar ve kapılar gibi engeller, fiziksel erişim kontrolü sayılırlar. Kurum içerisinde personelin dolaşımı da iş tanımı ve yetkisi çerçevesinde kısıtlanmak istenebilir.

İkinci tür erişim kontrolü, yönetim erişimidir. Fiziksel erişim kişileri fiilen engeller ya da izin verirken, yönetici erişimi, kimlerin yönetici haklarıyla hangi kaynakları kullanarak bir nesne üzerinde işlem yaptığının kontrolüdür. Kişilerin sanal olarak hangi kaynaklara ulaştıkları, hangi kaynağı ne amaçla kullandıklarını belirlemek için belirlenen stratejilerin ve yöntemlerin tümüne yönetici erişimi kontrolleri denir. Yetkilendirilmiş kişilerin ne yaptıklarının kontrolü bu başlık altında incelenir.

Üçüncü tür erişim kontrolü, mantıksal erişimdir. Mantıksal erişim kişilerin sanal olarak hangi kaynaklara ulaştıklarının kontrolüdür. Sanal ortamda, kişilerin işlem yaptıklarında nasıl bir iz bırakmaları gerektiği konusunda verilecek kararlar doğrultusunda, kaynakları güvenlik gereksinimleri sınırlarında kullanıp kullanmadıkları bu tip kontroller ile tespit edilir. Eğer gerekiyor ise mantıksal bilişim ağı ayrımlarına da gidilebilmektedir. Erişim kontrolü yukarıda belirtilen üç alanda sınıflanırken, her üç bölümde alınabilecek kontrol çeşitleri açısından kendi içinde beşe ayrılırlar;

1. Önleyici kontroller: Önleyici kontroller basitçe yetkisi olmayan kişinin kaynağı kullanmasına izin vermez.

2. Tespit edici önlemler: Önlemenin mümkün olmadığı durumlarda daha sonra tespit edilebilecek izler bırakılması sağlanır.

3. Caydırıcı önlemler: Önleyici kontrollere benzemekle beraber caydırıcı önlemler erişime izin verebilir, ama bunun karşılığında nasıl bir ceza olabileceği konusunda da kişileri bilgilendirir.

4. Düzeltici önlemler: Bir kaynağa erişilip zarar verildiği durumlarda nasıl düzeltileceğini belirler.

5. Geri döndürücü önlemler: Geri döndürücü önlemler düzeltici önlemlere benzemekle beraber düzeltmek yerine kaynağı belli bir tarihteki durumuna geri getirir.

2.3.3. Telekomünikasyon, Bilgisayar Ağları ve İnternet Güvenliği

Bilgisayar ağlarının nasıl çalıştığı, internet sisteminin nasıl işlev yaptığı anlaşılmadan etkin güvenlik kontrolleri yapmak neredeyse imkânsızdır. Bilgisayarlar birbirleri ile haberleşirken, haberleşme aşamalarının birbirlerinden soyutlanmasını sağlayan OSI (Birbirine Bağlı Açık Sistemler, Open Systems Interconnection) modelinin anlaşılması gerekmektedir. Katmanların birbirinden soyutlanmasının önemi, değişik sistemlerin birbirleri ile çalışabilmelerinin temini amacını gütmektedir.

2.3.4. Uygulama Yazılımı Güvenliği

Günümüz bilişim ortamında pek çok uygulamanın birbirleri ile uyumlu, güvenilir ve güvenlik gereksinimlerini sağlayacak şekilde tasarlanmaları ve çalışmaları beklenmektedir. Uygulamalar hazır satın alınan ya da geliştirilen yazılımlar olabilir. Yazılımların gelecekteki ihtiyaçları, şu anki kullanım amaçları ve birbirleri ile ilişkileri göz önüne alınarak güvenlik önlemleri alınmalıdır. Alınması gereken önlemler ve bu önlemleri gerekli kılan kavramlar aşağıdaki gibidir. Kurumsal ihtiyaçlar bazı yazılımların kurum için özel geliştirilmesini gerektirebilir. Kurumsal kullanımda hangi kullanıcının bilgisayarını hangi iş amaçlarına göre kullandığı tanımlandıktan sonra bilgisayarların yazılım konfigürasyonunun belirlenmesi gerekmektedir. Bu konfigürasyonun dışında yüklü tüm yazılımların potansiyel zararlı uygulamalar olabileceği ihtimali her zaman akılda tutulmalıdır.

Virüsler gibi zararlı kodlarda sistemlerde genellikle bilgisayar yönetici haklarının amaç dışı kullanımından kaynaklanmaktadır. Veritabanı tasarımları ve kullanımı bu alanda incelenmektedir. Kullanıcıların erişim yetkileri belirlenirken düşük yetkideki bir kullanıcının dahi veritabanlarındaki anlamsız değişik bilgilerden çok önemli gizli sınıflanmış sonuçlar çıkarabileceği ihtimali göz önüne alınarak tasarlanmalıdır. Veritabanları her türlü uygulamanın kullanmakta olduğu yazılımlardır. Veritabanı tasarımı güvenlikte önemli bir yer tutmaktadır.

2.3.5. Şifreleme

Şifreleme, bilişim güvenliğinin en önemli alt gereksinimlerinden birini oluşturmaktadır. Şifreleme, uygun anahtarı olmadan kimsenin çözemeyeceği şekilde mesajların dönüştürülmesidir. İletişimde de şifreleme önemli bir rol oynamaktadır. İletişimde şifreleme hem üçüncü bir kişinin mesajı okuyamamasını hem de mesajı gönderen kişinin mesajı gönderdiğini inkâr edememesini sağlamaktadır. Şifreleme sistemlerinde şifrenin gücünü belirleyen en önemli parametre olan anahtar, bir dizi rastgele bir ve sıfırdan oluşmaktadır. İkili sistemde gösterilen bu anahtarın uzunluğu şifrenin gücünü belirler. Bu uzunluklar genelde ikinin üsleridir ve şifreleme algoritmaları ile özdeşleştirilmiştir.

2.3.6. Kurumsal Güvenlik Mimarisi

Güvenlik mimarileri hazırlanırken bazı şablonlara bakmak ve arkalarında taşıdıkları mantığı kavramak önemlidir. Geçmişte güvenlik çalışmaları yapan kuruluşlar bu konuda detaylı dokümanlar ve yönergeler hazırlamışlardır. Burada bu uygulamalardan bazıları üzerinde durulacaktır.

Bunlardan biri "askerden arındırılmış bölge" kelimelerinin ingilizce baş harflerinden oluşan DMZ (De Militarized Zone, Askerden Arındırılmış, tarafsız bölge) kavramıdır. DMZ mantığına göre kurumlar internete bağlanırken, tüm dışarı giden trafik arada ateş duvarları olan ve içerisinde hassas bilgiler bulundurulmayan bir ara bilgisayar ağından geçmelidir. Güvenlik açısından potansiyel tehdit olabilecek tüm trafik bu bölgede tutulur. Örneğin dışarı hizmet veren web sunucuları DMZ' de tutulurlar. Bir diğer tanım ise kaynak gözlemleyicisi yapısıdır. Kaynak gözlemleyicisi erişilen kaynaklar ve erişmek isteyen objeler arasındaki kontrolcüdür.

Ateş duvarları buna bir örnek olabilir, ama kavram ateş duvarlarıyla sınırlı değildir. Kurumlarda e-mailleri virüs taramasından geçiren yazılımlar da kaynak gözlemleyicisi olarak adlandırılabilir. DMZ ve Kaynak Gözlemleyicisi gibi yapılar, kurumlara güvenilir bilgi temeli (TCB - Trusted Computing Base) hazırlamak için kurulurlar. TCB uygulamaların güven içinde çalıştırılabildiği bir altyapı olarak değerlendirilebilir.

2.3.7. İşletme Güvenliği

İşletme güvenliği, güvenliğin işleyiş şekli ile ilgilidir. İşletme seviyesi politikaların nasıl uygulanacağı burada belirlenir. Buradaki ilk nokta yönetimin güvenliğe bakışı olacaktır. Burada iki kavram öne çıkmaktadır; itinalı güvenlik ve güvenlikte sebat. İtinalı olmak her güvenlik olayına ilgi ve detayla eğilmek iken, güvenlikte sebat kavramı politika ve olayların üzerinden tekrar geri dönerek geçmektir. Güvenlikte de diğer kavramlar gibi zaman içinde ihtiyaçlar ve olgular değişebilir ve buna göre politikaların da değişmesi gerekebilir. Yönetimin asıl görevi, kurumun anlaşmalar ve kanuni gereksinimler ile kurumun işleyişi arasında uyumsuzluklar olmamasını sağlamaktır. Güvenlik politikaları bunu temin etmelidir. Burada tekrar bahsedilmesi gereken kavramlar hesap verebilirlik ve görev ayrılığı kavramlarıdır. İşler birbirini tamamlayacak şekilde tanımlanmalıdır. Hiç kimse bir işi baştan sona kadar götürmemeli, her süreç bir aşamasında bir sonraki personele teslim edilmelidir. Yedekler ve kayıt süreleri işletme güvenliğinin bir başka alt konusudur. Her türlü sistem kaydı, ne kadar önemsiz görünür ise görünsün, elden geldiğince uzun bir süre kayıt altında tutulmalıdır. Yedekleme politikaları da kritik bilginin düzenli olarak yedeklendiğini garanti altına almalıdır. Her yedek alındığında yedeklerin sağlıklı olup olmadıklarının kontrol edilmesi gereklidir. Yedekleme medyalarının üzerine yedekleme ile ilgili tarih başta olmak üzere yedek alan kişinin adı dâhil, her türlü detay yazılmalıdır. Bu medyalar yangına karşı etkilenmeyecekleri, yangın ihtimalinde dahi medyaların bozulamayacakları bir sıcaklıkta olacakları ortamlarda tutulmalıdır.

2.3.8. İş Sürekliliği Planı

İş sürekliliği planı, iş süreçlerinden biri yahut birkaçı kesintiye uğradığında işin kendisinin kesintiye uğramamasının teminidir. Bunu sağlamak üzere iş süreçleri

analiz edilir ve kritik işler ortaya konur. İlk bakılması gereken birimler asli görevleri icra eden birimler de olsa, ana destek birimlerinin hangileri olduğunun belirlenmesi de önemlidir.

Hangi hizmetlerin, birimlerin ve süreçlerin her olasılığa karşı çalışmaya devam edeceği kararlaştırıldıktan sonra planlama kurulu kurmak gerekecektir. Bu kurulun üyelerinin asli görevleri icra eden birimlerden, kritik destek birimlerinden, bilgi teknolojileri biriminden, güvenlik biriminden ve hukuk biriminden oluşmaları faydalıdır. Elbette üst yönetimin de bu planlamada mutlaka yer alması gerekmektedir. Üst yönetimin planlamada bizzat yer alması, verilen desteği ortaya koyacaktır. Bu destek, planın çalışıp çalışmadığı gerçek tatbikat yapılarak test edildiği (tüm hizmetlerin durdurulmak zorunda kaldığı) gibi zamanlarda gerekecektir. Ayrıca planlama kurulunun planlamayı yapabilmek için paraya ihtiyacı olacaktır. Tüm yedeklilik ihtiyaçlarını tedarik etmek oldukça yüksek maliyetlere çıkabilecektir. Üst yönetimin bu aşamada işin içerisinde olması, bu para ve bütçe ihtiyaçlarının belirlenip kaynak ayrılmasında da yardımcı olacaktır.

Planlama kurulunun karar vereceği en önemli nokta iş etki analizidir. İş etki analizi iş süreçlerinde olabilecek kesintilerin hangi diğer süreçleri ne kadar etkileyeceğini analiz eder. Bu yolla kritik iş fonksiyonlarını, darboğazları keşfetmeye çalışır. Bu yapılırken elden geldiğince nicel davranmak gereklidir. Analizler iş kesintisinin yol açacağı para kayıpları, itibar kayıpları ve kanuni yükümlülüklerden doğacak zararları nicel olarak hesaba katmalıdır.

İş süreçlerinin birbirlerine etkileri çıkarıldıktan sonraki aşama, devamlılık planlarının yapılmasıdır. Devamlılık planlarında ilk korunması gereken, tesis ve insanlardır. İnsanları korumak ilk hassasiyet olursa ve bu öncelik tüm çalışanlara belirtilirse, çalışanların iş süreklilik planına katkıları çok daha içten ve katılımcı olacaktır. Tesisin kendisinin korunmasından sonra tesis altyapısının da korunması ve alternatif planların yapılması gerekmektedir. Diğer planlamalar ancak insanlar, tesis ve altyapı çalışır durumda ise çalışabilecektir.

İş etki analizi ve devamlılık planlarının bir araya getirilmesi ile iş süreklilik planı ortaya çıkmış olacaktır. Bir sonraki aşama bu planın bütçeleme dâhil aşamaları belirtir halde yazılı bir hale getirilmesi ve üst yönetim tarafından onaylanmasıdır. Daha sonra ise katılımcıların eğitiminden başlayarak planın hayata geçirilmesi gerekmektedir.

İş süreklilik planı ne kadar iyi olursa olsun, kurumlar iş süreklilik planının öngörmediği ölçüde geniş çaplı iş kesintilerine uğrayabilirler. Bu çaplı kesintilere yol açan her türlü etki ancak felaket olarak adlandırılabilir ve bu tip geniş çaplı kurtarma harekâtına da felaket kurtarma planı adı verilir. İş süreklilik planının yetersiz kaldığı durumlarda felaket kurtarma planı devreye girer. Felaket kurtarma planı ve iş süreklilik planını kesin olarak birbirinden ayırmak imkânsızdır. Pek çok kurum da ikisini birbirinden ayırmaz ve beraber uygularlar. Ancak ikisinin farkını vurgulamak, iki sürece kaynak olan ihtiyaçları anlamayı kolaylaştıracaktır. Felaket olarak adlandırılabilecek olaylar ve riskler önceden kestirilemez olabilir. Felaket kurtarma da önemli olan kriz durumlarında elden geldiğince az karar verilmesi, sadece planın uygulanmasının sağlanmasıdır. Felaket planı, kurumun felaketten önce normal bir anına geri dönmesini hedefler.

Felaket kurtarma planında belirlenmesi gereken noktalardan en önemlisi kurumun ne kadar süre içerisinde normal ya da normale yakın bir durumda işe geri dönmesi gerektiğinin planlanmasıdır. Ne kadar sürede işe dönülmesi kadar önemli bir nokta da kurumun ne kadar bir kesintiye tahammül edebileceğidir. Felaket kurtarmada önemli noktalardan biri kurumun verilerinin kurtarılmasıdır. Verilerin her zaman kurum dışında bir noktada yedekli olması faydalı olacaktır. Verilerin kurtarılması ve yedeklenmesi felaket durumlarına göre planlanmalıdır. Altyapının da yedeklenmesi düşünülebilir. Kurumun ne kadar kesintiye tahammül edebileceği değişkeninden hareketle tüm altyapının yedeklenmesi dahi düşünülebilir.

Tüm bu planların yapılması yeterli olmayacaktır. Bu planların zaman zaman test edilmesi, adım adım üzerinden geçilmesi, yönetimin onayı ile bilinçli kesintiler yapılıp planların çalışıp çalışmadığının test edilmesi gerekmektedir.

2.3.9. Mevzuat

Güvenlik için en önemli kriterlerden birisi de mevzuattır. Çok ciddi hazırlanması gereken mevzuat güvenlik kriterlerine, standartlara ve uluslar arası mevzuata uygun olmalı, güvenliği sağlamanın yanında kişisel mahremiyete de özen göstermelidir.

2.3.10. Fiziksel Güvenlik

Fiziksel güvenlik, bilişim güvenliğinin kapsamının sınırında olmasına rağmen önlemlerin fiziksel ortamdaki gerçekleri göz ardı ederek alınması gerçekçi bir güvenlik yaklaşımı olmayacaktır. Güvenlik esas olarak toplumsal bir olgudur ve insanlar fiziksel bir ortamda yaşarlar. Bu gerçek değişmeden kalacağı için fiziksel güvenlik her türlü güvenlik önleminin ayrılmaz bir parçası olmalıdır. Fiziksel tehditleri ana başlıklar halinde örneklendirilir.

1. İletişim kesintisi
2. Su
3. Yangın ve duman
4. Patlamalar
5. Yer hareketleri
6. Binanın yıkılma ihtimali
7. Fırtınalar
8. Kesintiler
9. Sabotaj veya kurum mülkünün bilinçli olarak tahrip edilmesi
10. Malzeme kaybı
11. Personel kaybı

3. GÜNCEL TEHDİTLER VE BULGULAR

Günümüzde kurum ve kuruluşlar bilgilerini elektronik ortamlara açtıkça, elektronik ortamlarda yapılan iş ve işlemler artmakta karşılaşılan güncel tehdit ve tehlikelerde de doğal olarak artışlar gözlenmektedir. Zafiyet ve zayıflık açısından değerlendirildiğinde korunmasızlık seviyesinin yüksek olması nedeniyle güncel gelişmelerin en fazla yaşandığı alan web uygulamalarıdır. Günümüzde web uygulamaları, güncel bilgiye kurum, kuruluş veya bireylerin kolayca erişebilmesi için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır. Web üzerinden verilen hizmetler çoğaldıkça web' e yönelik saldırılar da her geçen gün artmaktadır. Bunun nedeni, web uygulamaları güvenliğinin ilgisizlikten ve bilgisizlikten kaynaklanan sebeplerden ötürü yeterince ciddiye alınmaması ve güvenli yazılım

geliştirme tekniklerinin kullanılmaması olarak açıklanabilir.(Vural ve Sağıroğlu, 2008,s:517)

3.1. Kimlik Doğrulama

Web uygulamalarında kimlik doğrulama mekanizmasını atlatmak veya istismar etmek için kullanılabilecek tehditlerdir. Kimlik doğrulamasında "sahip olunan bir nesne", "bilinen bir bilgi" veya "sahip olunan bir özellik" kullanılmaktadır. Kimlik doğrulama saldırıları, web sitesinin kullanıcı, servis veya uygulama kimliğini doğrulayan sistemleri hedef alan tehditleri kapsar. Web sitelerinin, kimlik doğrulama mekanizmasını atlatmak veya istismar etmede kullanılan saldırı teknikleri, yetersiz kimlik doğrulamaları ve şifre kurtarma denetimlerinin zayıflığının istismar edilmesi olarak sıralanabilir.

3.2. Yetkilendirme Zafiyeti

Yetkilendirme zafiyetleri, bir web sitesinin kullanıcı, servis veya uygulamanın istenen bir işlemi gerçekleştirmesi için gereken izinleri belirlemek için kullanılan yöntemlerin istismar edilmesini hedef alan saldırılardan etkilenmektedir. Yetkilendirme tehditlerini, oturum bilgisi tahmin etme, yetersiz yetkilendirme, yetersiz oturum sonlandırma, oturum sabitleme olmak üzere farklı gruplarda sınıflandırmak mümkündür.

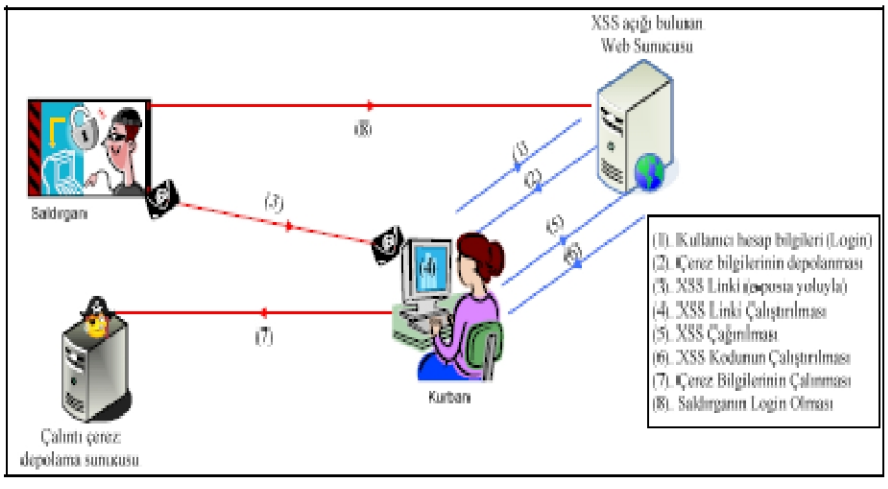
3.3. Siteler Arası Kod Yazma

Siteler arası kod yazma yöntemiyle yapılan saldırılar, kullanıcı ile web sitesi arasındaki güven ilişkisi istismar edilerek, web sitesinin saldırgan tarafından belirlenen çalıştırılabilir kodu kullanıcıya göndermesi ve bu kodun kullanıcı web tarayıcısında yüklenerek çalışmasıyla gerçekleşmektedir. XSS yöntemiyle yazılan küçük kodlar, HTML kodları arasına enjekte edildiğinden bazı kaynaklarda bu yöntemin adı HTML kod enjeksiyonu olarak adlandırılmaktadır. XSS kodları genellikle HTML / JavaScript dilinde yazılmaktadır ancak VBScript, ActiveX, Java,

Flash veya web tarayıcılar tarafından desteklenen diğer dillerde de kodlama yapılabilmektedir.

XSS yöntemiyle zararlı kodun kullanıcı web tarayıcısında çalıştığında, zararlı kod sunucu web sitesinin tarayıcı için tanımlı olduğu güvenlik ayarları kapsamında çalışacaktır. Eğer web tarayıcısı üzerinde herhangi bir kısıtlamaya gidilmemişse zararlı kod vasıtasıyla tarayıcı tarafından erişilen her türlü hassas veri okunabilir, değiştirilebilir ve e-posta aracılığıyla farklı yerlere iletilebilir. XSS yöntemiyle kullanıcı bilgisayarı üzerindeki oturum çerezleri çalınabilir, kullanıcının web tarayıcısı başka bir adrese yönlendirilebilir, web siteleri üzerinde bilgi toplama amaçlı kodlar çalıştırılabilir, sazan avlama yöntemine davetiye çıkartılır, web sayfalarının değiştirilmesi veya hizmet aksattırma saldırılarının yapılmasını sağlamaktadır. XSS saldırı yöntemi şematik gösterimi Şekil 3.1' de verilmiştir.

Şekil 3.1: XSS yönteminin mantıksal gösterimi



Kaynak: Vural ve Sağıroğlu,2008,s:518

Şekil 3.1'de görüldüğü gibi XSS yönteminde (1) nolu adımda kullanıcının şifre ve parolasını kullanarak web uygulamasına giriş yapması sonucunda;

(1). Kullanıcıya ait hesap bilgileri çerez formatında kullanıcı bilgisayarında saklanmak üzere XSS açığı bulunan uygulama sunucu bilgisayarından kullanıcı bilgisayarına gönderilmektedir.

(2). Saldırgan XSS zafiyetini kullanan URL' yi sazan e-posta aracılığıyla kurbana gönderir.

(3). XSS açığı bulunan web sunucusuna gitmesini sağlayacak bağlantıya tıklamasını sağlar.

(4). XSS açığının bulunduğu sayfa çağrılır.

(5). XSS saldırısı yapılmasını sağlayacak kod çalıştırılır.

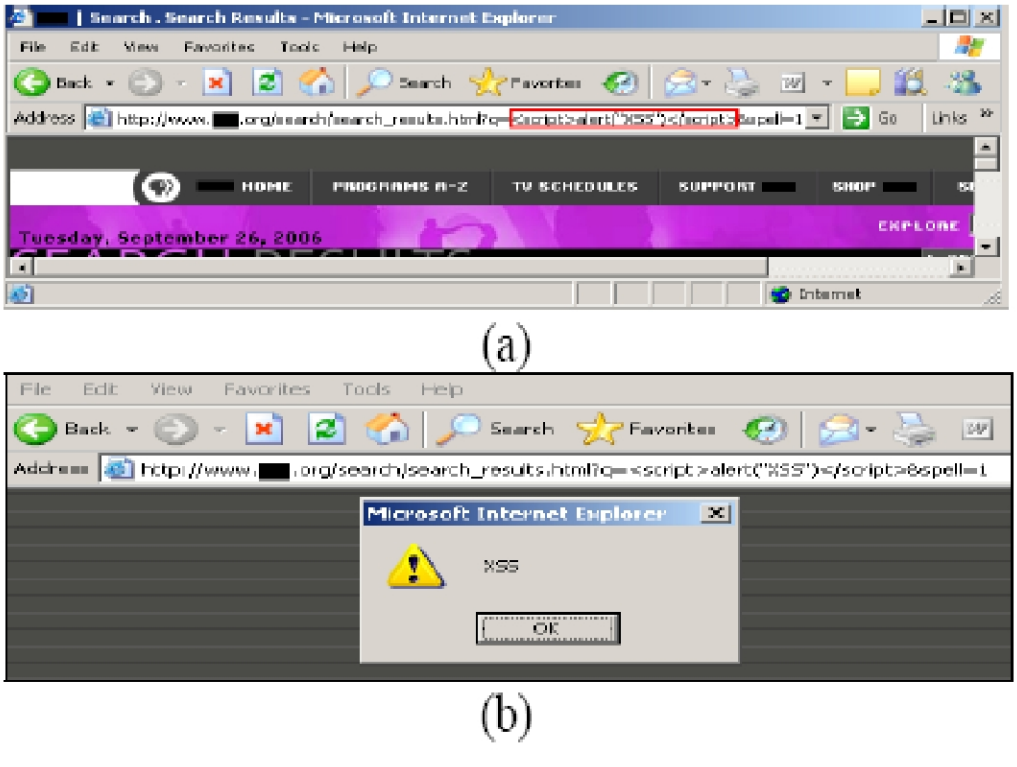
(6). XSS kodunun çalıştırılmasıyla kullanıcı bilgisayarında daha önceden depolanan çerez bilgileri çalınarak saldırganın denetiminde olan sunucu bilgisayarına depolanır.

(7). Çalıntı çerez depolama sunucusundaki kullanıcı erişim bilgilerinin yer aldığı çerez saldırgan tarafından kullanılarak web uygulamasına kurbanın kullanıcı haklarıyla erişir.

(8). XSS yöntemleri kalıcı, geçici ve temelli olmak üzere üç farklı kategoride sınıflandırılmaktadır.

Kalıcı olmayan XSS yöntemi, kullanıcının zararlı kod içeren özel olarak değiştirilmiş linkleri ziyaret etmesini gerektirir. Link ziyaret edildiğinde, URL içine gömülü zararlı kod, istemci tarafına gönderilir ve kod kullanıcının web tarayıcısında çalışır. Kalıcı olmayan XSS yöntemiyle ilgili örnek Şekil 3.2'de gösterilmiştir.

Şekil 2.2: Kalıcı olmayan XSS kodu işlemleri



Kaynak: Vural ve Sağıroğlu,2008,s:518

a) Kodlama, (b)İcra ettirme Şekil 3.2 (a)'da XSS açığı bulunan bir web sitesinde arama yapılmasını sağlayan HTML kodları arasına yerleştirilen XSS kodu web tarayıcısının adres kısmında kırmızı dikdörtgen içerisinde gösterilmektedir. Bu şekilde hazırlanan linkin kullanıcılar tarafından ziyaret edilmesi sağlandığında XSS yöntemiyle sızma testi Şekil 3.2 (b)'de gösterildiği gibi başarıyla gerçekleştirilmiş olacaktır.

Kalıcı XSS saldırısı, mesaj panoları, ziyaretçi defterleri, tartışma forumları, web posta mesajları gibi kullanıcı tarafından web sitelerine girdi yapılabilecek hedefler seçilerek zararlı kodların sunucu tarafında XML dosyaları veya veri tabanlarında depolanmasıyla sağlanır. Bu sızma yönteminde kullanıcının herhangi bir linke tıklamasına gerek yoktur, sadece zararlı kodu içeren web sayfasının tarayıcıda çalışması yeterlidir. Kalıcı XSS yöntemiyle zararlı kod hedef web sitesine sızdırıldıktan sonra; hedef web sitesini ziyaret eden geniş bir kullanıcı kitlesi bu durumdan etkilenmektedir.

Temelli XSS yönteminde, dinamik web sayfaları üzerinde çalışan diğer XSS yöntemlerinden farklı olarak sunucu tarafına zararlı kod gönderilmesine ihtiyaç duyulmayan, kullanıcı tarafında çalıştırılan kod parçalarını içerir. Bu yöntemle yapılan saldırılarda kullanıcının web tarayıcısında etkili olacak nesneler kullanılmaktadır.

3.4. Komut Çalıştırma

Komut çalıştırma yöntemi, web uygulamalarında uzaktan çalıştırılan komutlar yardımıyla yapılan saldırılardır. Web uygulamaları HTTP üzerinden gelen istekler (kullanıcı girdileri) doğrultusunda nasıl davranacağına karar vermektedir. Çoğu zaman bu kullanıcı girdileri dinamik web sitesi içeriğinin hazırlanılmasında kullanılan komutların çalıştırılmasını sağlarlar. Eğer dinamik web sitelerinin içeriğinin hazırlanmasında kullanılan bu komutların kodlanmasında güvenlik ölçütleri göz önüne alınmaz ve girdi doğruluğu sınanmazsa, çalıştırılan komutların saldırganlar tarafından manipüle edilmesi sonucu web siteleri üzerinde güvenlik ihlalleri oluşur.

3.5. SQL Enjeksiyonu

SQL veritabanları, sorgu yapmak üzerine özelleşmiş olan yapısal bir programlama dilidir. Değişen büyüklükteki ilişkisel veritabanı uygulamalarına SQL sorguları aracılığıyla ulaşılabilir. SQL'i destekleyen birçok veritabanı ürünü (Oracle, MS SQL Server, MS Access, DB2, Sybase, vb) standart dile özel eklentiler getirir. Web uygulamaları kullanıcı kaynaklı girdileri, dinamik web sayfası talepleri için, değişik SQL cümleleri oluşturmada kullanabilir. SQL enjeksiyonu yöntemi, kullanıcı girdilerine göre SQL cümleleri oluşturan web sitelerinde, kullanıcı kaynaklı girdilerin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin manipüle edilmesini sağlayan sızma testleridir.

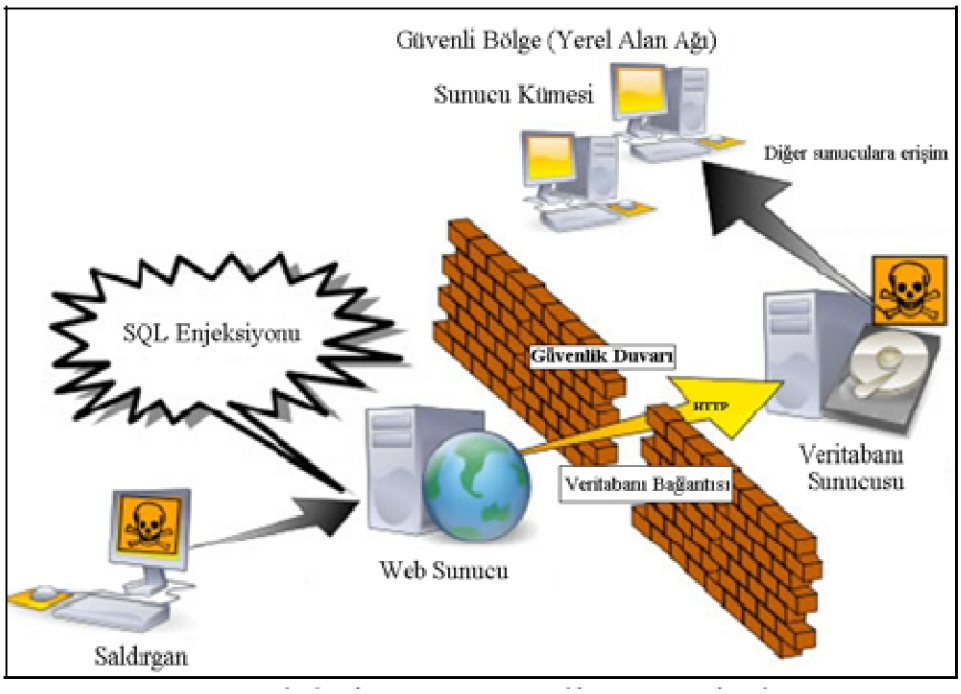
SQL enjeksiyonu sızma yöntemiyle yapılabilecek işlemler aşağıda sıralanmıştır.

- Veri tabanları üzerinde istenmeyen işlemler (sorgulama, ekleme, silme, değiştirme, vb.) yapılabilir.
- Kimlik doğrulama mekanizmaları atlatılabilir.
- İşletim sistemi seviyesinde komutlar çalıştırılabilir.
- Etki alanında yeni kullanıcılar veya gruplar oluşturulabilir.

Eğer bir web uygulaması, kullanıcı kaynaklı girdiyi etkin bir biçimde denetlemezse, SQL enjeksiyon yöntemiyle arka taraftaki SQL cümlesi oluşumu değiştirilerek güvenlik ihlalleri oluşturulabilir. SQL enjeksiyon yöntemiyle SQL cümlesi değiştirilerek bilgisayar sistemlerine sızılması durumunda, SQL servisini çalıştıran kullanıcı haklarına sahip olunacaktır. Veritabanı üzerinde bu haklara sahip olan kişi ileri derece sızma teknikleri kullanarak veritabanı dışındaki diğer sunucu bilgisayarları üzerinde de erişim hakkı kazanabilir. Şekil 3.3'de şematik olarak gösterildiği gibi saldırgan hedef web sitesi üzerinde SQL enjeksiyonu yapabileceği dinamik içerikli web sayfalarını tespit ettikten sonra, SQL enjeksiyonu aracılığıyla veritabanı sunucu bilgisayarına veritabanını çalıştıran servisin (muhtemelen üst

seviyede erişim hakları bulunan yönetici hesapları) kullanıcı hesabıyla ulaşabilir. Veritabanı sunucu bilgisayarı üzerinde, SQL enjeksiyonu yardımıyla işletim sistemi seviyesinde komutlar çalıştıran saldırganın bir sonraki hedefi diğer bilgisayarlar ve özellikle sunucular olacaktır. Saldırgan, diğer sunucu bilgisayarlarına veritabanı kullanıcı hesabıyla bağlantı yaptıktan sonra tüm sunucu bilgisayarlara daha sonra doğrudan bağlanabilmesi (uzak masaüstü, telnet, http, ftp, vb.) için gerekli olan servisleri kendi kullanımına açabilecek ve saldırıdan beklediği sonuçları elde edebilecektir.

Şekil 3.3: SQL Enjeksiyonu şematik gösterimi



Kaynak: Vural ve Sağıroğlu, 2008, s:519

Güncel tehditler incelendiğinde bilgi güvenliği alanında yaşanan güvenlik ihlallerinin, ağ ve sistemlerden web uygulamalarına doğru hızlı bir şekilde kaydığı görülmektedir. Ülkemizde de en fazla güvenlik açıklarına web uygulamalarında rastlanmaktadır. Kurumların genelde sınır ağ güvenliğinin sağlanmasıyla ilgili çözümleri (güvenlik duvarı, saldırı tespit sistemleri, antivirus programları, vb.) ve farkındalıkları olduğu saptanmıştır. Ancak web uygulama güvenliği kavramının dünyada olduğu gibi ülkemizde de uygulamayı geliştiren yazılımcılarında dâhil

olduğu büyük bir çoğunluk tarafından anlaşılamadığı, bilinmediği veya bilinse dahi uygulanamadığı da görülmektedir.

Kurumsal bilgi güvenliğinin sağlanmasıyla ilgili olarak bu çalışmada güvenliğin bir ürün veya hizmet olmadığı, İnsan, Teknoloji ve Eğitim üçgeninde güvenlik standartlarına bağlı olarak yaşayan canlı bir süreç olduğu ve bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı da saptanmıştır.

4. BİLGİ GÜVENLİĞİ STANDARTLARI

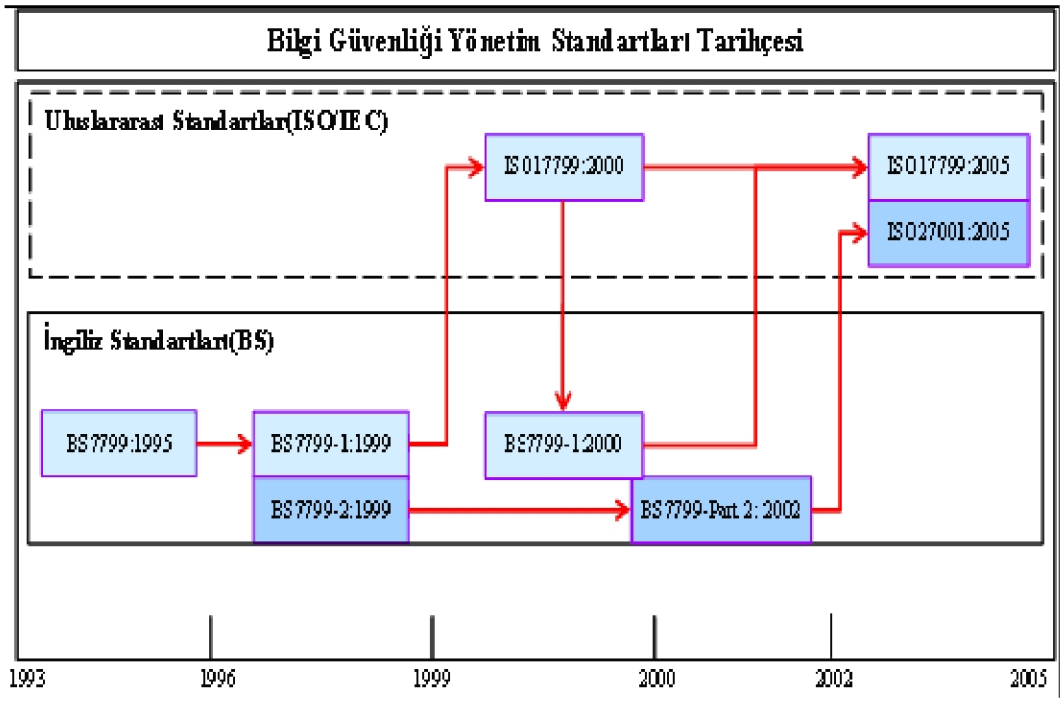
Tehditlerin sürekli olarak yenilenmesi, kullanılan yazılım veya donanımlarda meydana gelen güvenlik açıklarının takibi, insan faktörünün kontrolü gibi süreçlerin takip edilebilmesi ve üst seviyede bilgi güvenliğinin sağlanması için bilgi güvenliği sürecinin yönetilmesi için yapılan çalışmalar sonucunda İngiliz Standartlar Enstitüsü (British Standards Institute-BSI) tarafından 1995 yılında BS–7799 standardının ilk kısmı olan BS7799–1, 1999 yılında ise aynı standardın ikinci kısmı olan BS7799–2 İngiliz standardı olarak yayınlanmıştır.

BS7799–1 2000 yılında küçük düzeltme ve adaptasyonlardan geçerek ISO tarafından ISO/IEC– 17799 adıyla kabul edilmiş ve dünya genelinde kabul edilen bir standart halini almıştır. 2002 yılında ise BSI tarafından BS–7799 standardının ikinci kısmı olan BS–7799–2 standardı üzerinde eklemeler ve düzeltmeler yapılarak ikinci defa İngiliz standardı olarak yayınlanmıştır.

2005 yılında ise ISO tarafından ISO/IEC–17799 standardı üzerinde eklemeler ve düzeltmeler yapılmış ISO/IEC–17799:2005 adıyla yeniden yayınlanmıştır. Son olarak 2005 yılında ISO İngiliz standardı olan BS7799–2 üzerinde eklemeler ve düzeltmeler yaparak ISO/IEC:27001 standardını yayınlamıştır. Bilgi güvenliği yönetim sistemlerinin temelini teşkil eden standartların yayınlanma süreleri Şekil 4.1'de tarihsel akışa göre verilmiştir.

Şekil 4.2'de verilen ve kurumsal bilgi güvenliğinin üst düzeyde sağlanması için gerekli olan bilgi güvenliği yönetiminde kullanılan uluslararası standartlar takip eden alt bölümde sırasıyla açıklanmıştır.

Şekil 4.1: Standartların yayınlanma süreleri



Kaynak: Vural ve Sağıroğlu, 2008, s:511

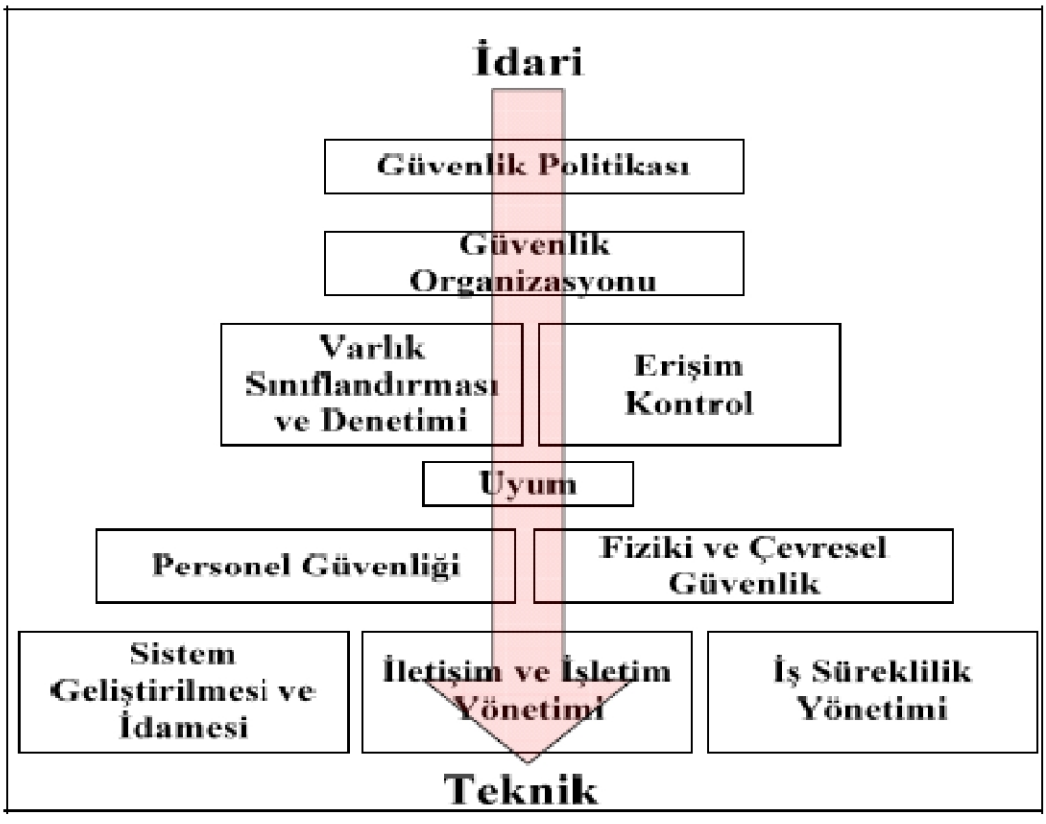
BS–7799, bilgi varlıklarının gizlilik, doğruluk ve erişilebilirliğini güvence altına almak için uygulanması gereken güvenlik denetimlerini düzenleyen ve belgelendiren iki aşamalı İngiliz standardıdır. 1999 yılında yayınlanan ilk sürümün birinci bölümünde bilişim güvenliği için çalışma kuralları anlatılmakta olup, 10 bölüm içerisinde 36 kontrol 127 alt kontrol maddesi bulundurmaktadır. İkinci bölümde bilgi güvenliği yönetim sistemini planlamak, kurmak ve devam ettirmek için gerekli olan süreçler adım adım tanımlamakta ve bilgi güvenliği yönetim sistemine ait belgelendirme (sertifikasyon) bu kısımda yapılmaktadır.

BS–7799 kurumların sadece kendi bilgi güvenlik prosedürlerini değil birlikte çalıştıkları iş ortaklarıyla ilgili sözleşmelerinde bilgi güvenliği yönünden analiz edilmesine yardımcı olmaktadır. BS–7799 standardı endüstri, devlet ve ticari kuruluşlardan ortak bir güvenlik modeli oluşturulmasına gelen talepler sonucu BSI kuruluşu ve BOC, BT, Marks Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever ve diğer bazı şirketlerin katılımıyla hazırlanmış bir standarttır. Standardın tarihsel oluşumuna bakıldığında 1993 yılında kural rehberi, 1995 yılında İngiliz standardı, 1998 yılında sertifikasyon tarifi yapılmış, 1999 yılında büyük bir

düzeltmeden geçerek birinci kısmı, 2002 yılında ise ikinci kısmı yayınlanmıştır. (Osborne, 2006, s:90)

BS–7799 standardı teknik ve idari bölümlerden oluşmaktadır. Standardın birinci kısmının ilk sürümünde yer alan etki alanlarının idari ve teknik kısımlara göre sınıflandırılması Şekil 4.2'de gösterilmiştir. Etki alanları aşağıda maddeler halinde özetlenmiştir.(British Standards Institute, 2005, s:4)

Şekil 4.2: BS–7799 (Sürüm–1) bölümleri



Kaynak: British Standards Institute, 2005, s:4

Güvenlik politikası: Bilgi güvenliği için yönetimin yönlendirilmesi ve desteğinin sağlanmasının yer aldığı bölümdür.

Güvenlik organizasyonu: İşletme içindeki bilgi güvenliğinin yönetilmesi, üçüncü taraflarca erişilen işletmeye ait bilgi işleme araçlarının ve bilgi varlıklarının güvenliğinin korunması ve bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından sağlandığında bilgi güvenliğinin sürdürülmesidir.

Varlık sınıflandırması ve denetimi: İşletmeye ait varlıklar için uygun korunmanın sağlanması ve bilgi kaynaklarının uygun koruma seviyesine sahip olduklarının garanti edilmesidir.

Erişim kontrol: Bilgiye erişimin denetlenmesi, bilgi sistemlerine yetkisiz erişimin engellenmesi, yetkisiz kullanıcı erişimine izin verilmemesi, hizmetlerin korunması, yetkisiz işlemlerin tespit edilmesi ve uzaktan çalışma ortamlarında bilgi güvenliğinin sağlanmasıdır.

Uyum: Herhangi bir suçtan kaçınılması, organizasyonun güvenlik politikalarının ve standartlarının sisteme uyumunun sağlanması, sistem izleme işlemlerinin etkisinin artırılması ve karşılaşılan engellerin azaltılmasıdır.

Personel güvenliği: İnsan hatalarını, hırsızlığı, sahtekârlığı ve araçların yanlış kullanılması risklerinin azaltılması, kullanıcıların bilgi güvenliği tehditlerinden ve sorunlarından haberdar olduklarının ve normal çalışma seyirleri içinde organizasyonla ilgili güvenlik politikasını desteklemek üzere donatıldıklarının garanti edilmesidir. Ayrıca güvenlik ihlallerinden meydana gelen hasarın en aza indirilmesi ve bu gibi olaylardan gerekli tecrübelerin edinilmesidir.

Fiziki ve çevresel güvenlik: İşyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

Sistem bakım ve idamesi: Bilişim sistemleri içerisinde güvenliğin temin edilmesi, uygulama sistemlerindeki kullanıcı verilerinin kaybedilmesini, değişmesini ya da hatalı kullanımının önlenmesi, bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması, IT projelerinin ve destek etkinliklerinin güvenli bir şekilde yürütülmesini temin etmek ve uygulama yazılımının ve bilgilerin güvenliğini sağlamaktır.

İletişim ve işletim yönetimi: Bilgi işlem tesislerinin doğru ve güvenle işletildiğinden emin olunması, sistem arızalarını en az seviyeye indirilmesi, bilgi ve yazılım bütünlüğünün korunması, bilgi işlem ve iletişim hizmetlerinin kullanılabilirliği ve bütünlüğünün sürdürülmesi, ağlarda yer alan bilgilerin

emniyetinin ve destekleyen altyapı sisteminin korunması, iş faaliyetlerinin kesintiye uğratılması ve varlıklara zarar verilmesinin önlenmesi ve organizasyonlar arasında akan bilginin yanlış amaçlarla kullanılması, değiştirilmesi ve kaybedilmesinin önlenmesidir.

İş süreklilik yönetimi: Ticari süreçlerde karşılaşılan olumsuzlukların giderilmesi ve kritik ticari işlemlerin devamlılığının sağlanmasıdır. Kurumlar bilgi varlıklarını tespit edip sınıflandırdıktan sonra, bilgi varlıklarına yönelik tehditleri ve zafiyetleri değerlendirerek yukarıda anlatılan kontrollerden hangilerinin uygulanıp, hangilerinin uygulanamayacağına karar vererek standardın kapsamını kendi kurumlarına özgü bir şekilde belirleyebilmektedirler. BS–7799 ikinci kısmında kurumsal güvenlik ihtiyaçlarının belirlenmesi için gerekli olan bilgi güvenliği yönetiminin çatısı tanımlanarak BS–7799 birinci kısmında tanımlanan kontroller uygulanmaktadır. Bu standart, yöneticilere ve personele etkin bir BGYS kurmaları ve yönetmeleri açısından bir model sağlamak üzere hazırlanmıştır. Bu modelde "Planla– Uygula– Kontrol Et–Önlem Al (PUKÖ)" adımları bulunmaktadır.

Bilgi güvenliği yönetim sistemleriyle ilgili diğer bir İngiliz standardı Aralık 2005'te BS7799–3,2005 Bilgi Güvenliği Yönetim Sistemleri Risk Yönetiminin Kuralları ismiyle hazırlanmıştır. Standart 2006 yılında tekrar gözden geçirilmiş ve BS7799–3,2006 ismiyle yayınlanmıştır. BS7799–3 standardı BS7799–2 standardının uygulanması için destek sağlayarak ölçeklenebilir (küçük, orta veya büyük kurumlar) yapıda standardın yaygınlaşmasına yardımcı olması için geliştirilmiştir. Standard içerisinde risk değerlendirmesi, belirlenen risklere kontrollerin uygulanması, tanımlanmış risklerin izlenmesi, kontrol yönetim sistemlerinin bakımı gibi risk yönetimi ile ilgili konular üzerine odaklanılmıştır. Kapsamın belirlenmesi, kural oluşturan kaynaklar, terimlerin tanımı, kurum bağlamında risk, risk değerlendirmesi, risk kararının verilmesi, risk yönetimi BS7799–3 standardının bölümlerini oluşturmaktadır.

4.1. ISO/IEC Standartları

Uluslararası Elektroteknik Komisyonunu (The International Electro Technical Organization-IEC) 1906 yılında Uluslararası Standartlar Organizasyonu

(International Organization for Standardization-ISO) 1947 yılında uluslararası alanda ticari (ISO) ve elektroteknik (IEC) standardizasyonun sağlanması için, İsviçre'nin Cenova şehrinde kurulmuştur. ISO ve IEC birlikte teknik çalışma grupları oluşturarak (Joint Technical Committee-JTC) tüm dünyada geçerli olacak standartlar oluşturmaktadırlar. Bununla birlikte ISO tarafından IT Güvenlik Standartları ile ilgili çalışmalar JTC–1 Bilişim Teknolojileri Komitesine bağlı SC27: BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bilgi güvenliği konusunda çalışan bu komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir.

Bu sorumluluklar;

- Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması,
- Güvenlik teknikleri ve mekanizmalarının geliştirilmesi,
- Güvenlik kılavuzlarının geliştirilmesi ve
- Yönetim destek dokümanları ile standartların geliştirilmesidir.

Yukarıda açıklanan görevleri yerine getirmek üzere bu komisyon içinde 5 ayrı çalışma grubu bulunmaktadır. Bu gruplar aşağıda belirtilmiştir.

- Çalışma Grubu–1 (JTC 1/SC 27/WG 1): Bilgi güvenliği yönetim sistemleri
- Çalışma Grubu–2 (JTC 1/SC 27/WG 2): Şifreleme ve güvenlik mekanizmaları
- Çalışma Grubu–3 (JTC 1/SC 27/WG 3): Güvenlik değerlendirme kriterleri
- Çalışma Grubu–4 (JTC 1/SC 27/WG 4): Güvenlik denetimleri ve hizmetleri
- Çalışma Grubu–5 (JTC 1/SC 27/WG 5): Kimlik yönetimi ve mahremiyet

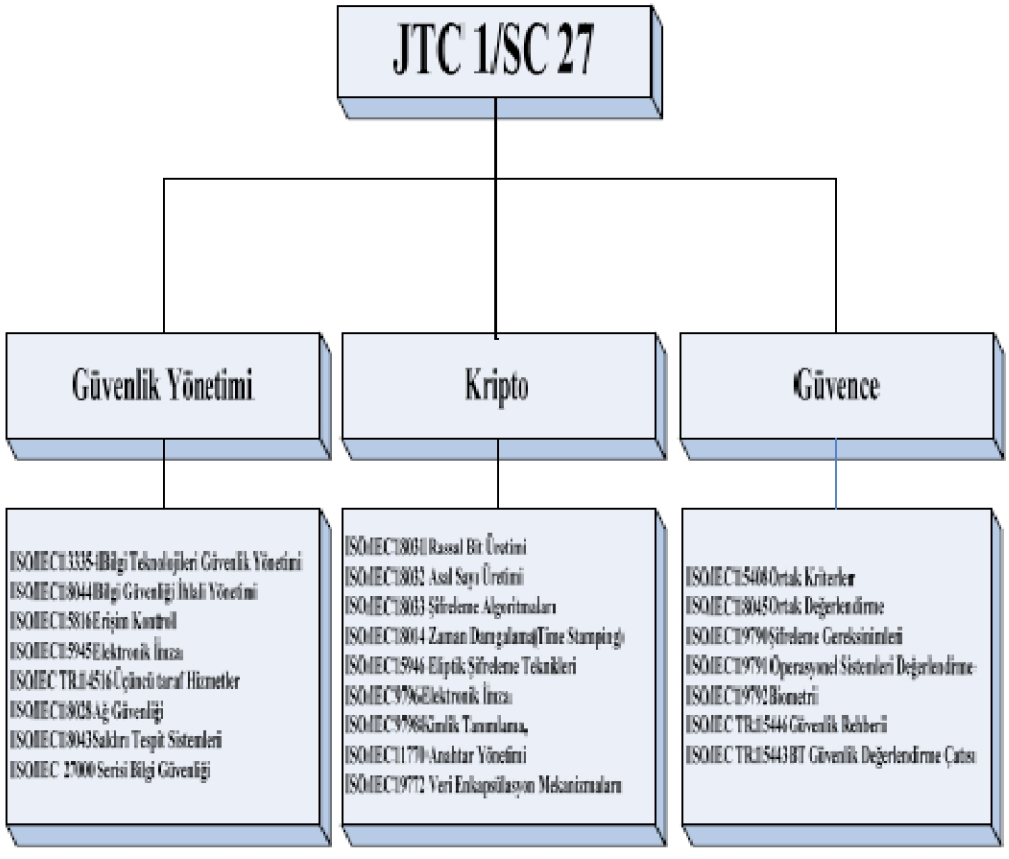
1, 2 ve 3 nolu çalışma grupları ve sorumlu oldukları konular Şekil 4.3'de gösterilmiştir.

SC27'ye bağlı çalışma gruplarından Çalışma Grubu–1 (WG-1), Şekil 4.3'de gösterilen bilgi güvenliği yönetim sistemleri standartları (ISO/IEC 17799, ISO/IEC 27000 Serisi) ile ilgili çalışmaları yürütmektedir. Bu standartlar aşağıda kısaca açıklanmıştır.

BS–7799 standardının ikinci sürümü Mayıs 1999'da çıktığında ISO, BSI' nın yayınladığı çalışmayla ilgilenmeye başlamıştır. Aralık 2000'de, ISO BS–7799

standardının ilk bölümünü alarak ISO/IEC 17779 olarak yeniden adlandırmış ve yeni bir standart olarak yayınlamıştır. ISO/IEC 17779 standardı daha önceki bölümde açıklanan BS–7799 standardının ilk bölümüne eşdeğerdir.

Şekil 4.3: ISO/IEC güvenlik çalışma grupları



Kaynak: ISO, 2007

ISO/IEC 17799 standardının uygulanmasıyla kurumsal bilgilerin tamamen güvende olduğunu söylemek doğru değildir. Bu standart bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kurumların kullanımı için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri kapsar. ISO/IEC 17799 güvenlik standartlarını bir kurumun uyguluyor olması kurumlara aşağıda sıralanan üstünlükleri sağlamaktadır. (ISO, 2007)

• Organizasyon Seviyesinde, sorumlulukları belirleyerek, kurumsal bilgi güvenliğinin her seviyede uygulanmasının yararlarını garanti eder.

• Kanuni Seviyede, kurumun ilgili tüm kural ve yönetmeliklere uyduğunu yetkili makamlara göstererek diğer standart ve mevzuatları tamamlar.

• İşletme Seviyesinde, Bilgi sistemleri, zafiyetleri ve nasıl korunacakları konusunda işletmenin yönlendirilmesini sağlayarak kurumsal bilgi sistemlerine daha güvenli erişim sağlanır.

• Ticari Seviyede, iş ortakları, hissedarlar ve müşteriler; kurumun bilgi koruması konusuna verdiği önem sayesinde kuruma olan güvenleri artırır ve ticari rakipleri arasında piyasada farklı bir yere gelmesini sağlar.

• Finansal Seviyede, güvenlik açıklarının belirlenerek önlem alınması sonucunda maliyetler azalacaktır.

• Çalışan Seviyesinde, çalışanın güvenlik konuları ve organizasyon içinde kendisine düşen sorumluluk hakkındaki bilgisini arttırarak bireysel olarak bilinçlendirilmesini sağlar.

ISO/IEC 17799 standardı 2005 yılında gözden geçirilerek ISO/IEC 17799:2005 ismiyle son halini almıştır. ISO/IEC 17799:2005 Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların bilgi güvenliği yönetim sistemini kurmaları, uygulamaları, sürdürmeleri ve iyileştirmeleri için hazırlanmış bir kılavuz olup önceki sürümünden farklı olarak, yaşanan problemlerden, arızalardan, kazalardan ders çıkarılması ve tekrar yaşanmaması için gerekli önlemlerin alınması için gerekli olan yönetim mekanizmasının kurulmasını sağlayan Bilgi Güvenliği İhlallerinin yönetimi ile ilgili bilgi güvenliği denetimlerini ve ilgili uygulamaları da içermektedir.

Tablo 4.1'de kısaca açıklanan standartların tamamı yayınlanarak kullanıma açılmamıştır. Yayınlanan standarda ek olarak geliştirme ve düşünce aşamasında olan standartlara ait açıklamalar aşağıda verilmiştir. ISO/IEC 27000, bilgi güvenliği serisinde yer alan standartlar içerisinde geçen teknik terimler ve açıklamalarının yer aldığı genel bir sözlük formatında geliştirilmektedir.

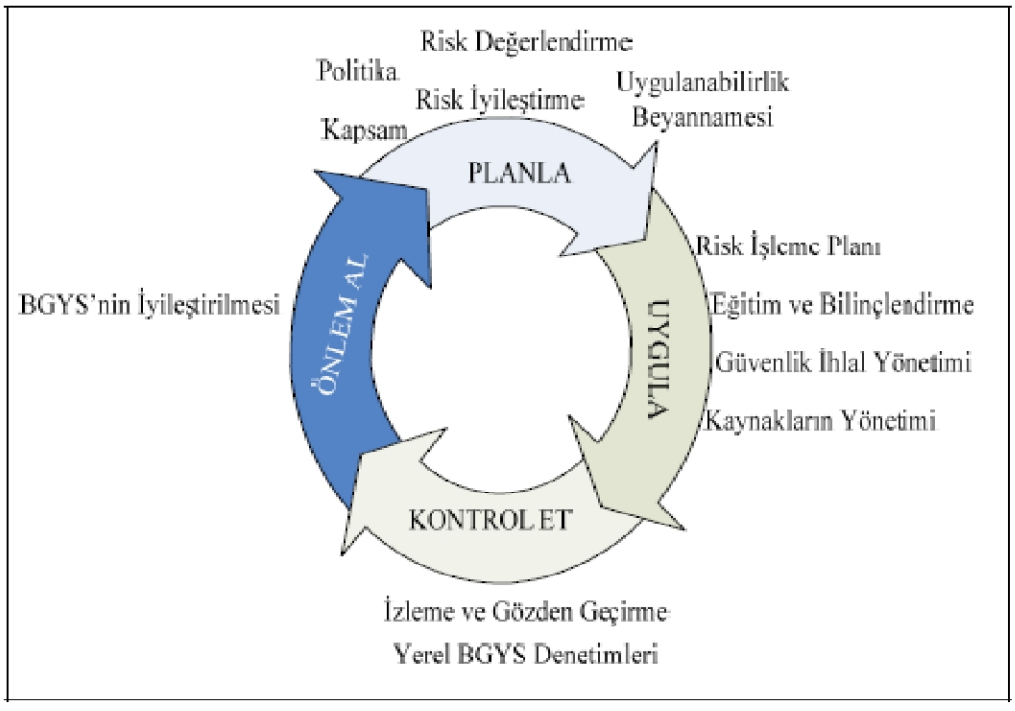
Tablo 4.1: ISO 27000 serisi standartları

Standart No	Açıklaması
ISO/IEC 27000–27059	Bilgi güvenliğiyle ilgili standartlar için ayrılmış aralık
ISO/IEC 27000	BGYS standartları için genel bir sözlük (hazırlanıyor)
ISO/IEC 27001	BGYS ihtiyaçları (BS7799 Bölüm–2) (2005 yılında yayınlanmıştır)
ISO/IEC 27002	BGYS uygulama ilkeleri (ISO/IEC 17799:2005)
ISO/IEC 27003	BGYS uygulama rehberi (hazırlanıyor)
ISO/IEC 27004	BGYS metrikleri ve ölçüm (hazırlanıyor)
ISO/IEC 27005	BGYS risk yönetimi (hazırlanıyor)
ISO/IEC 27006	BGYS belge kaydı ve belgelendirme süreçleri kılavuzu (hazırlanıyor)
ISO/IEC 27007	BGYS izleme (Audit) için kılavuz (hazırlanıyor)
ISO/IEC 27031	ISO/IEC 17799/27002 standardının Telekom sektörü için uyarlanması (hazırlanıyor)

Kaynak: Türk Standartları Enstitüsü, 2006, s:3-13

ISO/IEC 27001, BGYS için gereklilikleri ortaya koyan bir standarttır. Daha öncede anlatıldığı gibi bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur.

Şekil 4.4: ISO/IEC 27001 PUKÖ döngüsü



Kaynak: Türk Standartları Enstitüsü, 2006, s:3-13

Bu standart; yönetim standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirildiğinden yönetim standartlarının gereklerini de yerine getirmektedir. ISO/IEC 27001 standardının PUKÖ döngüsü Şekil 4.4'de gösterilmiş ve kısaca aşağıda açıklanmıştır.(Türk Standartları Enstitüsü, 2006, s:3-13)

Bunlar;

• Kapsam, daha önceki bölümlerde açıklandığı gibi kurumun tamamı veya belirli bir kısmını veya belirli bir hizmetini (internet bankacılığı, web uygulamaları, vb.) içerebilir.

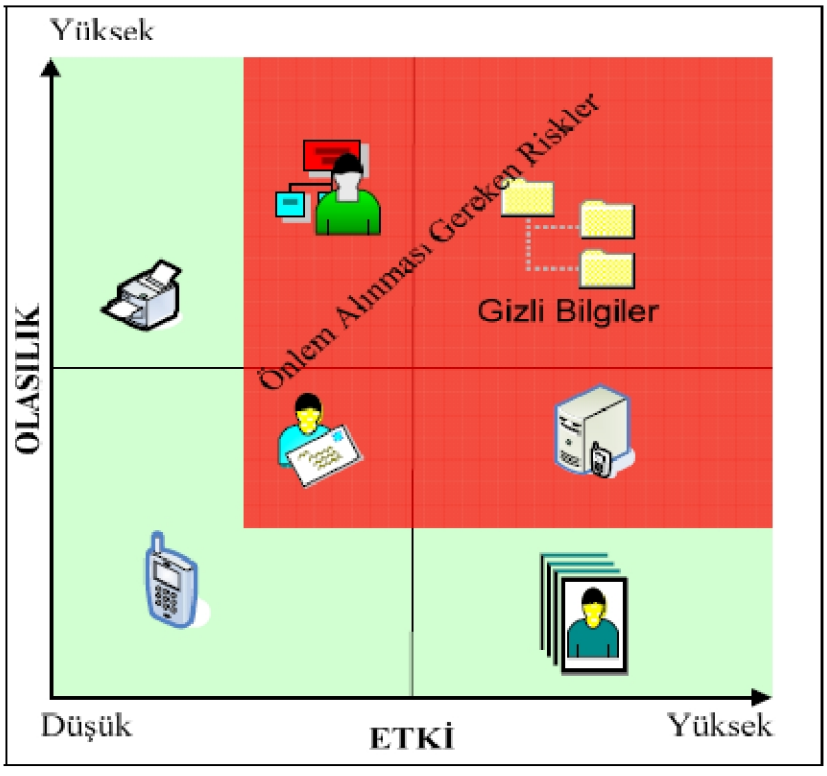
• Politika, Bilgi güvenliği neden önemlidir? Tehditler nelerdir? Risk yönetimi nasıl yapılmalıdır? Uyulması gereken kısıtlar (kanunlar yönetmelikler, vb.) nelerdir? Bu gibi soruların cevabını içeren üst yönetici tarafından onaylanan bilgi güvenliği politikasının bir üst kümesi olarak kabul edilen kısa dokümanlardır.

• Risk Değerlendirme, hangi bilgi varlıklarının korunacağı belirlendikten sonra kuruluşa uygun risk değerlendirme yönteminin seçilerek risklerin tanımlanması

yapılır. Seçilen risk değerlendirme yöntemine göre bilgi varlıkları Şekil 4.5'de örneği gösterilen risk haritasında konumlandırılır. Değerlendirilme yapıldıktan sonra risk değerlendirme haritasında, etkisi ve olasılığı yüksek olan tehditler için risklerin iyileştirilerek kontrol altına alınması işlemlerini kapsar. Risk haritasında bilgi varlıklarının yeri değişebileceğinden risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.

- Risk İyileştirme, risklerin değerlendirilmesi tamamlandıktan sonra ISO/IEC 27001 standardı risklerin nasıl iyileştirileceğinin açıklanmasını ister. İyileştirme çalışmaları kapsamında risk kabul edilebilir, transfer edilebilir (sigorta, vb.) azaltma çalışmaları yapılabilir. Riskler karşısında alınması gereken önlemlerin bulunduğu dokümanlar risk iyileştirme planlarını oluşturmaktadır.

Şekil 4.5: Risk değerlendirme haritası



Kaynak: ISO, 2007

- Uygulanabilirlik Beyannamesi, ISO/IEC 27001:2005 standardındaki kontrollerden hangilerinin kullanılıp kullanılmadığını gerekçeleriyle açıklayan belgelerdir. Kullanılan kontrollerin seçilme gerekçeleri, kullanılmayan kontrollerin

dışarıda bırakılmasının açıklamasını içerir. Kullanılmayan kontrollerin yanlışlıkla çıkarılmadığının çapraz denetimini sağlar. Uygulanabilirlik beyannamesi risk yönetimini ilgilendiren kararların özetini içerir.

• Risk İşleme Planı, güvenlik risklerini yönetmek için uygun yönetim eylemini, kaynaklarını, sorumluluklarını ve önceliklerini tanımlar. Seçilen kontrollerin yapılabilmesi için gerekli olan alt kontroller gerçekleştirilir ve kontrollerin etkinliği ölçülür.

• Eğitim ve Bilinçlendirme, programlarıyla kurumdaki tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin farkında olarak, BGYS' nin amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olması sağlanmalıdır. Ayrıca BGYS' yi teknik olarak etkileyecek işlerde çalışmak üzere uzman personel istihdam edilmesi veya ilgili personelin eğitimleri bu kapsamda yapılır.

• Güvenlik İhlal Yönetimi, güvenlik olaylarının anında tespit edilerek güvenlik ihlâllerine zamanında cevaplar verilmesini sağlar. Daha önce denenen ve başarılı olan güvenlik kırılmaları, güvenlik yöneticisinin güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığının belirlenebilmesi, güvenlik önlemlerinin alınarak güvenlik ihlallerinin önlenmesi, bir güvenlik kırılmasını önlemek için alınan önlemlerin etkili olup olmadığına karar verilir.

• Kaynakların Yönetimi, BGYS' yi kurma, gerçekleştirme, işletme, izleme, gözden geçirme, sürekliliğini sağlama ve iyileştirme için gereken kaynaklar kurum tarafından sağlanarak yönetimi yapılmalıdır.

• İzleme ve Gözden Geçirme, BGYS' nin etkinliğinin düzenli olarak gözden geçirilmesi ve oluşabilecek değişiklikleri (teknoloji, iş amaçları ve süreçleri, tehditler, vb.) dikkate alarak, bilgi varlıklarının risk değerlendirmesinin belirli aralıklarla yeniden yapılmasını sağlar.

• Yerel BGYS Denetimleri, ilk taraf denetimleri olarak adlandırılan yönetim tarafından kapsamın uygun kalması ve süreçlerin iyileştirilmesini sağlamak için

düzenli olarak kuruluş tarafından veya kuruluş adına danışman firmalar tarafından gerçekleştirilir. BGYS' nin iyileştirilmesi için kurum tarafından önleyici ve düzeltici tedbirler alınması gereklidir. Olumsuzlukların yaşanmaması için, risk değerlendirme sonuçlarına bağlı olarak değişen riskler bazında önleyici tedbirler alınmalıdır. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. BGYS gereksinimleriyle olumsuzlukları gidermek üzere düzeltici önlemler alınmalıdır. Önleyici tedbirler için gerçekleştirilen faaliyetler çoğunlukla düzenleyici tedbirler için gerçekleştirilen faaliyetlerden daha az maliyetlidir. ISO/IEC 27002, halen hazırlanma aşamasındadır. Bu standardın daha önceki bölümde açıklanan ISO/IEC 17799:2005 standardına eşdeğer olması beklenmektedir. Bilgi güvenliği ile ilgili standartların 27000 serisi altında yer almasından dolayı ISO/IEC tarafından böyle bir düzenlemeye gidilmiştir.

Geliştirilen standart içerisinde temel olarak; kritik başarı faktörleri, süreç yaklaşımı üzerine rehber, PUKÖ modeli rehberi, planlama süreç rehberi, uygulama süreç rehberi, kontrol süreç rehberi, önlem alma süreç rehberi ve diğer kurumlarla birlikte çalışma gibi konu başlıklarının yer alması beklenmektedir.

ISO/IEC 27004, halen geliştirilme aşamasında olan bu standart bilgi güvenliği yönetim metrikleri ve ölçümüne tahsis edilmiştir. Bilgi güvenliği yönetim sistemlerinin etkinliğinin ölçülmesi ve raporlanmasında kurumlara yardımcı olması beklenen bu standardın 2009 yılı içerisinde yayınlanmıştır. (ISO, 2007)

ISO/IEC 27005, halen geliştirilme aşamasında olan bu standart BS 7799 Kısım–3 "BS 7799–3,2006 – Bilgi Güvenliği Yönetim Sistemleri – Bilgi Güvenliği Risk Yönetimi Kılavuzları" isimli İngiliz standardının ISO tarafından uyarlanması çalışmasını içermektedir. BS 7799–3,2006 standardı 16 Mart 2006 tarihinde İngiliz standardı olarak kabul edilmiş, risklerin değerlendirilmesi, kontrollerin uygulanması, risklerin düzenli olarak izlenmesi ve gözden geçirilmesi gibi konu başlıklarını içermektedir.

ISO/IEC 27006, halen geliştirilme aşamasında olan bu standart "Bilgi Teknolojileri Felaket Önleme Hizmetleri Kılavuzu" ismiyle duyurulmuştur.

ISO/IEC 27007, ISO 27001 standardına göre BGYS denetlemesinde kullanılacak kılavuz niteliğinde geliştirilmesi düşünülen bu standart henüz tamamlanmamıştır.

ISO/IEC 27031, standardı ISO 17799/27002 standardı esas alınarak Telekom sektörü için özel olarak geliştirilmektedir. Kısa süre içerisinde ITU-T X.1051 ve ISO/IEC 27031 ismiyle yayınlanması beklenmektedir.

4.2. Türk Standartları

Türkiye'de bilgi güvenliği standartlarıyla ilgili çalışmalar ve belgelendirmeler, Türk Standartları Enstitüsü (TSE) tarafından yapılmaktadır. TSE teknik kurulunun ISO/IEC 17799:2000 standardını tercüme ederek 11 Kasım 2002 tarihinde aldığı karar ile TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri Türk Standardı olarak kabul edilmiştir. TS ISO/IEC 17799 standardı; kuruluşlar bünyesinde bilgi güvenliğini başlatan, gerçekleştiren ve süreklilik sağlayan, bilgi güvenliği yönetimi ile ilgili tavsiyeleri içermektedir.

BGYS belgelendirilmesine yönelik TSE teknik kurulu tarafından yapılan çalışmalar sonucunda BS 7799– 2,2002 standardının tercümesi yapılarak "Bilgi Güvenliği Yönetim Sistemleri–Özellikler ve Kullanım Kılavuzu" ismiyle TS 17799–2 standardı olarak 17 Şubat 2005 tarihinde kabul edilmiş ve yürürlüğe girmiştir. Ancak TS ISO/IEC 27001:2006 "Bilgi Teknolojisi–Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri–Gereksinimler", 2.3.2006 tarihinde Türk standardı olarak kabul edildiğinden TS 17799–2 standardı TSE tarafından iptal edilmiştir. (Türkiye Bilişim Derneği, 2005, s: 9)

TS ISO/IEC 27001:2006 standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kâr amaçlı olmayan kuruluşlar) kapsar. Bu standart, bir BGYS' yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. Bu standart ISO/IEC 27001:2005 standardından yararlanarak hazırlanmıştır. ISO/IEC 27001:2005 standardın tercümesidir.

4.3. Belgelendirme

BGYS' de belgelendirme, kurumsal bilgi güvenliğinin standartlara uyumlu bir şekilde yönetildiğine dair otoriteler tarafından verilen sertifikasyonlar aracılığıyla yapılmaktadır. Dünyada ve ülkemizde kurumsal bilgi güvenliği yönetim sistemlerinin belgelendirilmesinde uyumluluğa esas teşkil eden standart 2005 yılına kadar BS7799–2 standardı olurken bu yıldan sonra ISO/IEC 27001 standardı olarak değiştirilmiştir. 15 Nisan 2006 tarihine kadar olan 6 aylık bir hazırlık dönemi sırasında, denetimler ve belgelendirme ISO/IEC 27001:2005 veya BS 7799–2,2002 standartlarına göre gerçekleştirilmiştir. Ancak, bu süre içerisinde yayınlanmış olan yeni bir BS 7799–2,2002 sertifikasının, 15 Nisan 2007 tarihine kadar ISO/IEC 27001:2005'e geçişi tamamlanmıştır. 15 Nisan 2006 tarihinden sonra ise bütün denetimler ve belgelendirmeler ISO/IEC 27001:2005 standardına göre gerçekleştirilmiştir. ISO/IEC 27001:2005 belgelendirmesi için yapılması gereken altı aşama aşağıda kısaca açıklanmıştır. (BSI Eurasia 1, 2008)

Birinci aşamada, ISO/IEC 27001:2005 standardının tüm gereklerinin yerine getirilmesi ve standartta belirtilen yönetim iskelet yapısı oluşturulur. İkinci aşamada, uyumluluk denetimleri için yetkilendirilmiş sertifikalandırma kurumuna ön başvuru yapılır. Bu başvuruya istinaden denetimi yapacak firma belgelendirme için maliyet ve zaman çizelgesi sunar. Üçüncü aşamada, maliyet ve zaman çizelgesi kurum tarafından onaylanarak denetimi gerçekleştirecek firmaya resmi başvuru yapılır. Dördüncü aşamada, denetimi gerçekleştirecek olan kurum güvenlik politikasını, risk değerlendirmesi dokümanlarını, risk eylem planını, uygunluk beyanını ve güvenlik prosedürlerini içeren dokümantasyonu gözden geçirir. Bu işlem sonucunda, bilgi güvenliği yönetim sistemindeki sorunlu olan ve çözüme kavuşturulması gereken herhangi bir zayıflığın veya göz ardı edilen bir hususun ortaya çıkarılması hedeflenir. Beşinci aşamada, masaüstü kontrolü başarılı şekilde sonuçlandıktan sonra, denetim firmasının belirlediği denetçiler tarafından yerinde denetim gerçekleştirilir. Kuruluşun büyüklüğüne ve iş tipine uygun kontrollerin olup olmadığı gözden geçirilir ve elde edilen sonuçlara göre kurumlara önerilerde bulunulur.Altıncı aşamada ise değerlendirmenin başarı ile tamamlanmasının ardından, Bilgi Güvenliği Yönetim Sisteminin kapsamını açık bir şekilde tanımlayan bir sertifika verilecektir. Bu sertifika 3 yıl boyunca geçerliliğini korur ve rutin değerlendirme ziyaretleri ile desteklenir. ISO/IEC 27001 standardına göre kurulmuş olan bir bilgi güvenliği

yönetim sistemi ile kurumların bilgi güvenliği yönetiminde, kapsamlı prosedürler aracılığıyla güvenlik kontrollerini sürekli ve düzenli olarak işletmeyi ve sistemin sürekli iyileştirilmesi gerçekleştirilmektedir. Güven ve güvenilirliğin hayati önem taşıdığı alanlarda hizmet veren kuruluşların, uluslararası geçerlilikte bilgi güvenliği yönetim sistemleri standardına uygunluk belgesine sahip olması, hem mevzuat hem de kuruluşun güvenli işleyişi açısından bir zorunluluk olarak değerlendirilmektedir.

4.4. Kurumların ISO/IEC 27001 sertifikası almasının avantajları

(BSI Eurasia 2, 2008)

4.4.1. Kredilendirilebilirlik, güven ve itimat

Belgelendirme, kurum veya kuruluşun bilgi güvenliğini dikkate aldığını, bilgi güvenliğinin sağlanması için gerekli olan adımları uyguladığını ve kontrol ettiğini ispatlamaktadır. Bu sayede kurumlar veya kuruluşlar birlikte iş yaptıkları veya hizmet verdikleri kurum veya bireylerin tüm bilgilerinin BGYS sayesinde güvende tutulacağı konusunda verdikleri taahhütten dolayı iş yaptıkları kurum, kuruluş veya bireylerin kendilerini güvende hissetmelerini sağlayacaklardır. Belgelendirme sonucunda özellikle özel sektör firmalarında rekabet anlamında sertifika almamış rakiplerinin bir adım önüne geçerek avantaj sağlayacaklardır. Ayrıca günümüzde uluslararası yapılan işlerde ISO/IEC 27001:2005 şartı koşulmaktadır.

4.4.2. Tasarruf

Oluşabilecek güvenlik ihlallerine karşı kontrollerin uygulanması ile maliyetler düşmektedir. Sadece bir bilgi güvenliği ihlalinin oluşturacağı zarar bile çoğu zaman çok büyük maddi kayıplara yol açabilir. Belgelendirme işlemi kurumların maruz kalacağı bu tür ihlalleri azaltarak bilgi güvenliği ihlallerinden doğan zararları en aza indirecektir.

4.4.3. Yasal Uygunluk

Belgelendirme işlemi, kanun ve tüzüklere uygunluğun yetkili ve ilgili makamlara yasal anlamda uygunluğun sağlandığına dair kanıt teşkil edilmesine yardımcı olur.

4.4.4. Taahhüt

Belgelendirme işlemi, organizasyonun tüm aşamalarında taahhüt/bağlılığın sağlanması ve kanıtlanmasında yardımcı olur.

4.4.5. Operasyonel Seviye Risk Yönetimi

Kuruluş genelinde, bilgi sistemleri ve zayıflıklarının nasıl korunacağı konusundaki farkındalık artar. Ayrıca donanım ve veriye daha güvenli bir şekilde erişim sağlanır.

4.4.6. Çalışanlar

Çalışanların kuruluş içerisindeki sorumlulukları ve bilgi güvenliği konularındaki bilinçlerinin artmasını sağlar.

4.4.7. Sürekli İyileşme

Düzenli olarak gerçekleştirilen denetimlere bağlı olarak bilgi sistemlerinin etkinliği izlenecek ve izleme sonucunda tespit edilen problemler giderilerek bilgi sistemlerinde genel anlamda bir iyileşme sağlanabilecektir.

4.4.8. Onay

Organizasyon için tüm seviyelerde bilgi güvenliği varlığının bağımsız kuruluşlar tarafından onaylandığını göstermektedir.

5. KURUMLARDA BİLGİ GÜVENLİĞİ FARKINDALIĞININ ÖNEMİ

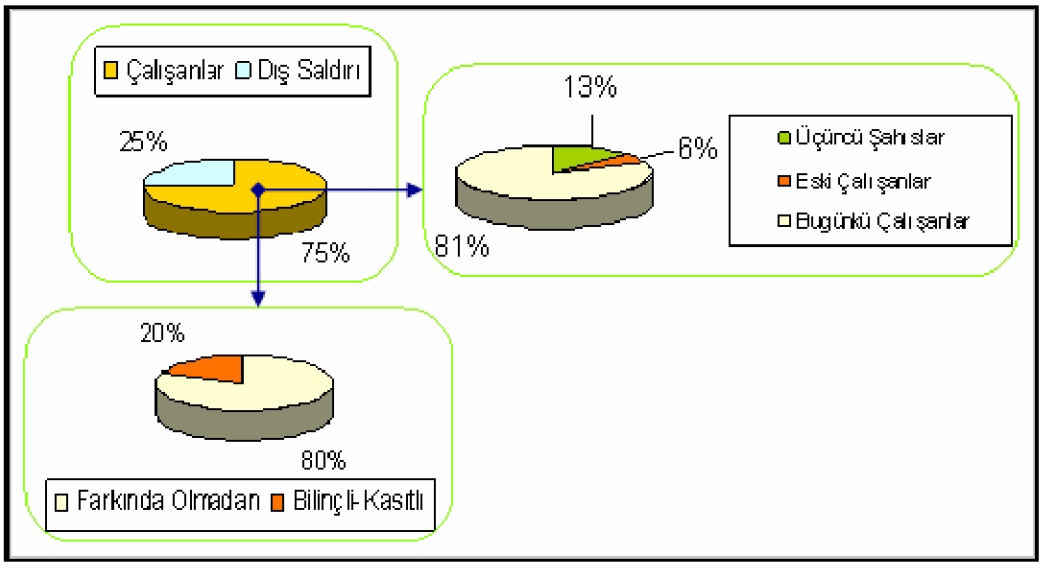
Kurumlarda bilgi güvenliği farkındalığı çalışmalarının ana hedefi; basta çalışanları olmak üzere bilgi alışverişi yaptığı bireylere kurumu için değerli bir varlık olan bilgi ve bilgi varlıklarının koruması konusunda üzerlerine düsen sorumlulukları anlamalarını sağlamak olmalıdır. Kurum için bu durum kritik bir öneme sahiptir.

Kurumun bilgi güvenliğinden sadece bilgi güvenliği çalışanları değil kurumun tüm çalışanları hatta paydaşları, tedarikçileri kısaca kurum bilgi güvenliği politikasında yer alan tüm bireyler sorumludur. Farkındalık ile çalışanlar üzerinde güvenlik bilinci oluşturulurken hangi bilgilerin korunması gerektiği, bunların ne tür tehditlere karsı nasıl korunması gerektiği konusunda bilinçlendirme yapılır.

Kurumlarda Bilgi Güvenliğini, çalışanların düşünce ekseninde tutmanın en etkili yollarından biri çalışanın bilgi güvenliği sorumluluklarını aynı zamanda bir iş sorumluluğu olarak görmesini sağlamaktan geçer. Ancak bunu çalışanlar üzerinde bir farkındalık oluşturmadan tek basına görev tanımlarına yazmakla sağlamayı ummak bir beklentiden öteye gidemez. Kurum bilgi güvenlik risklerini kabul edilebilir. Seviyeye indirgemede yararlanılan bilgi güvenliği farkındalığı oluşturmada ki asıl amaç; bilgi eksikliğinden kaynaklanabilecek insan hatalarını ve teknolojinin yanlış kullanılması risklerinin azaltmak, bireylerin bilgi güvenliği tehditleri ve sorunlarından haberdar edilmesi, normal çalışma zamanları içinde kurumun güvenlik politikasını desteklemek üzere donanımlı bir hale getirebilmeyi sağlamak olmalıdır.

Gartner Datapro Research şirketi tarafından yapılan araştırmanın sonuçları, kurumsal bilgilerin nasıl, kimler tarafından tehdit edilebileceği ve zarar verilebileceği hakkında ilginç sonuçlar vermektedir. Genel olarak ilk başlarda saldırıları yapanların yaşça oldukça genç ve kendilerine ün sağlamak isteyen bilgisayar saldırganları olduğu ancak son zamanlarda bunların yerlerini daha çok maddi gelir sağlamayı amaçlayan organize örgütlerin aldığı yönündedir. Bu ve benzeri araştırma sonuçları doğrultusunda oluşturulmuş aşağıdaki grafiklerde güvenlikte insan unsurunun önemi ve farkındalık oluşturulması zorunluluğunu açık bir şekilde sergilenmektedir. (Şahinaslan ve diğerleri, 2009, s:2)

Şekil 5.1: Bilgi Güvenlik İhlallerinde İnsan Faktörü



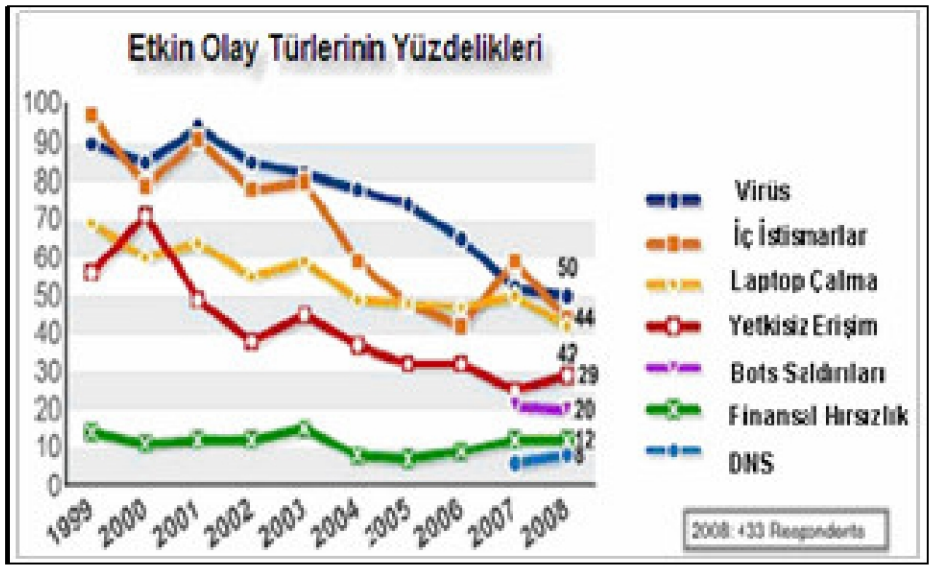
Kaynak: Şahinaslan ve diğerleri, 2009, s:3

Kurumlar her geçen gün gelişen teknolojiden biraz daha fazla faydalanır hale gelmişler ve pazarlarda kendilerine rekabet üstünlüğü sağlamak amacıyla süreçlerini güçlendirmektedirler.

Internet'in çok yaygın olarak kullanılmasına paralel olarak güvenlik açıklarının artması, davranış temelli güvenlik açıklarını oluşturan sosyal mühendislik, kimlik hırsızlığı gibi tehditlerini ortaya çıkartmıştır. Araştırmalar gösteriyor ki, etkili atak modelleri arasından ilk ikisi, bilgilere yetkisiz erişim ve kurum bilgilerinin çalınması üzerine gerçekleşmiştir. Yapılan araştırmaların ikinci yönü ise günümüz dünyasında geçmiş yıllara göre atakların artık yıkıcı yönünün geride kaldığını; yerine bilgi sızdırma, hırsızlığı ve istihbarat çalışmaları yönünün daha ön planda olduğunu gösterir.

2008 SANS ISC raporuna göre saldırganların güvenlik duvarını, anti virüs hatta saldırı tespit sistemlerini aşmada kullandığı ilk hedefin kolayca kandırılabilen insan faktörü olduğudur. Bilgisayar Güvenlik Enstitüsünün, 2008 bilgisayar suçu ve güvenlik araştırmasına göre; virüs, iç istismarlar, bilgisayar hırsızlığı ve yetkisiz erişim en çok rastlanan güvenlik olaylarıdır. Bu rapora; güvenlik olaylarının yıllara göre gösterdikleri değişimler aşağıdaki grafik de gösterilmektedir. Bu grafik de genel olarak 1999 yılından 2008 yılına kadar bazı tehditlerin gerekli farkındalık çalışmaları ve kullanılan güvenlik teknolojileri sayesinde büyük bir düşüş yaşandığı gözlemlenmektedir.

Şekil 5.2: Etkin Bilgi Güvenlik Olayları



Kaynak: Şahinaslan ve diğerleri, 2009, s:3

Tablo 5.1'de görülebileceği gibi 2007 yılındaki kurum içinde bilinçli ya da bilinçsiz bir şekilde yapılan güvenlik istismarları %59' dan 2008 yılında bu durum bilgi güvenliği farkındalık çalışmaları ile %44'e kadar düşürülebildiği gözlemlenmektedir. Yine etkin bilgi güvenlik olaylarına ait yüzdelik dilimler incelendiğinde en büyük tehdit unsurunu iç tehditler olduğu görülmektedir. Bu durumda insan faktörünün kurum için önemini açık bir şekilde göstermektedir.

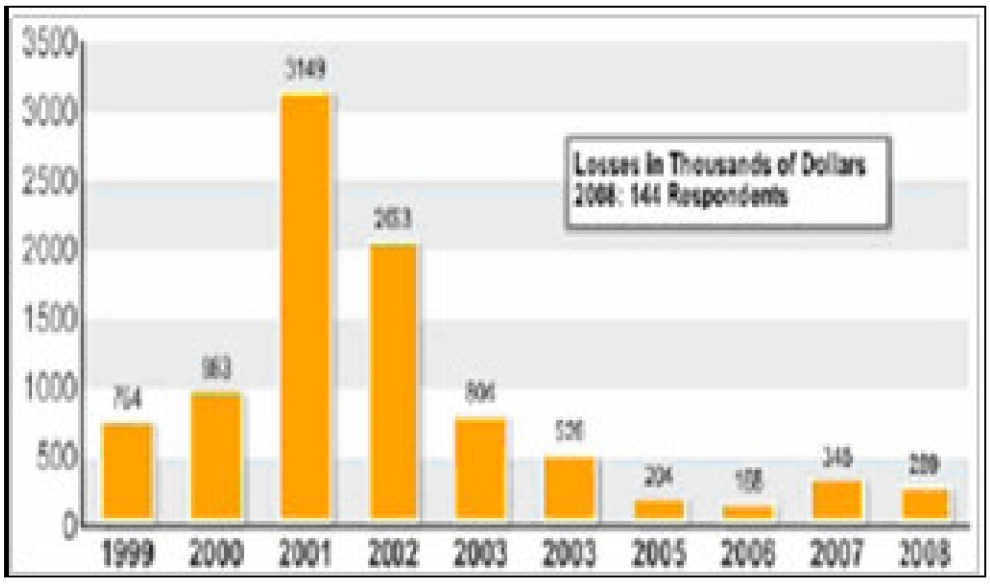
Tablo 5.1: Bilgi Güvenlik Olayları Yüzdelik Dilimleri

Saldırı Turleri	2004	2005	2006	2007	2008
DOS Ataklan	39%	32%	25%	25%	21%
Laptop Çalma	49%	48%	47%	50%	40%
Telekom Dolandırıcılığı	10%	10%	8%	5%	5%
Yetkisiz Erişim	37%	32%	32%	25%	29%
Virüs	78%	74%	65%	52%	50%
Finansal Sahtekarlık	8%	7%	9%	12%	12%
İç Suistimaller	59%	48%	42%	59%	44%
Sisteme Sızma	17%	14%	15%	13%	13%
Sabotaj	5%	2%	3%	4%	2%
Çalma/ Özel bilgi kayıpları	10%	9%	9%	8%	9%
Kablosuz Ağ Suistimalleri	15%	16%	14%	17%	14%
Web Site Saldırıları	7%	5%	6%	10%	6%
Web Uygulamalarını kötüye kullanma	10%	5%	6%	9%	11%
Bots (DDoS, Spam, Sniffer)	-	-	-	21%	20%
DNS Ataklan	-	-	-	6%	8%
Anlık Mesajlaşma Suistimalleri	-	-	-	25%	21%
Parola dinleme	-	-	-	10%	9%
Çalma/Müşteri bilgileri kayıpları	-	-	-	17%	17%

Kaynak: Şahinaslan ve diğerleri, 2009, s:4

Şekil 5.2'deki grafik de yukarıdaki tablo 5.1'de gösterilen güvenlik olaylarının kurumlar bazında 1999–2008 ortalama maddi zarar dağılımı gösterilmektedir. En yüksek maddi zarar 2001 yılında vuku bulmakla birlikte 2001'den 2008 yılına kadar belirli oranlarda düşüşler yaşanmıştır.

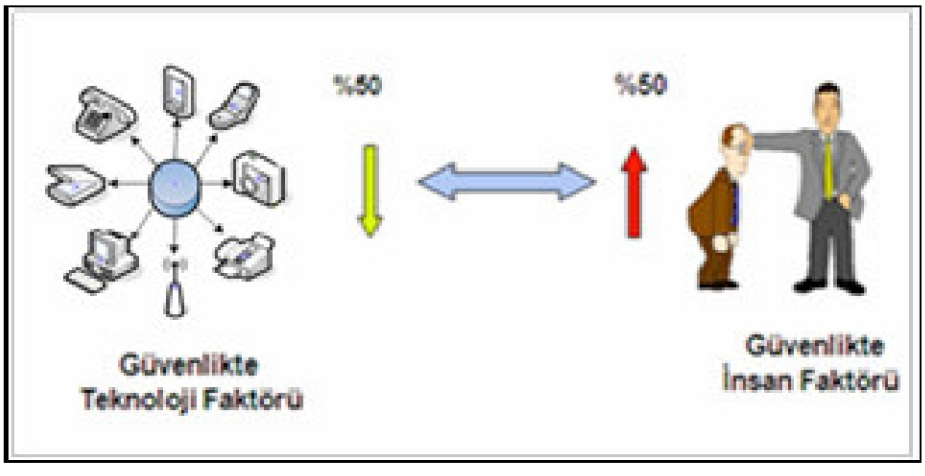
Şekil 5.3: Yıllara Göre Ortalama Zarar Kaybı



Kaynak: Şahinaslan ve diğerleri, 2009, s:4

Tüm bu grafiklerden çıkarılabilecek sonuca göre, aşağıdaki şekil 5.4'de güvenlikte teknoloji ve insan faktörünün etkisinin yüzdelik oranı %50 olarak verilmiştir fakat bu değerin önümüzdeki günlerde ilerleyen teknolojiye paralel olarak daha da artacağı düşünülmektedir.

Şekil 5.4: Güvenlikte Teknoloji ve İnsan Faktörünün Yönü



Kaynak: Şahinaslan ve diğerleri, 2009, s:4

Bütün bunlardan çıkartılması gereken sonuç güvenliğin bir teknoloji sorunu olmaktan çok süreç ve is yönetimi sorunu olduğunun kabul edilmesinden geçer. Bu nedenle günümüz koşullarında kurumların esas değerini oluşturan insan varlığı ve onun bu süreçlere göre performansından ödün vermeden güvenli şekilde yönetmek, kurumun olduğu kadar çalışanlarında yararınadır. Bunu sağlamanın yolu kurumsal bir farkındalık programı oluşturmak ve bunu belirli dönemlerde veya farklı yöntemlerle çalışan zihinlerde aktif bir şekilde tutacak bilinçlendirme çalışmalarını yapmaktan geçmektedir. Kurumlarda bilginin paylaşıldığı bireylerin yapabilecekleri çok küçük hatalar, dikkatsizlikler, bilinçli ya da bilinçsiz yapılabilecek her türlü suistimaller teknik anlamda alınan tüm güvenlik önlemlerini boşa çıkaracaktır. Bu nedenle kurumlar, günümüz şartlarına uygun bir farkındalık oluşturmak zorundadır.

5.1. Bilgi Güvenliği Farkındalığı Oluşturma Yöntemleri

Bilgi Güvenliği çalışanları bu konuda yeteri kadar donanıma sahip olmalı veya gerekiyorsa bu anlamda bir danışmanlık hizmeti de alınabilir. Bilgi güvenliği farkındalığını oluşturmanın ana yolu kurumda en üst seviyedeki yönetimden en alt seviyedeki çalışana hatta tedarikçilere kadar çalışanların görev ve pozisyonları da dikkate alınarak ihtiyaç ve beklentilere göre farklı eğitim ve farkındalık programları hazırlanmalı ve eğitimler düzenlenmelidir. Bu eğitimler bir çalışan işe başladığında verilen oryantasyon eğitimlerinin ayrılmaz bir parçası olarak düşünülmeli ve mutlaka her çalışana en az bir kez verilmelidir. Daha sonraki dönemlerde ise çalışana planlamış varsa alması gereken diğer eğitimler düzenli olarak verilmedir. Kurumlarda çalışanlar/bireyler üzerinde farkındalık oluşturmada sınıf içi eğitimler yanında pek çok farklı yöntemler de bulunmaktadır.

Bunlar;

- Internet tabanlı interaktif sanal eğitimleri verilebilir.

- E-Learning eğitimleri; zorunlu bilgi güvenliği eğitimleri ya da pozisyona göre özel interaktif sanal eğitimler hazırlanabilir.

- Çalışanlara yönelik masaüstü bilgi güvenliği (el kitabı) kitapçığı ve renkli broşürler, posterler hazırlanabilir.

- Kurumdaki birimler bazında aylık etkinlikler düzenlenip, ilgili birimlerin güvenlik konusundaki eksiklikleri ve dikkat edilmesi gereken güvenlik unsurları açıklanarak, bir farkındalık oluşturulabilir.

- LCD' lerde çeşitli animasyonlar hazırlanabilir.

- Film gösterileri (Multimedya) hazırlanabilir.

- Bilgi güvenliği e-posta bülteni hazırlanabilir.

- Ekran koruyucu ile mesajlar iletilebilir. Bu mesajlar bilgisayar güvenliği ve kurumun bilgi güvenliği politikasını yansıtacak şekilde parola güvenliği, e-posta güvenliği vs. gibi konuları içerebilir.

- Bilgi güvenliği mesajlarını iletmek için farklı küpler hazırlanabilir. Her çalışanın masasına konur ve bunlar günlük olarak bir biriyle değiştirilebilir.

- Bilgi Güvenliği konusunda oyunlar hazırlanabilir.

- Son kullanıcının seviyesine göre simülasyonlar hazırlanabilir. Bu oyunlarda kullanıcıya güvenlik açıklarının bulunması yönünde bir strateji ile farkındalık oluşturulabilir. Bilgi güvenliği oyunu ile hedeflenen ana nokta, kurum çalışanlarına kurum için önem ve gizlilik taşıyan bilgi varlıklarının neler olduğu ve bunların saklanması konusunda bilgilendirilmesi, kurumsal bilginin kolayca savunmasız kalabileceği, gereksiz görülen şeylerin izinsiz erişime neden olabileceği hakkında bilinirliğin arttırılması ve kurumsal bilgi güvenliğinin sağlanmasının kurum için ne kadar önemli olduğunun çalışana fark ettirilmesidir.

- Karikatürlerle, insanlara hoş eğlenceli gelecek şekilde kullanıcıyı bilinçlendirecek bir kurgu üzerinden gidilerek sunular hazırlanabilir.

- Belirli aralıklarla kurumda çalışanlara yönelik yazılar ya da yukarıda ifade edilen şekilde sunular hazırlanıp, yayınlanabilir.

- Kullanıcıların masaüstü arka planları bilgi güvenliği farkındalığına uygun şekilde tasarlanabilir.

- Güvenliği hatırlatan sisteme giriş mesajları, mousepad, anahtarlık, not kâğıtları logo veya sloganlar hazırlanabilir.

- Çalışanlara güvenlikle ilgili sesli e-posta ve video görüntüleri gönderilebilir veya bir portal üzerinden yayınlanabilir.

- Çalışanların güvenlik hassasiyetleri değerlendirilip ödüllendirme yoluna gidilebilir.

- Farkındalık amaçlı bulmacalar hazırlanıp kurum bazında periyodik olarak yayınlanabilir, bulmacayı doğru çözen ilk üç çalışan ödüllendirilebilir.

- Bu anlamda kurumda etkinlikler oluşturulup, çeşitli skeçler, oyunlar hazırlanabilir.

- Bilgi güvenliği oyun turnuvaları düzenlenebilir.

- Yapboz türü oyunlar geliştirilebilir.

Ayrıca kurum çalışanların yanı sıra müşterilere de bu tür eğitimler verilmelidir.

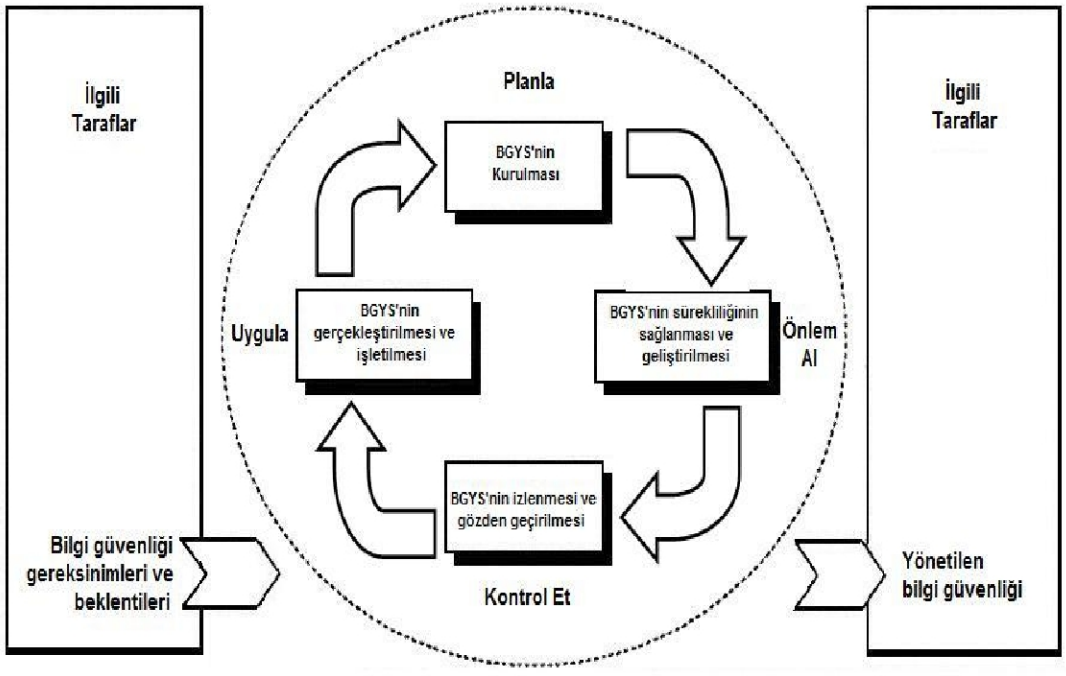
6. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Bilgi Güvenliği Yönetim Sistemi 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 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, 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, dokümante edilmiş bir 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. Her iki standardın 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. Bu iki standart da doğrudan bilgi güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir.

BGYS standartları kapsamında BGYS' in kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için PUKÖ (Planla – Uygula –Kontrol et – Önlem al) modeli kullanılmaktadır. PUKÖ modelini görsel olarak anlatan Şekil 6.1, bir BGYS' nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve işlemler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir. (Önel ve Dinçkan, 2007, s:7)

Şekil 6.1: BGYS Süreçlerine uygulanan PUKÖ modeli



Kaynak: Önel ve Dinçkan, 2007, s:8

Planla (BGYS' nin kurulması)

BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesidir.

Uygula (BGYS' nin gerçekleştirilmesi ve işletilmesi)

BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesidir.

Kontrol Et (BGYS' nin izlenmesi ve gözden geçirilmesi)

BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesidir.

Önlem al (BGYS' nin sürekliliğinin sağlanması ve iyileştirilmesi)

Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesidir

Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi (Planla – Uygula – Kontrol et – Önlem al) faaliyetleri 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.

BGYS kurulumu PUKÖ modelinin ilk adımını (Planla) teşkil etmektedir. Yerleşik bir sistemden bahsedebilmek için diğer adımların da uygulanması ve bunların bir döngü içinde yaşaması gerekir.

6.1. BGYS Kurulumu

Kurulum adımlarına geçmeden önce BGYS ile ilgili bilinmesi gereken gerçeklerden bahsetmek gerekir. Öncelikle sağlıklı işleyiş ve yarar sağlaması açısından BGYS kurulum isteği kurumun üst yönetimi tarafından benimsenmelidir. Üst yönetim desteği BGYS' nin başarıya ulaşması açısından hayati öneme sahiptir. Öncelikle üst yönetim BGYS' nin gerekliliğine ve faydasına inanmalıdır. Bu birincil şarttır. Diğer önemli bir husus, BGYS kurulumu bir BT ürünü veya sistemi kurulumuyla karıştırılmamalıdır. BGYS kurumun iş yapma tarzını etkileyen köklü bir sistemdir ve kurumu tümden etkiler. Tüm kademelerdeki çalışanların işini yaparken bilgi güvenliği prensiplerine uygun hareket etmesini gerekli kılar. Bu bilincin oluşması ve işleyişe geçmesi de bir gelişim sürecinin sonucu olacaktır. Bir önceki bölümde bahsedildiği gibi BGYS sürekli bir gelişim sürecidir.

BGYS ile ilgili en yaygın yanlış kanılardan bir tanesi de bunun sadece kurumun BT bölümüne ait bir iş olduğunun düşünülmesidir. BGYS bir teknoloji meselesi veya teknik bir iş değildir. Tüm kurumun aktif halde katılımıyla hedefine ulaşabilecek bir sistemdir. En üst kademe yöneticiden en alt seviye çalışana kadar katılım ve destek şarttır. Aksi halde BGYS' den beklenen faydanın elde edilmesi mümkün değildir.

Etkin bir BGYS kurulumu konusunda ilk yapılması gereken işlerden bir diğeri de kurum içinde bir Bilgi Güvenliği Komisyonu oluşturulmasıdır. Bilgi güvenliği komisyonu (Güvenlik Forumu da denir) kurum içindeki her bölümden

temsilcilerden oluşur. Bilgi işlem, iç denetim, muhasebe, insan kaynakları, güvenlik ve diğer tüm bölümlerden temsilciler bu komisyonda yer almalıdır. Komisyon temsilcileri bilgi güvenliği konusunda deneyimli ve bilgili, bunun yanında kendi bölümlerini temsil edebilme yetkisine sahip kişiler olmalıdır. Komisyon temsilcileri bilgi güvenliği konusunda yeterli bilgi seviyesine sahip değilse mutlaka BGYS eğitimleri almalıdır. Tüm bölümlerden temsilcilerin komisyonda yer alması BGYS' nin başarı şansını arttırır. BGYS' in kurumun tamamına nüfuz etmesini kolaylaştırır. Kurum çapındaki güvenlik ihtiyaçlarının daha etkin bir biçimde farkında olunmasını sağlar. Bu durum BGYS' in doğru planlanması ve sağlıklı işlemesi açısından hayati öneme sahiptir. Her bölümden bir temsilcinin katılımı yönetim ve teknik kadro arasındaki iletişim kopukluğunu gidermeye de yarar. Sorunları ve ihtiyaçları yerinde yaşayan kişiler belli konularda yönetimin daha rahat ikna edilmesini sağlar. Bilgi güvenliği komisyonu sayesinde BGYS ile ilgili görev ve sorumluluklar da kurum içinde dağıtılmış olur. Daha önce de belirtildiği gibi BGYS sadece BT bölümüne ait bir iş değildir. (Önel ve Dinçkan, 2007, s:9)

6.2. Kurulum Adımları

BGYS konusunda temel başvuru kaynakları ISO/IEC 27001 ve ISO/IEC 27002 standartlarıdır. BGYS kurulumu öncesinde bu standartların mutlaka dikkatlice okunup anlaşılması gerekmektedir. BGYS kurulumu TS ISO/IEC 27001:2005'teki "BGYS' nin Kurulması" ve TS 13268-1 "BGYS' nin kurulması" başlıkları altında detaylı olarak açıklanmaktadır.

BGYS kurulumunda sırasıyla izlenmesi gereken adımlar şöyledir:

6.2.1. Kapsam Belirleme

BGYS' nin kapsamı ve sınırları belirlenmelidir. BGYS' nin kapsamı kurumun belli bir kısmı olabileceği gibi, kurumun bütünü de olabilir. Ancak, her iki durumda da, kurumun BGYS kapsamını ve sınırlarını eksiksiz ve doğru bir biçimde tanımlaması gerekmektedir. Örneğin sadece kurum içindeki bir bölüm veya bir bölümün verdiği tek bir hizmet için de bir 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 ve diğer kurumlarla olan etkileşimleri de dikkate almak gereklidir. Kapsam dışında bırakılanların hangi sebeplerle dışarıda bırakıldıklarını kurumun sağlam gerekçelerle açıklayabilmesi gerekmektedir. Bu adımın sonunda bir kapsam dokümanı yayınlanmalı ve üst yönetim tarafından onaylanmalıdır. BGYS kapsamı belirlenmesi konusunda daha detaylı bilgiler için BGYS0002 kodlu dokümana başvurulmalıdır.

6.2.2. BGYS Politikası

Ardından BGYS politikasının oluşturulması gerekmektedir. Bu politika, hedefleri ortaya koyan, yönetime yön veren ve harekete geçiren, hangi riskin değerlendirmeye alınacağına ilişkin risk yönetim kapsamı ve kriterini belirleyen bir çerçeve sunmalıdır. BGYS politikasının amacını bulması için yönetim politika içeriğindeki maddelerin uygulamaya geçirileceğine ilişkin kararlarlığını çalışanlara hissettirmelidir.

6.2.3. Risk Değerlendirme Yaklaşımı

Bilgi güvenliği politikası temel alınarak sistematik bir risk değerlendirme yaklaşımı belirlenmelidir. Kurum kendine uygun bir metodoloji seçmekte serbesttir. Seçilen risk değerlendirme metodolojisi kıyaslanabilir ve tekrarlanabilir sonuçlar üretmeyi garanti etmelidir. Bu adımda kabul edilebilecek risk seviyeleri belirlenmeli ve bunlar için ölçütler geliştirilmelidir. Risk değerlendirme metodu seçiminde kurumlar risk değerlendirme konusunda daha fazla bilgi veren BS 7799-3 standardına başvurabilirler.

6.2.4. Risk Belirleme

Korunması gereken varlıkları tehdit eden riskler, Adım 3'te belirlenen yöntem kullanılarak tespit edilmelidir. BGYS içerisindeki tüm varlıkların tanımlanması, yani varlık envanterinin çıkarılması risk değerlendirme işinin esasını oluşturur. Kurum BGYS kapsamına dâhil edeceği tüm varlıkların sahiplerini, türünü ve önem derecesini bir envanter 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. Varlıkların bu üç temel güvenlik özelliğine gelecek zararlar farklı etki derecelerine sahip olabilirler. Örneğin çok gizli seviyede bir bilginin açığa

çıkması kuruma büyük zararlar verebilecekken aynı gizli bilginin kullanılamaz hale gelmesi o kadar büyük zarar yaratmayabilir.

6.2.5. Risk Analizi ve Derecelendirilmesi

Tespit edilen risklerin analizi ve derecelendirilmesi yapılmalıdır. Bu adım bir önceki adımda tespit edilen risklerin yorumlanması olarak görülebilir. Risk analizi yaparken riske neden olan tehdit ve açıklıklardan yola çıkılmalıdır. Risk, açıklığın bir tehdit tarafından kullanılmasıyla oluşur. Örneğin duvarı delik bir ev düşünelim. Duvardaki delik açıklığı temsil eder. Olası bir sel ise burada tehdidi oluşturur. Bu ikisinin bir araya gelmesiyle risk oluşur ki bu örnekte risk evi su basmasından dolayı evdeki insanların veya eşyaların zarar görmesidir. 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 nitel değerlerle de belirlenebilir. Riskin kabul edilebilir olup olmadığı Adım 3'te belirlenen ölçütler kullanılarak tespit edilmelidir. Tüm bu hesaplama ve değerlemeler uygulanmakta olan mevcut kontroller de dikkate alınarak yapılmalıdır. Kontroller risk değerini azaltabilir. Bu adım sonunda bir risk değerlendirme sonuç raporu yayınlanmalıdır.

6.2.6. Risk İşleme

Bu adımda risk değerlendirme sonuç raporundan yola çıkılarak uygun risk işleme 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 edilmesi

6.2.7. 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. Bu kontroller standartta yol gösterici olması amacıyla verilmiştir. 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. Sadece TS ISO/IEC 17799:2005'ten değil herhangi bir bilgi güvenliği kaynağından uygun kontrol seçilebileceği gibi kurumun kendine özel geliştirebileceği kontroller de olabilmektedir. Fakat gözden kaçan önemli bir kontrol hedefi veya kontrol olmadığından emin olmak için bu listeyi bir başlangıç noktası olarak kullanmakta fayda görülmektedir.

6.2.8. Artık Risk Onayı

Risk işleme süreci sonrasında geriye kalan riske artık risk denir. Bunlar kabul edilen riskler veya tamamen ortadan kaldırılamayan riskler olabilir. Kurum üst yönetimi artık riskler için onay vermelidir. Bu adım sonunda artık risk onay belgesi oluşturulmalıdır.

6.2.9. Yönetim Onayı

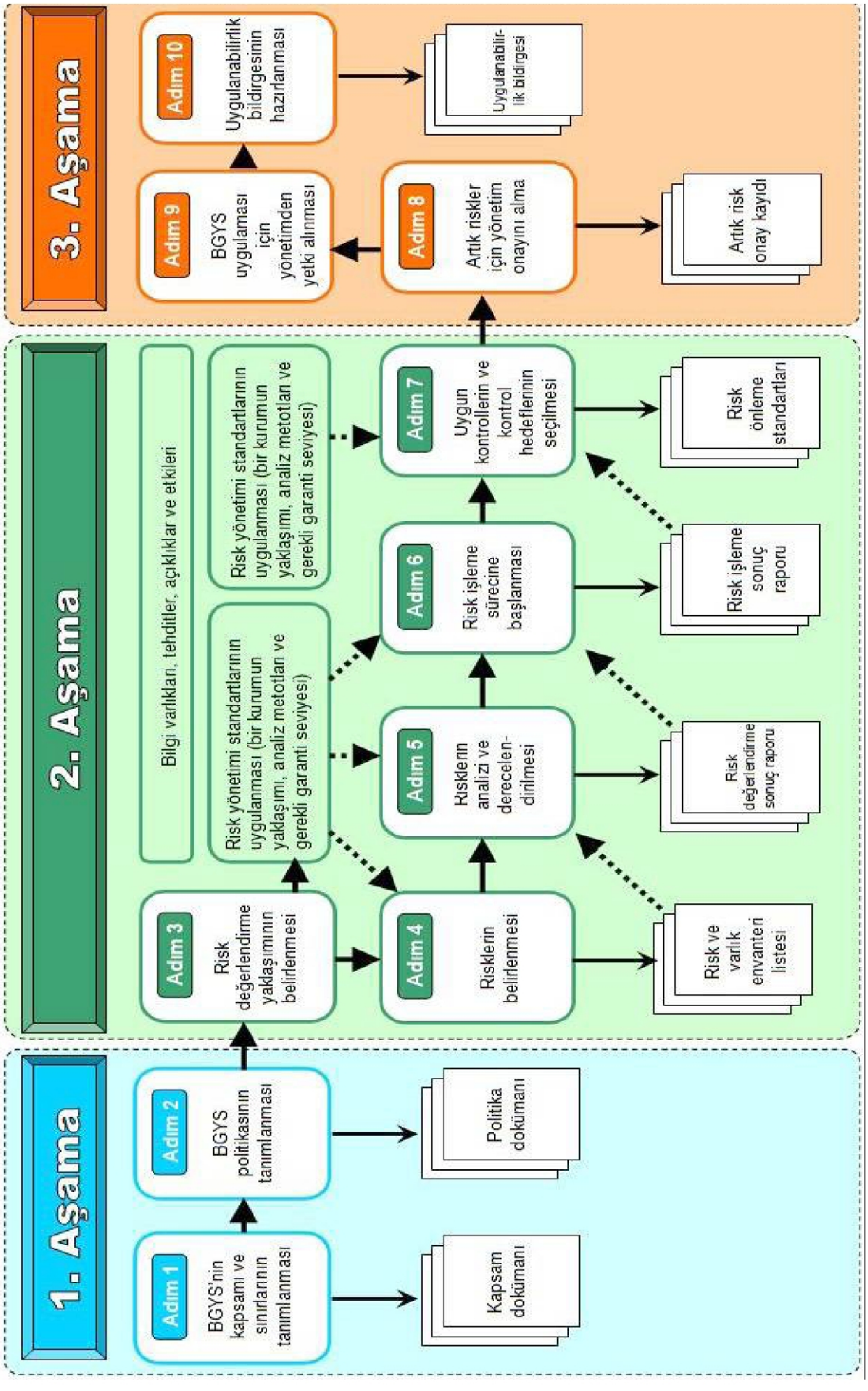
Risk yönetimi adımlarını geçtikten sonra BGYS işletimi ve uygulamasını yapmak için yönetimden onay almak gerekmektedir.

6.2.10. Uygulanabilirlik Bildirgesi

Son olarak risklere karşı seçilen kontrolleri içeren bir Uygulanabilirlik Bildirgesi hazırlanarak BGYS kurulum işi tamamlanır. Uygulanabilirlik Bildirgesi Adım 7'de seçilen kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatmalıdır. TS ISO/IEC 27001'den seçilmeyen kontrollerin neler olduğu ile bunların seçilmeme gerekçeleri de Uygulanabilirlik Bildirgesinde verilmelidir. Ayrıca mevcut durumda uygulanmakta olan kontroller de yine bu belge içinde yer bulmalıdır.

Bir sonraki sayfada şekil 6.2'de BGYS kurulum adımları özetlenmektedir.

Şekil 6.2: BGYS kurulum adımları



Kaynak: (Önel ve Dinçkan, 2007, s:14)

BGYS, günümüz iş dünyasında vazgeçilmez hale gelen bilgi güvenliği konusunda tüm dünya tarafından kabul görmüş standartlara uygun bir yapı sunmaktadır. BGYS kavramının ve bağlı olduğu standartların doğru anlaşılması bu yapının sağlayacağı faydayı önemli ölçüde arttıracaktır. BGYS kurulumunu fazladan bir iş yükü ve gereksiz zaman kaybı olarak görmenin baştan kaybetmek anlamına geleceği bilinmelidir. Bu sistemin vaat ettiklerine ulaşmak için yönetimlere büyük görev ve sorumluluklar düşmektedir.

7. BİLGİ TEKNOLOJİLERİ İÇİN KONTROL HEDEFLERİ (COBIT) NEDİR?

Bilgi Teknolojileri İçin Kontrol Hedefleri, Control Objectives For Information and Related Technology kelimelerinden oluşmakta olup, COBIT olarak ifade edilir. ISACA ve ITGI tarafından 1992 yılında geliştirilmiş, BT yönetimi için en iyi uygulamalar kümesidir. Bilgi Teknolojileri İçin Kontrol Hedefleri; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA, GAO tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir. Bir şirkette teknolojinin kullanımından ve BT yönetişimi ile kontrol geliştirmekten türeyen faydayı en üst düzeye çıkarmaya yardım etmesi için yöneticilere, denetçilere ve BT kullanıcılarına genel olarak kabul görmüş ölçüler, göstergeler, süreçler ve en iyi uygulamalar sağlar.

Bilgi Teknolojileri İçin Kontrol Hedefleri'nin vizyonu; bilişim teknolojileri yönetişim (IT Governance) modeli olmaktır. Bilgi Teknolojileri İçin Kontrol Hedefleri sadece bir denetim aracı değil, aynı zamanda bir yönetişim aracı olma amacını taşır. Bu nedenle yönetimden bilişim teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlama amacını da yerine getirmeyi hedeflemektedir.

Organizasyonların iş hedeflerini ve gereksinimlerini karşılayacak bilgilerin üretimi ve aktarımının hızlı, sürekli ve güvenli olarak sağlanabilmesi için teknoloji kullanımından kaynaklanan risklerin belirlenmesi, yönetimi ve kontrolünün etkin ve verimli olarak yapılması gerekmektedir. Kısaca "Teknoloji risklerini nasıl

yöneteceğiz ve bağlı oldukları yapıyı daha güvenli hale nasıl getireceğiz?" sorularının yanıtları, sadece bilgi işlem yöneticileri değil, teknoloji yoğun çalışan ve iş süreçlerine teknolojiyi entegre etmiş olan tüm kurumların yöneticileri için önem taşımaktadır.

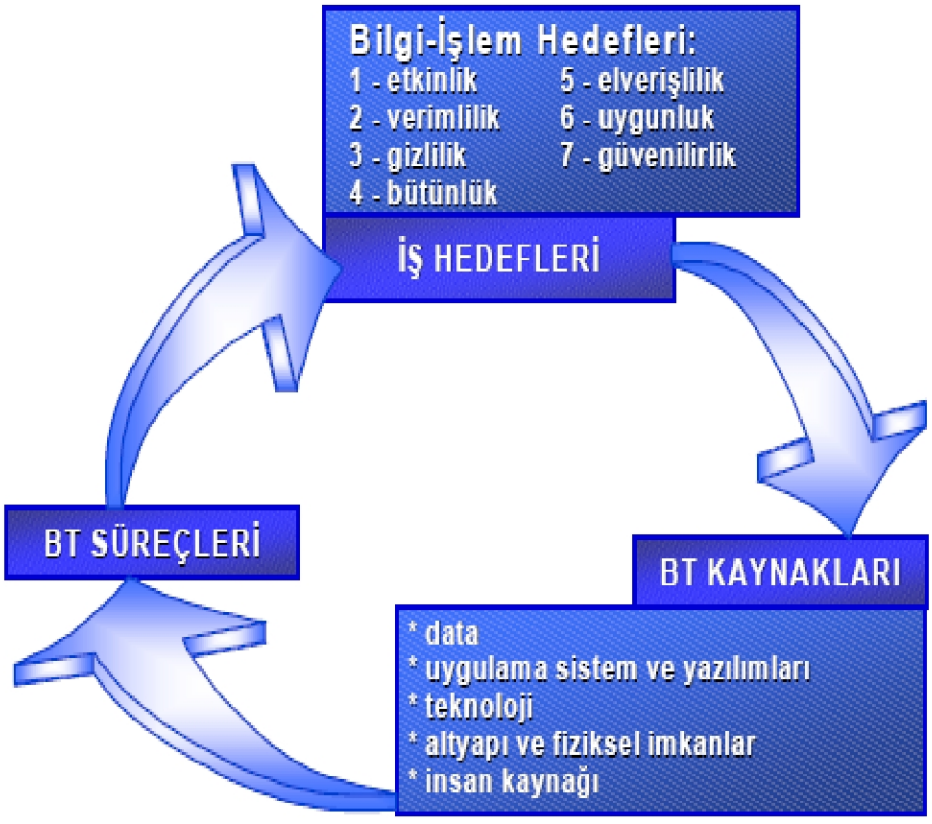
7.1. Bilgi Teknolojileri İçin Kontrol Hedeflerinin (COBIT) Tarihçesi

Bilgi Teknolojileri İçin Kontrol Hedefleri' in ilk sürümü 1996 yılında yayımlandı. Amacı; iş yöneticileri ve denetçilerinin günlük kullanımı için geçerli, güncel, uluslararası kabul görmüş BT amaçlarını araştırmak, geliştirmek, teşvik etmekti. "Yönetim Rehberi", 1998'de yayınlanan 2. sürüme eklendi. 2000 yılında 3. sürüm yayınlandı. 2003 yılında bilgisayar bağlantılı versiyonu kullanılır duruma geldi. 2005 yılının aralık ayında 4. basım ilk olarak yayınlandı. 2007 yılının mayıs ayında, şu anda kullanılan 4,1 sürümü yayınlandı.

7.2. Bilgi Teknolojileri İçin Kontrol Hedeflerinin (COBIT) Prensibi

Bilgi Teknolojileri İçin Kontrol Hedefleri, bu sorulara sistematik bir yaklaşım sergileyerek ve yönetsel ihtiyaçlara da yanıt verecek şekilde oluşturulmuş bir yöntemdir. Şekil 7.1'de iş hedefleri'nin bilgi işlem hedefleri'ne dönüşümü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirir. (Artinyan, 2008, s:1)

Şekil 7.1: BT süreçleri, bilgi işlem hedefleri, BT kaynakları döngüsü



Kaynak: Artinyan, 2008, s:1

Bilgi Teknolojileri İçin Kontrol Hedefleri aynı zamanda bilgi teknolojilerinin maruz kaldıkları riskleri, bu risklerin değerlemesi ve ortadan kaldırılmasına yönelik kontrolleri ve bu kontrollerin denetlenme yöntemlerini de ele alan bir bakış açısı ile oluşturulmuş bir mimariye sahiptir. Bilgi Teknolojileri İçin Kontrol Hedefleri, IT Governance Institute tarafından ortaya koyulmuştur ve teknolojinin hızlı değişimi doğrultusunda güncel tutulmaktadır. 1996'da ilk kez yayınlanan Bilgi Teknolojileri İçin Kontrol Hedefleri, güncellenerek 1998'da 2. 2000 yılında 3. ve son olarak da 4. versiyonuna ulaşmış olan bir standarttır. Bilgi Teknolojileri İçin Kontrol Hedefleri'nin jenerik bir model olarak herhangi bir kurumda yer alabilecek tüm teknoloji süreçlerini kapsayan yapısı içerisinde, gruplanmış 4 süreç alanı ve 34 tane temel Bilgi Teknolojisi süreci yer almaktadır.

7.3. Bilgi Teknolojileri İçin Kontrol Hedefleri (COBIT) Unsurları

Bilgi Teknolojileri İçin Kontrol Hedefleri beş unsurdan oluşan bir modeldir.

Bunlar;

- Yönetici özeti
- Çerçeve
- Kontrol amaçları
- Denetim ilkeleri
- Yönetim ilkeleri

Yönetici özeti, Bilgi Teknolojileri İçin Kontrol Hedefleri'nin amaçlarını ve süreçlerini özetler.

Çerçeve, denetçiler, yöneticiler, işletme ve iş süreç sahipleri için kapsamlı rehberlik sağlar.

Kontrol amaçları, sürecin uygulanmasını kolaylaştırmak için üst düzey yönetici ihtiyaçlarını tanımlar.

Denetim ilkeleri, kapsamlı kontrol değerlendirmesi için gerekli bilgilerin elde edilmesi, değerlendirilmesi amacıyla oluşturulan bir modeldir.

Yönetim ilkeleri, yöneticinin aşağıdaki soruları yanıtlamasını sağlamak için, faaliyete yönelik ilkelerdir:

1. Fayda maliyetten fazla mı?
2. İyi bir performansın göstergeleri nelerdir?
3. Kritik başarı faktörleri nelerdir?
4. Amaçları gerçekleştirememenin riskleri nelerdir?
5. Diğerleri ne yapıyor?
6. Nasıl karşılaştırma ve değerlendirme yapabiliriz?

7.4. Bilgi Teknolojileri İçin Kontrol Hedeflerinin (COBIT) Çerçevesi

Bilgi Teknolojileri İçin Kontrol Hedefleri unsurlarından çerçeve, bir iş süreç akım şeması olarak şekil 7.2'de gösterilmiştir. Organizasyonun elindeki kaynaklardan elde ettiği mevcut bilgilerden iş süreçleri sonucunda ihtiyaç duyulan

bilgilerin elde edilmesini sağlayan bir yapıdır. Bilgi Teknolojileri İçin Kontrol Hedefleri'nin çerçevesi; işletme odaklı, süreç yönelimli, kontrol esaslı ve ölçmeye dayalı olarak düzenlenmiştir. Bilgi Teknolojileri İçin Kontrol Hedefleri çerçevesi, işletmenin hedeflerini gerçekleştirmesi için gerekli bilgiyi sağlamak, kuruluşların gerekli bilgi hizmetlerini sunması için yapısal süreçlerde kullanılan bilgi teknolojisi kaynaklarını yönetmek ve kontrol etmek esaslıdır.

Bilgi Teknolojileri İçin Kontrol Hedefleri'nin çerçevesi üç unsurdan oluşur. Bunlar;

Bilgi için işletme gereksinimleri
Bilgi teknolojisi kaynakları
Bilgi teknolojisi süreçleridir.

İşletmenin hedeflerini gerçekleştirmesi için bilginin Bilgi Teknolojileri İçin Kontrol Hedefleri'nin kullandığı kontrol kriterlerine uyumlu olması gerekir. Bilgi kriterleri etkililik, verimlilik, gizlilik, bütünlük, kullanırlık, uyum ve güvenirliktir.

Bilgi teknolojisi kaynakları bilgi, uygulama sistemleri, teknoloji, olanaklar ve insanlardır. Bilgi teknolojisi süreçleri planlama ve organizasyon, kazanım ve uygulama, teslim ve destekleme, izleme olmak üzere dört alandan oluşur. Bu alanlar, bilgi teknolojisi geleneksel sorumluluk alanları olan planlama, yapılanma, işleme, izleme ile eşleşir.

Planlama ve organizasyon süreci strateji ve taktikleri içerir, bilgi teknolojisinin iş hedeflerini gerçekleştirmesi adına en iyi katkıyı sağlamasının yollarını belirtir. Planlama ve organizasyon süreci; bilgi teknolojisi için stratejiler ve taktiksel planlar oluşturma, bilgi teknolojisinin iş hedeflerini en iyi şekilde gerçekleştirmesini sağlayacak yolları tanımlama, stratejik vizyonun gerçekleştirilmesini sağlama, planlama, bildirme, bilgi teknolojisi organizasyonunu kurma, bilgi yönetimi ve teknoloji altyapısı için alan oluşturma faaliyetlerinden oluşmaktadır.

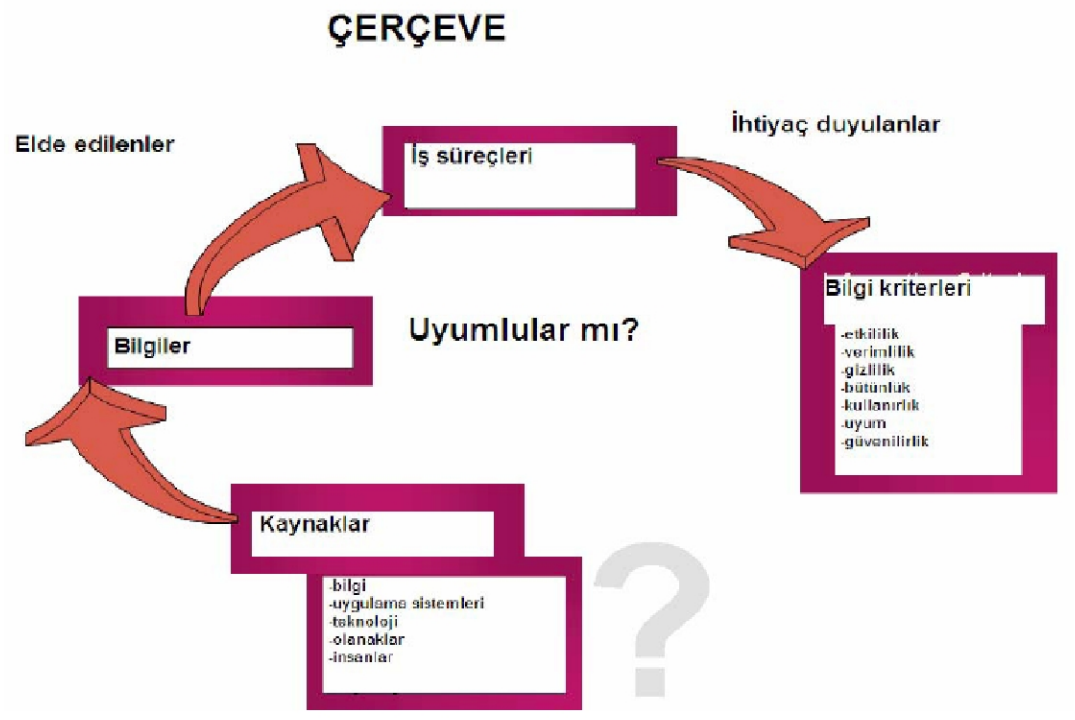
Kazanım ve uygulama süreci; tanımlanan, geliştirilen, uygulanan, iş sürecine adapte edilen bilgi teknolojisi çözümleri, var olan sistemlerin değiştirilmesi ve sürdürülmesi faaliyetlerinden oluşmaktadır.

Teslim ve destekleme süreci; gerekli hizmetlerin yerine getirilmesi, hizmetlerin güvenliğinin ve devamlılığının sağlanması, eğitim ve stajı içeren destekleme sürecinin oluşturulması, uygulama kontrollerini içeren bilgi süreci faaliyetlerden oluşmaktadır.

İzleme süreci; bütün bilgi teknolojisi süreçlerinin, kaliteleri ve kontrol gereksinimlerine uyumu açısından düzenli olarak gözden geçirilmesi faaliyetlerini gerektirmektedir. Bilgi teknolojisi sürecin kalitesi, kontrollerin uygunluğu, kontrol gereksinimlerine uyumunu düzenli olarak değerlendirilmesi, denetim fonksiyonunu gerçekleştirme faaliyetlerinden oluşmaktadır.

Bilgi Teknolojileri İçin Kontrol Hedefleri içerisinde 34 kontrol amacı ve 318 ayrıntılı kontrol amacı yer almaktadır. (Uzunay, 2007, s:7)

Şekil 7.2: Bilgi Teknolojileri İçin Kontrol Hedefleri çerçevesi



Kaynak: Uzunay, 2007, s:7

7.5. Bilgi Teknolojileri İçin Kontrol Hedeflerinin (COBIT) Yapısı

Bilgi Teknolojileri İçin Kontrol Hedefleri şekil 7.3'de gösterildiği gibi dört süreç alanında gruplanmış 34 BT sürecini ele alır.

Bu dört grup;

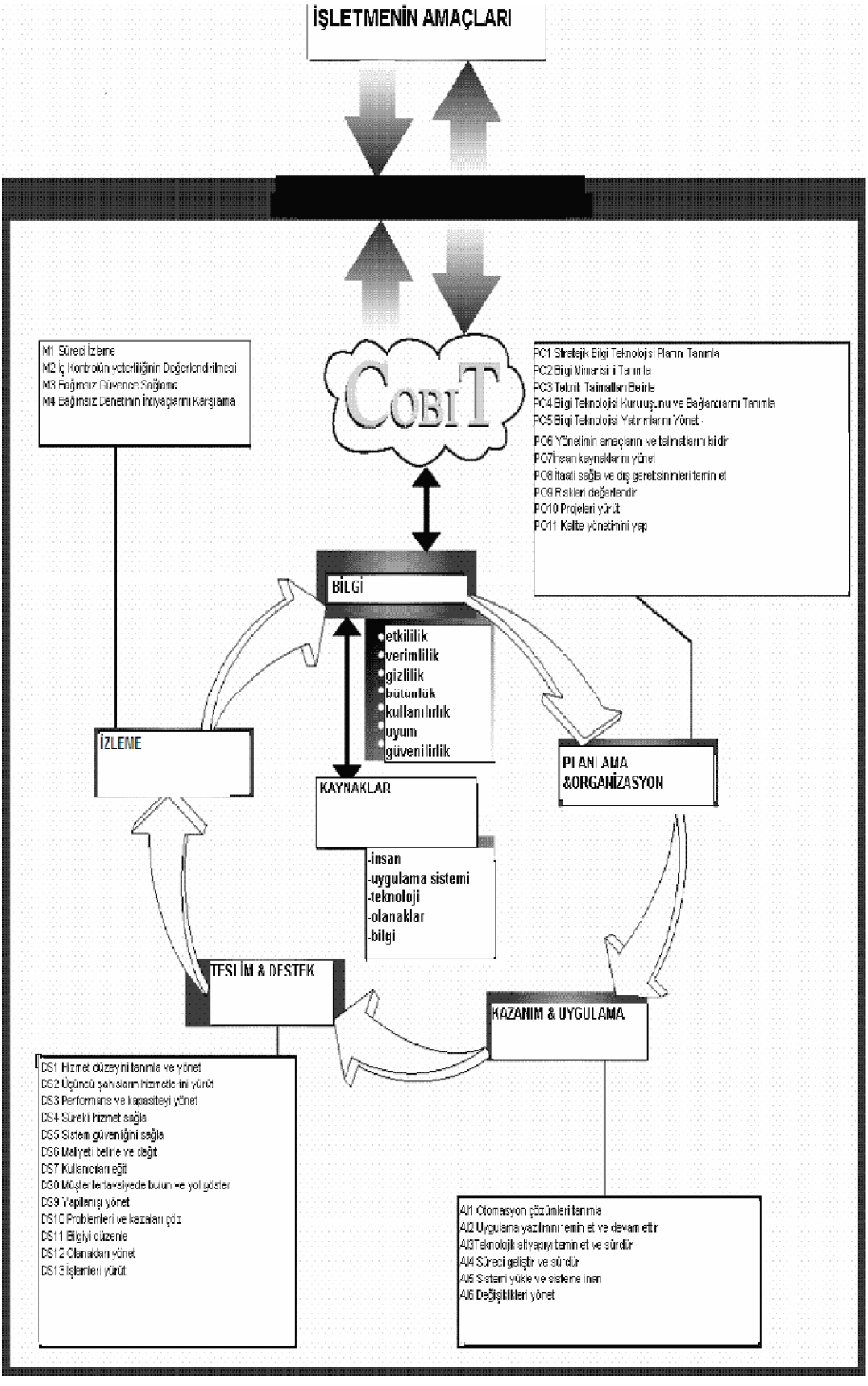
1) Planla ve Organize Et
2) Tedarik ve Uygulama
3) Teslimat ve Destek
4) İzle ve Değerlendir

Her bir sürecin 0-5 arası bir olgunluk seviyesi vardır. (0 yok, 5 optimize edilmiş) Bu ölçek, bir organizasyondaki sürecin olgunluk seviyesi, o sürecin hangi olgunluk seviyesinde olması gerektiği, hangi seviyenin en iyi uygulama olarak varsayıldığı ve diğer organizasyonların ne seviyede olduğu gibi anahtar değerlendirmeler için kullanılır.

Bilgi teknolojilerinin iş hayatındaki önemi arttıkça, oldukça yüklü yatırım ve riskli proje yönetimlerini gerektiren bilgi teknolojileri süreçlerinin olgunluk seviyeleri hakkında güvence sağlayacak denetim metodolojilerine olan ihtiyaç da artmaktadır. Bu amaçla Bilgi Teknolojileri İçin Kontrol Hedefleri için düzenlenmiş olan olgunluk seviyeleri kurumun bugün nerede olduğunu, endüstrideki durum ve karşılaştırmalarını ve kurumun ileride nerede olmak istediği sorularına cevap vermektedir.

Son zamanlarda Bilgi Teknolojileri İçin Kontrol Hedefleri olgunluk seviyeleri hakkında bir sürü spekülasyonun ortaya atılması Bilgi Teknolojileri İçin Kontrol Hedefleri 4,1' in ortaya çıkması ile durmuştur.

Şekil 7.3: Bilgi Teknolojileri İçin Kontrol Hedefleri yapısı



Kaynak: Uzunay, 2007, s:9

Ana hatları ile Bilgi Teknolojileri İçin Kontrol Hedefleri olgunluk modellerinin hesaplaması şu şekildedir:

Bilgi Teknolojileri İçin Kontrol Hedefleri Olgunluk Modelleri; (TDB Kamu-BİB, 2008, s:11)

0.Olmayan	Tanımlanmış süreç bulunmamaktadır.
1.Başlangıç	Organize olmayan ve standartlaşmamış fakat kurumda farkındalığın mevcut olduğu ve adresleme ve standartlaştırma ihtiyacının tespit edildiği seviyedir.
2.Tekrarlanan	Bireye dayalı ve tekrarlanan işleri farklı kişilerin aynı şekilde yapabildiği seviyedir. Bu seviyede formal eğitim ve iletişim metodları belirlenmemiş fakat sorumluluk büyük oranda kişiye bağlı kılınmıştır.
3.Tanımlı	Prosedürler standartlaşmış ve dokümante edilmiş, eğitim aracılığı ile kurum içinde iletilmiştir. Ancak bu süreçleri izleyip izlememe kararı kişinin kendisine bırakılmıştır; bu nedenle yapılan işler arasında çeşitli farklılıklar mevcuttur. Prosedürlerin kendisi gelişmiş değildir; ancak mevcut uygulamaların biçimselleştirilmiş halidir.
4.Yönetilen	Prosedürlerle uyumu izlemek ve ölçmek, süreçlerin etkin çalışmadığının anlaşılması durumunda faaliyete geçmek mümkündür. Süreçler sürekli gelişmekte ve iyi uygulamaların tanımlanması sağlanmaktadır. Otomasyon ve araçlar kısıtlı veya parçalı bir biçimde kullanılabilmektedir.
5.Optimize	Süreçler en iyi uygulamalar seviyesine indirgenmiş, sürekli gelişim ve olgunluk modelleme konusunda diğer şirketlerin sonuçları ile çalışmaktadır. BT, iş akışlarının otomatize edilmesi, kalite ve etkinliğin artırılması ve kurumun çabuk adapte olabilmesi için entegre olmuştur.

7.5.1. Planla ve Organize Et

Planla ve Organize Et Süreç Alanı, bir şirketin amaçlarına ve hedeflerine ulaşması için bilgi ve teknolojilerin nasıl kullanılacağını kapsar. BT' nin kullanımından en iyi sonuçları alarak fayda sağlamak için BT' nin organizasyonel ve altyapısal şekline işaret eder. Planla ve Organize Et Süreç Alanına ait üst seviye kontrol hedefleri Tablo 7.1'de listelenmiştir.

.

Tablo 7.1: Planla ve Organize Et Süreç Alanına Ait Üst Seviye Kontrol Hedefleri

PO	Planla ve Organize Et
PO1	Stratejik BT Planının Tanımlanması
PO2	Bilgi Mimarisinin Tanımlanması
PO3	Teknolojik Yönün Belirlenmesi
PO4	BT Organizasyon ve İlişkilerinin Tanımlanması
PO5	BT Yatırımlarının Yönetimi
PO6	Yönetimin Hedeflerinin ve Talimatlarının İletilmesi
PO7	Kalite Yönetimi
PO8	İnsan Kaynakları Yönetimi
PO9	Risk Değerlendirme
PO10	Proje Yönetimi

Kaynak: TDB Kamu-BİB, 2008, s:12

7.5.2. Tedarik ve Uygulama

Tedarik ve Gerçekleştirme Süreç Alanı, BT gereksinimlerini belirlemeyi, teknolojiyi tedarik etmeyi ve şirketin mevcut iş süreçleri içinde uygulamayı kapsar. Bu süreç alanı ayrıca, şirketin BT sistemi ve bileşenlerinin ömrünü uzatmak için bir bakım planı oluşturmayı adresler. Tedarik ve Uygulama Süreç Alanına ait üst seviye kontrol hedefleri Tablo 7.2'de listelenmiştir.

Tablo 7.2: Tedarik ve Uygulama Süreç Alanına Üst Seviye Kontrol Hedefleri

AI	Tedarik ve Uygulama
AI1	Otomasyon Çözümlerinin Belirlenmesi
AI2	Uygulama Yazılımı Tedarik Edilmesi ve Bakımı
AI3	Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı
AI4	ĠĞ ve Kullanımın Etkin Kılınması
AI5	BT Kaynaklarının Sağlanması
AI6	Değişiklik Yönetimi
AI7	Çözüm ve Değişikliklerin Kurulması ve Kabul Edilmesi

Kaynak: TDB Kamu-BİB, 2008, s:13

7.5.3. Teslimat ve Destek

Teslimat ve Destek Süreç Alanı, BT' nin teslimat durumlarına odaklanır. Uygulamaların BT sistemi içinde yürütülmesi ve sonuçlarıyla olduğu kadar, BT sistemlerinin etkili ve yeterli işletilmesine olanak sağlayan destek süreçlerini de kapsar. Destek süreçleri; güvenlik konuları ve eğitimi içerir. Teslimat ve Destek Süreç Alanına ait üst seviye kontrol hedefleri Tablo 7.3'de listelenmiştir.

Tablo 7.3: Teslimat ve Destek Süreç Alanına Üst Seviye Kontrol Hedefleri

DS	Teslimat ve Destek
DS1	Hizmet Düzeyi Belirleme ve Yönetimi
DS2	Üçüncü Parti Hizmet Yönetimi
DS3	Performans ve Kapasite Yönetimi
DS4	Sürekli Hizmetin Sağlanması
DS5	Sistem Güvenliğinin Sağlanması
DS6	Harcamaların Belirlenmesi ve Bütçelenmesi
DS7	Kullanıcı Eğitimi
DS8	Kullanıcılara Yardım ve Danışmanlık
DS9	Konfigürasyon Yönetimi
DS10	Problem ve Olay Yönetimi
DS11	Veri Yönetimi
DS12	Fiziksel Çevre Yönetimi
DS13	Operasyon Yönetimi

Kaynak: TDB Kamu-BİB, 2008, s:14

7.5.4. İzle ve Değerlendir

İzle ve Değerlendir Süreç Alanı, şirket ihtiyaçlarının tayin edilmesiyle ilgili şirket stratejilerinin belirlenmesi ve mevcut BT sisteminin tasarlanırken niyetlenildiği ihtiyaçları karşılayıp karşılamadığı ile ilgilenir. Bu Süreç Alanı ayrıca BT sisteminin iş amaçları ve şirketin kontrol süreçlerinin iç ve dış denetçiler tarafından etkinliğinin değerlendirilmesini de kapsar. İzle ve Değerlendir Süreç Alanına ait üst seviye kontrol hedefleri Tablo 7.4'de listelenmiştir.

Tablo 2.4: İzle ve Değerlendir Süreç Alanına Üst Seviye Kontrol Hedefleri

ME	İzle ve Değerlendir
ME1	Süreç İzleme
ME2	İç Kontrol Değerlendirme Yeterliliği
ME3	Bağımsız Güvence Elde Edilmesi
ME4	Bağımsız Denetimin Sağlanması

Kaynak: TDB Kamu-BİB, 2008, s:15

Bilgi Teknolojileri İçin Kontrol Hedefleri'nin 4 temel süreç alanının altında toplam 34 adet BT süreci bulunmaktadır. Bu BT süreçleri 318 adet detaylı kontrol amacı içermektedir. Bilgi Teknolojileri İçin Kontrol Hedefleri, BT süreçlerini aşağıdaki bilgi kriterleri ve bilgi kaynakları ile ilişkilendirilir.

Tablo 7.5: Bilgi Kriterleri

Etkililik	Bilginin iş süreçleri ihtiyaçları ile ilgili ve bu ihtiyaçlara cevap verir nitelikte olması.
Verimlilik	Bilgi kaynakların en etkin kullanımı ile elde edilmesi.
Gizlilik	Hassas bilginin yetkisiz erişime karşı korunması
Bütünlük	Bilginin kendi içinde ve çevresel veriler ile bütünlük göstermesi, yetkisiz değişikliğinin engellenmesi.
Devamlılık	Bilginin ihtiyaç duyulduğunda erişilebilir olması.
Uyumluluk	İş süreçlerinde kanun, düzenleme ve kontratlara uyumun sağlanması.
Güvenilirlilik	Yönetimin finansal ve diğer raporlamalar için güvenilir veriye ulaşabilmesi.

Kaynak: TDB Kamu-BİB, 2008, s:15

Tablo 7.6: Bilgi kaynakları

İnsan Kaynakları	BT personel yetenekleri, bilinç, bilgi sistemleri planlama, organizasyon, uygulama, destek, gözetim üretkenliği.
Uygulama Sistemleri	Manuel ve programlanmış iş süreçlerinin tümü.
Teknoloji	Donanım, işletim sistemi, veritabanı yönetim sistemi, bilgi ağı ve diğer teknoloji altyapısı.
Fiziksel Ortam	Bilgi sistemlerini barındıran ve koruyan fiziksel ortamlar.
Veri	En geniş anlamıyla, iç, dış veri türlerinin tamamı.

Kaynak: TDB Kamu-BİB, 2008, s:15

7.6. Hangi kurumlar Bilgi Teknolojileri İçin Kontrol Hedeflerini (COBIT) Uygulayabilirler?

Geçmiş 30 - 40 yıla bakıp hem Türkiye hem de Dünyadaki gelişimi incelediğimizde, BT' nin ilk ve en yaygın olarak finans sektöründe kendini gösterdiğinin farkına varıyoruz. Çünkü bu sektörler, hesaplama ve veri tutma gereksinimleri en yüksek olan sektörlerden biridir. Bilim, sağlık, eğitim, üretim, endüstri ve inşaat derken, buna kamu hizmetleri ve e-devlet de dâhil olmak üzere, artık en basit yapılan işlemlerde bile BT kullanılmaya başlandı. Bu nedenle günümüzde Bilgi Teknolojileri İçin Kontrol Hedefleri için şu veya bu sektörde uygulanmalı diye bir ayırım yapılamaz.

BT' nin kullanıldığı ve entegre olduğu her alanda bu yöntemin uygulanabilirliği mümkündür. BT' yi ülkemizde geniş çapta ilk kullananlar bankacılar olmuştur. Özellikle bilgisayarlarının bir network üzerinden birbirleriyle konuşmaları sonucunda; yaygın şubeli bankalarda provizyon alma ve havale gönderme gibi telefonla yapılan; güvenlik amacıyla sözel şifreler kullanılarak gerçekleştirilen zahmetli ve masraflı işlemler online hale gelmiştir. Finans sektörü; paranın döndüğü sektördür ve tehditlere, saldırılara, zimmet, sahtecilik, soygun ve dolandırıcılık yapılmaya en çok maruz kalan, bu nedenle de en çok kontrol altında

tutulması gereken sektördür. Mali bilgiler işlenmekte, paranın söz konusu olduğu süreçler işletilmektedir. Dolaylısıyla da Bilgi Teknolojileri İçin Kontrol Hedefleri, ilk olarak ülkemizde ve dünya genelinde ağırlıklı olarak finans sektöründe kullanılmaya başlamıştır. Diğer sektörler de finans sektöründeki pratikleri kendi sektörlerine adapte etmişlerdir. Büyüklük ve küçüklük ayrımına gelirsek; 10 kişilik bir şirketin, biz Bilgi Teknolojileri İçin Kontrol Hedefleri'ni uygulayacağız diye normal işini yapmaması gibi bir lükse sahip değildir. Zorunlu ve zorunlu olmayan sektörler olarak bakılırsa, Finans sektörü, özellikle İmar Bankası olayından sonra Türkiye'de tüm bankaların Bilgi Teknolojileri İçin Kontrol Hedefleri denetiminden geçmesini şart hale getirmiş durumdadır. Ne fayda sağlayacağı konusunda çok kısa olarak şunu söyleyebilirim; planlı, hedeflerini ortaya koymuş, şeffaf, tutarlı, yasal gereksinimlere uyumlu, risklerin yönetildiği, fayda / maliyet esaslarına riayet edilerek değer yaratma üzerine kurulu ve iplerin yönetimin elinde kontrollü olarak yer aldığı ve yetki & görevler ayrılığı ilkesine uyum sağlayan bir yapı ortaya koyulmuş olur.

7.7. Bilgi Teknolojileri İçin Kontrol Hedefleri'nin (COBIT) Sağladığı Faydalar

7.7.1. Bilgi Teknolojileri İçin Kontrol Hedefleri'nin (COBIT) yönetime ve bilişim teknolojileri yönlendirme komitesine sağladığı faydalar

- Kurum yönetiminin sorumluluğunda olan bilişim teknolojileri süreç kontrollerinin uygulanabilmesi için gerekli çatıyı sağlar.

- Bilişim teknolojileri ve iş süreçleri arasındaki ilişkiyi gözeterek öncelikli bilgi sistemleri kontrollerinin tespitinin daha etkin yapılabilmesini sağlar.

- BT yatırımlarının iş süreçlerine uygun olarak gerçekleştirilmesi ve risk/maliyet oranı yüksek projelere ağırlık verilebilmesi için alınacak kararlara ışık tutar.

- Bilişim teknolojileri süreçlerinin olgunluğunu sadece üretilen sonuçlar ile değil aynı zamanda performans belirteçleri ile de değerlendirilebilmesine imkân tanır.
- Bu sayede bilişim teknolojileri amaç belirteçlerinin yanı sıra performans belirteçlerinin de belirlenerek "IT Scorecard" ın ortaya konabilmesine ve yönetimin geleceğe yönelik daha kesin beklentilere sahip olabilmesine olanak sağlar.

7.7.2. Bilgi Teknoloji personeline sağladığı yararlar

- Bilgi Teknolojileri İçin Kontrol Hedeflerinden özellikle Planla ve Organize Et sahasında bulunanların uygulamaya alınması ile önceliklendirme süreci ve diğer birimlerle olan ilişkilerde iyileşme yaşanabilecek, verimlilik artışı sağlanabilecektir. Bu fayda tüm kurumu etkilemekle birlikte bilişim teknolojileri personeli tarafından daha fazla hissedilecektir.

- BT personeli bilişim teknolojileri denetiminin hangi kriterlere göre yapıldığını bilerek denetimin daha verimli gerçekleştirilmesine katkıda bulunabilir.

- BT personeli için bir rehberlik hizmeti sağlar. Böylece BT personeli kontrol sahasında bulunan süreçlerinin olgunluk seviyesini Bilgi Teknolojileri İçin Kontrol Hedeflerinde belirtilen kriterlere göre kendi insiyatifi ile yükseltebilir.

7.7.3. Bilişim teknolojileri denetçilerine sağladığı yararlar

- Bilgi Teknolojileri İçin Kontrol Hedefleri BT denetimi alanında çok sayıda uzmanın katkısı ile var olan diğer kriterlerin de dikkate alınarak hazırlandığı kabul görmüş bir metodolojidir. BT denetçileri tüm denetim konularında yaşanabilecek kapsam ve objektif kriter belirleme sorununu Bilgi Teknolojileri İçin Kontrol Hedefleri ile aşabilir.

- BT denetçileri denetim rehberinden faydalanarak tespit edilen risklerin doğurabileceği zararları somutlaştırabilir ve yönetime daha net bir bakış açısı kazandırabilir.

- Bilgi Teknolojileri İçin Kontrol Hedeflerinde her süreç için sunulan kritik başarı faktörlerinden yola çıkarak denetim sonuçlarını ölçümleyebilir ve iyileştirme önerileri getirebilir.

7.7.4. Bilişim teknolojileri kullanıcılarına sağladığı yararlar

- Bir kontrol metodolojisinin uygulanması iç ve dış kullanıcılara kullanılan bilgi kaynaklarının kontrollü olarak yönetildiğini ifade edecektir. Özellikle dış kullanıcılara sağladığı güvence zorunlu yükümlülüklerin yerine getirilmesine imkân tanıyabileceği gibi kurum için bir rekabet avantajı haline de dönüşebilir.

- Süreçlerin kontrollü olarak yürütülmesi, kullanıcıların gizlilik, bütünlük ve erişilebilirlik ihtiyaçlarının beklenen ve daha üstü düzeylerde sağlanmasına olanak sağlar.(TDB Kamu-BİB, 2008, s:17)

8. SONUÇ VE ÖNERİLER

Bu çalışmada, kurumsal bilgi güvenliğinin sağlanmasında önemli olan unsurlar gözden geçirilmiştir. Yüksek seviyede kurumsal bilgi güvenliği sağlanabilmesi için bilgi güvenliği standartlarının bilinmesi ve uygulanmasının yanında güncel tehditlerin bilinmesi önemlidir. Yüksek seviyede bir kurumsal bilgi güvenliği sağlanabilmesi için teknoloji-insan-eğitim üçgeninde yönetilen bir yaklaşımın dikkate alınması gerektiği tespit edilmiştir. Yapılan diğer tespitler aşağıda sunulmuştur.

• Ülkemizde genellikle güvenlik politikaları standartlara uygun olmadan yazılı veya sözlü, onaylı veya onaysız bir biçimde kuruluşlar tarafından uygulanmakta ve çoğu kurum tarafından da "Bilgi Güvenliği Yönetimi" yeterli görülmektedir. Bu yanlış anlamanın giderilmesi için dünya genelinde kabul görmüş ve uygulanabilirliği test edilmiş bilgi güvenliği standartları esas alınarak kuruluşların "Bilgi Güvenliği Yönetimi" konusunda eksikliklerini gidererek BGYS kurmaları, uygulamaları ve belgelendirilmeleri gerekmektedir. BGYS çerçevesinde oluşturulacak güvenlik politikalarına, üst yönetim ve tüm çalışanların destek vermesi ve tavizsiz bir şekilde uygulanması, işbirliğinde bulunulan tüm kişi ve kuruluşlarında bu politikalara uyma zorunluluğu, kurumsal bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir faktördür.

• BGYS standartlarının kurumlara uyarlanması, anlatılması, kullanıcı, teknik çalışanların ve yöneticilerin eğitilmesi konusunda kuruluşların bünyelerinde güvenlik uzmanları çalıştırmaları veya danışmanlık hizmetleri almaları gerekmektedir. BGYS uygulamaları, kurumlar tarafından başarılı bir şekilde uygulandıktan sonra kuruluşların bilgi güvenliğini yönettiklerine dair uluslararası alanda geçerli sertifikasyona sahip olmaları önemlidir.

• Bilgi güvenliğinin yönetilmesi bilgi güvenliğinin sağlandığı anlamına gelmemektedir. BGYS' nin kurumsal bilgi güvenliğini taahhüt ettiği seviyede sağlayıp sağlamadığı, sağlamıyorsa 'eksikliklerinin neler olduğu, güvenlik denetimlerinin güvenli biçimde kurulup kurulmadığı, güvenlik denetimlerinin etkin ve politikalara uygun olarak uygulanıp uygulanmadığı, iyi bir belgelendirme yapılıp yapılmadığı gibi bilgi güvenliğinin sağlanması açısından çok kritik olan soruları cevaplamanın tek yolu BGYS kapsamında belirlenen bilgi varlıklarının (insan faktörü, yazılımlar, donanımlar, ortamlar, vb.) güvenliğini "sızma testleriyle" test etmekten geçmektedir. Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında sızma testlerinin katkısı çok yüksektir. Sızma testleri felaket başa gelmeden önce, onu önleyecek ve ona karşı savunulacak ihtiyaçların ve tedbirlerin alınmasında kullanılan önemli bir erken uyarı sistemidir. Bu önemden dolayı, sızma testleri belirli periyotlarda (bu yılda en az 2-3 kez olabilir) veya sistem yenilenmelerinde yapılmalı ve kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasındaki rolü her zaman dikkate alınmalıdır. Yukarıda anlatılan hususların yanında, yüksek seviyede

kurumsal bilgi güvenliğinin sağlanmasında aşağıdaki hususlara da dikkat edilmesi önerilmektedir.

Bunlar:

• Kurumsal bilgi güvenliğini sağlamanın dinamik bir süreç olduğu ve süreklilik arz ettiği,

• Kurumsal bilgi güvenliğinin sadece teknolojiyle sağlanır yaklaşımından uzaklaşılarak insan-eğitim teknoloji üçgeninde yeni bir yaklaşımla sağlanması gerektiği,

• Uluslararası standartlara uygun olarak yapılması ve uygulanması gerektiği,

• Standartlar yüksek seviyede bir güvenliği garanti etse de bazen standartlarında yetersiz kalabileceği,

• Kurumsal bilgi güvenliği seviyesinin güncel durumunun belirlenmesi amacıyla iç ve dış ortamlardan zaman zaman bağımsız uzman kuruluşlar tarafından denetlenmesi gerektiği,

• Kurumsal bilgi güvenliğinin yönetilmesinin zorunlu bir süreç olduğu ve her zaman iyileştirmelere ihtiyaç duyulduğu ve

• En zayıf halka kadar güvende olunacağı varsayımıyla hareket edilerek gerekli önlemlerin alınması gerektiği bilinmeli ve uygulanmalıdır.

9. KAYNAKÇA

ARTİNYAN, E. Natasa , "Kurumsal Risk Hizmetleri", Deloitte, 2008

British Standards Institute, "Information Technology — Security Techniques — Code of Practice for Information Security Management",BSI BS 7799-1:2005, Bristol, 2005.

BSI Eurasia 1,"BSI Belgelendirme Yöntemi" http://www.bsiturkey.com/BilgiGuvenligi/ISMStescil/BSItescilyontemi.xalter?print_only=1, 24.01.2008.

BSI Eurasia 2, "Bilgi Güvenliği Yönetim Sisteminin Belgelendirilmesi" http://www.bsiturkey.com/BilgiGuvenligi/ISMStescil/index.xalter, 24.01.2008.

HANSCHE, Susan, "Official (ISC2) Guide to the CISSP Exam", Auerbach Publication, 2003

ISO - International Organization for Standardization "JTC 1 / SC 27" http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=143, 09.07.2007.

ISO 27001 Security, "ISO/IEC-17799&ISO/IEC-27002" http://www.iso27001security.com/html/iso17799.html, 09.07.2007

ITGI (Information Technologies Governance Institude – Bilgi Teknolojileri Yönetim Enstitüsü), PriceWaterhouseCoopers-ITGI, 2006

KARABACAK, Bilge, "Türkiye'de Bilişim Güvenliğiyle İlgili Yasal Altyapının Analizi", TÜBİTAK-UEKAE, 29.06.2009

KOVACICH, Gerald L. "The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program, 2003

OSBORNE, M."How to Cheat at Managing Information Security", Syngress Publishing Inc. Rockland, 2006

ÖNEL Dinçer ve DİNÇKAN Ali ; "Bilgi Güvenliği Yönetim Sistemi Kurulumu" TÜBİTAK ÜEKAE Doküman kodu: BGYS 0001, Kocaeli, 28.08.2007

ŞAHİNASLAN, Ender, KANTÜRK, Arzu, ŞAHİNASLAN Önder ve BORANDAĞ Emin, "Kurumlarda Bilgi Güvenliği Farkındalığının Önemi ve Oluşturma Yöntemleri", 2009

TBD Kamu-BİB, "Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri", Kamu Bilişim Platformu, Sürüm 1.0, 16.04.2008

Türk Standartları Enstitüsü, "Bilgi Teknolojisi–Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler", TSE- TS ISO/IEC 27001, Ankara, 2006.

Türkiye Bilişim Derneği, "E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları 4. Çalışma Grubu Sonuç Raporu",TBD Kamu-BİB IV, Ankara, 2005.

UZUNAY, Vildan, "COBIT (Control Objectives for Information and Related Technology)", İç Kontrol Merkezi Uyumlaştırma Dairesi Ankara, 2007

ÜVEY, M. Cüneyt, "Orkestra şefiniz: COBIT, Röportaj", 2009

VURAL, Yılmaz ve SAĞIROĞLU, Şeref, "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme",Gazi Üniv. Müh. Mim. Fak. Der. Cilt 23, No 2, 2008

YILDIZ, Bünyamin. ; "Bilgi güvenliği ve e-devlet kapsamında kamu kurumlarında bilgi güvenliği yönetimi ve standartların uygulanması", Yüksek Lisans Tezi, Gebze Yüksek teknoloji Enstitüsü, Gebze, 2007

10. ÖZGEÇMİŞ

İLETİŞİM BİLGİLERİ

Adı Soyadı : Bilal ÖZCAN

Ev Adresi : Yıldırım Mah. Karanfil Sokak No: 47/5
Bayrampaşa / İstanbul

Ev Telefonu : 0 212 537 18 90

İş Telefonu : 0 212 531 01 41

Cep Telefonu : 0 505 825 50 57

E-Posta : bilalozcan@ismek.org, ozcanbilal@gmail.com

KİŞİSEL BİLGİLER

Doğum Tarihi : 23.09.1981

Doğum Yeri : Libya / Sebha

Medeni Durum : Evli

Sürücü Ehliyeti : B

Askerlik Durumu : Tecilli (Yüksek Lisans Yapıyorum)

YABANCI DİL BİLGİSİ

Bildiği Diller	**Derecesi**
1.İngilizce	İyi

BİLGİSAYAR BİLGİSİ

Programlama Dilleri: Basic, Pascal, Visual Basic, C++, Asp.Net, C# , SQL, PL SQL Dreamweaver, Photoshop, Swish, Html

Donanım / Sistem : İyi derecede Donanım ve Network (LAN / WAN) bilgisi

YAYINLAR

1. Bilgisayar İşletmenliği Windows XP Office 2003 Kitabı
2. Bilgisayar İşletmenliği Windows XP Office 2007 Kitabı
3. Yeni başlayanlar için Web tasarımı Kitabı

EĞİTİM DURUMU

Yüksek Lisans Tez Konusu: Kurumsal Bilgi Güvenliği ve COBIT

Eğitim Kurumu	**Bölüm**	**Mezuniyet**
1.Haliç Üniversitesi (Yüksek Lisans)	**MIS(Yönetim Bilişim Sist.)**	2006-Devam Ediyor
2.Haliç Üniversitesi (Lisans)	**Bilgisayar Mühendisliği**	2002–2006
3.Sakarya Üniversitesi (Ön Lisans)	**Bilgisayar Programcılığı**	2000–2002

KATILDIĞIM SEMİNERLER VE EĞİTİMLER

1. Yönetim Becerilerinin Geliştirilmesi
2. Takım Çalışmasının Geliştirilmesi
3. Ast üst ilişkileri
4. Zaman yönetimi
5. NLP Seminerleri
6. Kişisel Kalite ve Motivasyon Seminerleri
7. Girişimcilik Eğitimi
8. Eğitim Kurumlarında Yönetim İlkeleri
9. Formasyon Eğitimi

İŞ DENEYİMİ

Çalıştığı Kurum	**Görev**	**Süre**
İSMEK	Bilgisayar Teknik Rehber	2002- Devam Ediyor
BELBİM A.Ş.	Staj	2003 Yaz dönemi

İSMEK iş tanımı: İSMEK bünyesinde bulunan;

- Bilgisayar işletmenliği,
- Web tasarım
- Grafik tasarım
- Bilgisayar bakım onarım

Kurslarının eğitim danışmanlığı ve rehberlik hizmetleri.