T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ VE E-DEVLET KAPSAMINDA KAMU KURUMLARINDA BİLGİ GÜVENLİĞİ YÖNETİMİ STANDARTLARININ UYGULANMASI

Bünyamin YILDIZ
YÜKSEK LİSANS TEZİ
STRATEJİ BİLİMİ ANABİLİM DALI

DANIŞMANI
Yard. Doç. Dr. S. Zeki İMAMOĞLU

GEBZE
2007

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ	YÜKSEK LİSANS JÜRİ ONAY FORMU

G.Y.T.E. Sosyal Bilimler Enstitü Yönetim Kurulu'nun …… tarih ve ……./……. sayılı kararıyla oluşturulan jüri tarafından ……/……/……. Tarihinde tez savunma sınavı yapılan Bünyamin YILDIZ'ın tez çalışması, Milli Güvenlik Stratejileri Anabilim Dalında, YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE : **Yard. Doç. Dr. S. Zeki İMAMOĞLU**

ÜYE :

ÜYE :

ÜYE :

ÜYE :

ONAY

G.Y.T.E. Sosyal Bilimler Enstitü Yönetim Kurulu'nun …… tarih ve ……./……. sayılı kararı.

İMZA/MÜHÜR

ÖZET

BİLGİ GÜVENLİĞİ VE E-DEVLET KAPSAMINDA KAMU KURUMLARINDA BİLGİ GÜVENLİĞİ YÖNETİMİ STANDARTLARININ UYGULANMASI

Bünyamin YILDIZ

Bilgi teknolojileri güvenliği konusunu anlayabilmek için bilgi teknolojileri yönetim sistemlerini ve bilgi güvenliğinin bu konular içerisinde tutmakta olduğu yeri anlamak gereklidir. Bilgi teknolojileri yönetimi konusunda dünyada en yaygın uygulama alanı bulan iki standart, bu tez kapsamında incelenmiştir. Bu iki standarttan birincisi olan ISO 20000 standardı, bilgi teknolojileri yönetimi için çok iyi sınıflandırılmış, taktik ve operasyonel seviyede işleyen ve kolay uygulanabilen bir standart iken, COBIT standardının bilgi teknolojileri yönetimine stratejik açıdan bakan ve temelini yönetim kararları, yönetilebilirlik ve denetlenebilirlik üzerine kuran geniş kapsamlı bir yapısı vardır. Her iki standartta da, bilgi teknolojileri yönetiminin değişik öğelerinin bu yönetim sistemlerinde yer almakta olduğu değerlendirilmiştir.

Bilgi güvenliği kavramları ve alt öğeleri ise ISC^2'in (Uluslararası Bilgi Sistemleri Güvenliği Sertifikasyon Kurumu, International Information Systems Security Certification Consortium) sınıflandırması CBK (Common Body of Knowledge, Ortak Bilgi Kitlesi) esas alınarak tanıtılmıştır. Bilgi güvenliği uygulamaları kapsamında yapılması gereken etkinlikler ve faaliyetler bu başlıklar altında incelenmiştir.

E-devlet kapsamında kurumların bilgi teknolojileri konusunda durumları irdelenmiş, ISO/IEC 17799:2005 ve ISO/IEC 27001:2005 standartlarının kurumlarda "Bilgi Güvenliği Yönetim Sistemi"ni hangi aşamalarda ve alt başlıklar altında kurduğu anlatılmış, her ISO/IEC 17799 alt başlığı içerisinde kurumlar için ilgili konuda öneriler yapılmıştır.

Sonuç bölümünde, kamu kurumlarında bilişim teknolojileri yönetim sistemi ve bilişim teknolojileri güvenlik sistemi kurulması için hareket planı önerilmiştir.

SUMMARY

INFORMATION SECURITY AND IMPLEMENTATION OF THE INFORMATION SECURITY STANDARTS AT PUBLIC FOUNDATIONS WITHIN THE SCOPE OF E-GOVERNMENT

Bünyamin YILDIZ

In order to understand information technology security, it is essential to understand information technology management and governance concepts. The two most widely practiced and popular information technology management and governance standards are, first ISO 20000 standard, which is a quite easy to implement and understand information technology management system with a tactical and operational point of view, and the second COBIT standard, which is an information technology governance system with a strategic perspective to implement information technology strategies for manageability and effective auditing of the system. Both standards include key aspects of information technology security system elements.

Information technology security concepts and sub categories are studied based on ISC^2's "Common Body of Knowledge". Information security applications and practices are studied under this topic.

Status of the Foundations at the issue of Information Technologies was examined within the scope of e-government. The implementation phases of "Information Technologies Security System" (ISMS) in organizations using ISO/IEC 17799:2005 and ISO/IEC 27001:2005 standarts and the 17799 clauses are covered. In each clause, related suggestions are made for public foundations.

In the conclusion, IT securtiy applications in public foundations are discussed and an action plan to implement IT governance and management systems in the organization.

TEŞEKKÜR

Bu denli zor bir çalışmada bana hep destek olan, e-devlet projesinin ülkemizdeki mimarı sayılan ve çalışmalarını DPT'da sürdüren, Mülki İdare Amiri meslektaşım Ramazan ALTINOK'a, standartların temini, ilgili siteler ve diğer kaynaklar konusunda yardımcı olan DPT E-Dönüşüm Türkiye projesinin yürütücülerinden olan Kamil TAŞÇI ve UEKAE (TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) çalışanı Mehmet ERİŞ'e, sevgili hocam Prof. Dr. Salih AYNURAL'a, danışmanım Yard. Doç. Dr. S. Zeki İMAMOĞLU'na ve sevgili eşime dostlukları ve destekleri için teşekkür ederim.

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

ABD	: Amerika Birleşik Devletleri
AES	: Advanced Encryption Standart
API	: Application Programming Interface-Uygulama Yazılım Arabirimi
BGYS	: Bilgi Güvenliği Yönetim Sistemi
BS	: Bilgi Sistemleri
BT	: Bilgi Teknolojileri
CBC	: Cipher Block Chain
CBK	: Common Body of Knowledge-Ortak Bilgi Kitlesi
CFB	: Cipher Feedback Mode
CISSP	: Certified Information Security Systems Professional
CMM	: Capability Maturity Model
COBIT	: Control Objectives for Information Technologies-Bilgi Teknolojileri için denetim hedefleri/kıstasları
CRC	: Cyclic Redundancy Check- hata kontrol kodu
DES	: Digital Encryption Standart
DoS	: Hizmet reddi saldırısı, Denial of Service
DMZ	: DeMilitarized Zone (Askerden Arındırılmış Bölge)
DPT	: T.C. Başbakanlık Devlet Planlama Teşkilatı
ECB	: Electronic Codebook
HTTP	: HyperText Transport Protocol)
$(ISC)^2$	: International Information Systems Security Certification : Consortium
IPsec	: Internet Protocol Security-internet protokol güvenlik
ISACA	: Information Systems Audit and Control Association
ISO	: Uluslararası Standartlar Örgütü
ITGI	: Information Technologies Governance Institude
ITSEC	: Information Technology Security Evaluation Criteria
ITIL	: Information Technology Infrastructure Library-BT Altyapı Kütüphanesi
LLC	: Logical Link Control
KPS	: Kimlik Paylaşımı Sistemi

MAC	: Media Access Control
MERNİS	: Merkezi Nüfus İdaresi
NetBEUI	: NetBIOS Extended User Interface
OASIS	: Organization for the Advancement of Structured Information Standards
OGC	: Office of Government Commerce
OFB	: Output Feedback Mode
OSI	: Birbirine Bağlı Açık Sistemler,Open Systems Interconnection
OODA	: Observe-Orient-Decide-Act -Gözle-Yönlendir-Karar Ver-Harekete Geç
PIN	: Personal Identification Number- Kişisel Tanımlama Sayısı
SAPs	: Service Access Points
SECOQC	: Secure Communication based on Quantum Cryptography
SESAME	: Avrupa Çok Kaynaklı Uygulamalar Ortamında Güvenlik Sistemi, Secure European System for Applications in a Multivendor Environments
SPX	: Sequenced Packet Exchange
SSO	: Single Sign On, Tek Giriş
T.B.M.M.	: Türkiye Büyük Millet Meclisi
TCB	: Trusted Computing Base
TCP	: Transmission Control Protocol
TCSEC	: Güvenilen Bilgisayar Sistemleri Değerlendirme Kıstasları, Trusted Computing Systems Evaluation Criteria
TÜİK	: Türkiye İstatistik Kurumu
UEKAE	: Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UYAP	: Ulusal Yargı Ağı projesinde
VPN	: Virtual Private Network, Sanal Özel Ağ
YTCK	: Yeni Türk Ceza Kanunu

ŞEKİLLER DİZİNİ

Sayfa

TABLOLAR DİZİNİ

Sayfa

1. GİRİŞ

"E-dönüşüm Türkiye" projesi Başbakanlık'ın 2003/12[1] sayılı genelgesi ile başlamış, 2003/48 sayılı Genelge[2] ile de DPT (T.C. Başbakanlık Devlet Planlama Teşkilatı) projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile görevlendirilmiştir. Bu bağlamda çalışmalarına başlayan DPT Bilgi Toplumu Dairesi, "E-dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi"ni yayınlamıştır. Rehber'de kamu kurumlarında bilgi güvenliği yönetim sistemlerinin kurulmasının önemi anlatılmış, ISO/IEC 17799 standardının e-devlet çalışması yapan tüm kurumlarda uygulanması öngörülmüştür. Kamu kurumlarını bağlayıcı nitelikteki bu dokümanda bilginin önemini ve bilgi güvenliğine ihtiyacı anlatan, "Kurumlar için en kritik varlık bilgidir. Kurumların değerleri, sahip oldukları bilgi ile ölçülmektedir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir. Kurum bünyesinde yaratılan, işlenen, depolanan, iletilen, imha edilen ve kullanılan bilgi ile kurumlar arasında iletilen bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumak güvenliğin temel hedefidir." (e-dönüşüm projesi, 2005, s. 24) ibaresi bu çalışmanın esasını oluşturmaktadır.

Ülkemizde yukarıda belirtilen çalışmalar ile başlayan bilgi güvenliği çalışmalarının gelecekte ne boyutlara varacağını bu konuda geçmişte adımlar atmış ülkeler incelenerek görülebilir. ABD'de (Amerika Birleşik Devletleri) bilgi de dâhil olmak üzere, hassas altyapıları korumak için iki önemli çalışma yapmıştır. İlki önemli altyapıların hizmet sürekliliğini sağlamak üzere çıkarılmış "ABD Başkanlık Emri 63[3]", ikincisi ise Bilgi Sistemlerini Korumak için Ulusal Plan (National Plan For Information Systems Protection[4])dır. Bu dokümanlar ABD'de bilgi güvenliği ihtiyaçlarını ulus çapında belirlemeye çalışmakta ve tartışma açarak farkındalık yaratmayı amaçlamaktadır.

Benzer çalışmalar e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı[5] çerçevesinde, UEKAE (Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) tarafından kamu kurumlarında güvenlik taramaları olarak yapılmıştır. Gelecek

[1] T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü, 2003/12, 27/02/2003.
[2] T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü, 2003/48, 03/11/2003.
[3] Presidential Decision Directive NSC/63, 23/05/1998.
[4] National System for Information Sysytems Protection, The White House, 2000.
[5] e-Dönüşüm Türkiye Projesi 2005 Eylem Planı, 03/2005, s.3-4.

günlerde bu konuda gelişmiş ülkelerin uygulamaları Türkiye'de de görülebilecek şekilde planlamalar yapılmaktadır. "Bilgi Toplumu Stratejisi Eylem Planı (2006-2010)"nda güvenlik ve kişisel bilgilerin mahremiyeti eylem planının ana temaları arasında sayılmaktadır. Plan'da "Bilgi Sistemleri Olağanüstü Durum Yönetim Merkezi" (Eylem Planı, 2006, s. 26) oluşturulması, "ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenleme" (Eylem Planı, 2006, s. 29) yapılması ve "Ulusal Bilgi Sistemleri Güvenlik Programı" (Eylem Planı, 2006, s. 29) oluşturulması eylemleri de bulunmaktadır.

Ülkemizdeki mevcut durumda kurumların çoğu e-dönüşüm kapsamında kendi altyapılarını oluşturmuşlar, ancak tam entegre hale gelememişlerdir. E-devlet Projesiyle ilgili çalışmalar DPT - Bilgi Toplumu Dairesi tarafından yürütülmektedir. Çok kritik bilgileri barındıran kamu kurumlarının, güvenliğinin yönetilmesi de o kadar önemli ve kritiktir.

Kamu kurumlarında BGYS (Bilgi Güvenliği Yönetim Sistemi)[6] uygulanabilmesi için bilgi güvenliği kavramlarından önce bilgi teknolojileri sistemlerinin yönetim stratejilerinin neler olacağının belirlenmesi gerekmektedir. "Bilgi Teknolojileri Yönetim Sistemleri" olarak anılan COBIT ISO 20000-1,2 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, erişilebilirliği ve bütünlüğü ile ilgilidir.

Bilgi sistemi ile ilgili tüm standartlarının atıf yaptığı kavramlar göz önünde bulundurulduğunda, yedi temel kavram öne çıkmaktadır ki bunlar etkinlik, verimlilik, gizlilik, bütünlük, erişilebilirlik, uyumluluk ve güvenilirlik olarak sıralanırlar. Standartlar bu kavramların içini değişik oranlarda doldurmaya çalışırlar. Güvenlik, bilgi teknolojileri yönetim sistemlerinin içerisinde bir alt başlıktır. Bilişim dünyasında genel kabul gören yöntem, bilgi yönetimi sistemlerinden birini uygulamak, güvenlik standartları arasında en kabul göreni olan güvenlik

[6] Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 17799-1 ve 27001 standartlarının kurumlarda oluşturdukları güvenlik yapısının adıdır.

standartlarının bilgi yönetimi sistemlerinin alt öğesi olarak yürütülmesidir.[7] Bu şekilde kurumlar, sistemin güvenliğini garanti altına almakta, hizmet kalitesinin belli seviyelerin altına düşmemesini sağlamakta ve bu iki iş için iki ayrı sistem kurmak yerine tüm güvenlik ve bilgi teknolojileri yönetim sistemleri için merkezi bir sistem kurmaktadırlar.

Çalışmanın ikinci bölümünde, bilgi teknolojileri yönetim sistemleri anlatılmaktadır. Yönetim sistemlerinin en yaygını olarak bilinen COBIT ve ISO 20000-1 ve 2 bu kapsamda irdelenmektedir. Üçüncü bölümde, bilgi güvenliği kavramları, dördüncü bölümde yer alan ISO/IEC 17799:2005 ve ISO/IEC 27001:2005 standartlarının anlaşılmasına temel olmak üzere anlatılacaktır. Dördüncü bölümde, ISO/IEC 17799:2005 standardı içeriği ve kurduğu BGYS yapısına yer verilmiştir. Bu bölümün her alt bölümünde e-devlet bilgi güvenliği ihtiyaçlarından bahsedilerek, bunlar standarda uyumluluk çerçevesinde irdelenmiştir.Tezin sonuç bölümünde ise kurumun bilgi teknolojilerinden beklentilerinin belirlemesi ve güvenlik ihtiyaçları da dahil olmak üzere bilgi teknolojileri yönetim sistemi kurulması için hareket planı önerilmektedir.

[7] Bkz: 2.2.2. Cobit yapısı, 2.1.1.12. Bilgi teknolojileri güvenlik yönetimi

2. BİLGİ TEKNOLOJİLERİ YÖNETİMİ

Bilgi teknolojileri, veri, malumat ve bilgiyi teknoloji yardımıyla işlemek, dağıtmak için kullanılan sistemler ve yöntemlerin genel adıdır. Burada bahsedilen sistem, yöntem ve teknolojiler, büyük oranda bilgisayar yazılım ve donanımlarını ifade etmektedir. (http://en.wikipedia.org)

Giderek artan karmaşıklığı ile bilgi teknolojileri araçlarını yönetmek zorlaşmaktadır. Bu karmaşıklığı azaltmak, bilgi teknolojisi araçlarının, iş verimine katkısını artırmak ve iş sürekliliğini sağlamak için çeşitli standartlar ortaya konulmuştur. Bilgi güvenliği, bu standartların bir alt başlığını oluşturmaktadır. Bilgi teknolojileri yönetiminin değişkenlerini, süreçlerini, işin bilgi teknolojileri ortamına aktarılması süreçlerini anlamadan bilgi güvenliğini sağlamak zorlaşmaktadır. Bunun nedeni, güvenlik standartlarının kapasite yönetimi, varlık yönetimi, iş sürekliliği yönetimi gibi konulara atıf yapması, ama bu konularda tanımlı bir yapı kurmamasıdır.

Bilgi güvenliği kavramlarını açıklamadan önce, bilgi teknolojilerinin yönetimlerinin nasıl olacağı konusunda kriterler ortaya koymuş standartların bir özeti yapılmıştır. Böylece genelden özele doğru inilmiştir. Bilgi teknolojileri yönetimi konusunda en önemli iki standarda burada kısaca yer verilmesi gerekmektedir.

Bu Standartlar:

- ISO 20000-1 “Bilgi Teknolojisi – Hizmet Yönetimi – Tanımlama” ve ISO 20000-2 “Bilgi Teknolojisi – Hizmet Yönetimi – Uygulama Prensipleri” Standartları,
- COBIT “Bilgi teknolojileri için denetim hedefleri/kıstasları” standartlarıdır.

2.1. ISO 20000 ve ITIL

ITIL (Information Technology Infrastructure Library - Bilgi Teknolojileri Altyapı Kütüphanesi), BT (Bilgi Teknolojileri) Servislerini yönetmede ayrıntılı ve yapısal en iyi uygulama örnekleri serisidir. ITIL, 80'lerin sonunda İngiltere Ticaret Bakanlığı (OGC - Office of Government Commerce - İngiltere Ticaret Bakanlığı) tarafından geliştirilmiştir. Süreç yaklaşımı sayesinde ITIL müşteri, tedarikçi, BT

bölümü ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını mümkün kılmaktadır. İngiltere ve Hollanda da hızlı uyumu ile şimdi ITIL dünya çağında kullanılan ve tanınan bir iş standardı haline gelmiştir (http://www.infratech.com.tr).

İngiliz Hükümeti, pek çok değişik kurumunun farklı teknoloji altyapılarının fazla karmaşık hale gelmesi, arıza sayısının artması, planlamanın zor hale gelmesi ve hizmet sürekliliğinin gitgide artan oranlarda kesilmesi sonucunda tüm kamu kurumlarını ve bazı özel kurumları kapsayan bir "en iyi bilgi teknolojileri uygulamaları kütüphanesi oluşturma" çalışmalarına başlamıştır. Bu çalışmalar kapsamında her kurumun bilgi teknolojileri alanındaki en iyi uygulamaları esas alınıp her kurum için geçerli olabilecek bir "en iyi uygulamalar kütüphanesi" oluşturulmuştur. Bu kütüphane İngiliz Standart Kurumu British Standart'ın 15000 numaralı standardı olarak 1980'lerde yayınlanmıştır. Bu standart özellikle 1990'lı yıllarda kendine geniş uygulama alanı bulmuştur. Bilişim teknoloji hizmetlerini sınıflama şekli ve getirdiği önlemler ile özel sektör ya da kâr amacı gütmeyen her kurumun bilişim teknolojileri hizmetlerine uygulanabilir bir standart geliştirmiştir.

Bugün yürürlükte olan ve kökeni yukarıda anlatılan BSI 15000 standardına dayanan 15.12.2005 tarihinde yürürlüğe girmiş olan ISO 20000 standardı iki bölümden oluşmaktadır;

ISO 20000–1 Bilgi Teknolojileri – Hizmet Yönetimi – Tanımlama

ISO 20000-2 "Bilgi Teknolojisi – Hizmet Yönetimi – Uygulama Prensipleri"

2.1.1. ISO 20000–1 Bilgi Teknolojileri – Hizmet Yönetimi – Tanımlama

BT işletimi ve hizmet yönetiminde sürekli iyileştirme, ISO 20000'in en temel unsurudur. Bir kere sistem kurulduktan sonra sürekli olarak süreçlerin performansı takip edilmelidir.

ISO 20000 BT Hizmet Yönetim Sistemi , hizmet kalitesinin artması, güvenilir kurumsal destek, hizmetler hakkında daha net veriler elde edilmesi, çalışanların daha iyi motivesi ve yeteneklerin doğru analizi yapılması, müşterilere tatmin ve doğru hizmet sunulması, hizmet süreçlerinin güvenliğinin sağlanması ve sürekli erişim gibi bir çok faydalar sağlayabilen bir sistemdir (http://www.infrateech.com.tr).

ISO 20000 standardının 1. bölümü ITIL kütüphanesini oluşturan parçacıkların neler olduğunu, tanımlamalarını, içeriklerini ve çıktı-girdi ilişkilerini açıklayan standarttır. Şekil 2.1'den de görülebileceği gibi hizmet yönetimi on iki alt

düzenlemeden oluşmaktadır. Birbirleri ile ilişkileri gösterilen bu alt yönetimler ve açıklamaları şunlardır; (ISO/IEC 20000–1- 2005(E))

- Olay Yönetimi
- Sorun Yönetimi
- Konfigürasyon Yönetimi
- Değişim Yönetimi
- Sürüm Yönetimi
- Yardım Masası
- Servis Seviyesi Anlaşmaları
- Bilgi Teknolojileri Maliyet Yönetimi
- Bilgi Teknolojileri Kapasite Yönetimi
- Kullanılabilirlik (Mevcudiyet) Yönetimi
- Hizmet Sürekliliği Yönetimi
- Bilgi Teknolojileri Güvenlik Yönetimi

Şekil 2. 1: ISO 20000 alt parçaları ve birbirleri ile ilişkileri (ISO/IEC 20000-1:2005(E))

2.1.1.1. Olay Yönetimi

Kurumda standart olmayan, hizmetin ulaşmasını engelleyen veya hizmetin kalitesini düşüren olaylar "vaka" olarak adlandırılır. Bu tip bir olay gerçekleştiğinde servis hizmetinin ilk ve en temel aşamasında, gelen servis taleplerinin tanımlanarak ilgili kişi veya gruplara aktarılmasından sorun çözümünün gerçekleştirilmesi ve çözüm veritabanına aktarılmasına kadar tüm aşamaları takip eder. (ISO/IEC 20000–1- 2005(E)). Standart olarak gelen çağrıların (servis taleplerinin) ilk seviye servis elemanları tarafından çözülmesi, çözülemezse diğer çözüm seviyelerine aktarılması, olay kayıtlarının tutulması, alarm/uyarı mekanizması ve gelişmiş arama fonksiyonlarıyla diğer modül ve ürünlerle entegre olarak BT altyapısını ilgilendiren tüm olayların başlangıcından sonuçlanmasına kadar tüm aşamalarda yönetiminin yapılmasını sağlar (http://www.infrateech.com.tr).

2.1.1.2. Sorun Yönetimi

Vaka yönetiminden farklı olarak sorun yönetimi pek çok soruna yol açan temel bir sorunun teşhisini ve tedavisini yapar. Vaka yönetiminden farkı kapsamıdır. Sorun yönetimi çeşitli şekillerde kendini gösteren küçük sorunların temelindeki büyük sorunları çözmeye çalışır. Verilen hizmet esnasında sık karşılaşılan sorun / arızaların kaynaklarının bulunması, araştırma süresince geçici çözümlerin esas sorunla ilişkilendirilmesi, daha sonra sorunun kaynağı bulunduğunda, bu bilginin bilinen hatalar veritabanına otomatik olarak konulabilmesini sağlar. Bu sayede daha önce karşılaşılan problemlerin daha kısa sürede çözülmesine veya henüz ortaya çıkmadan müdahale edilmesine olanak tanır. (ISO/IEC 20000–1- 2005(E))

2.1.1.3. Konfigürasyon Yönetimi

Konfigürasyon yönetimi bilgi teknolojileri altyapısını oluşturan tüm bileşenlerin, bu bileşenlerin amacına uygun çalışabilmeleri için gereken tüm özelliklerinin kayıt altında tutulmasıdır. Kayıt altında tutulan her bir bileşene "konfigürasyon bileşeni" adı verilir. Bu yönetim şu alt aşamalardan oluşur: (ISO/IEC 20000–1- 2005(E))

- Planlama
- Tanımlama ve isimlendirme
- Kontrol
- Mevcut durum muhasebesi
- Denetleme

2.1.1.4. Değişim Yönetimi

Değişim yönetimi, değişimle ilgili konuların hizmet sürekliliğini ve kalitesini etkilememesi için standart değişim yöntemleri oluşturulması sürecidir. Bu sürecin alt parçaları şunlardır:

- Değişim isteği yapılması
- Değişim isteklerinin incelenmesi ve konfigürasyon yönetimi tablosuyla karşılaştırılması
- Değişim isteklerinin filtrelenmesi
- Değişim isteklerinin değişim planlama tablosuna işlenmesi

Önemli veya geniş çapta yapılacak altyapı değişikliklerini planlı, iş akışları ve onay süreçlerine dayalı, riskleri ve olası sorunları minimize ederek yönetebilmeyi sağlar. Değişiklikler, kritik faaliyetleri yöneten altyapılarda yönetimi zor ve riski yüksek olabilirler. Değişim Yönetimi modülü detaylı iş akışı, onaylama mekanizması ve takip seçenekleri ile potansiyel olarak kritik değişim faaliyetlerinin kolaylıkla yapılmasını sağlar. Ayrıca son kullanıcıların yeni ürün veya parça taleplerinin onay mekanizması kontrollü yönetimine ve periyodik olarak yapılması gereken bakım işlemlerinin belirlenen herhangi bir zaman aralığı içinde otomatik uyarı ve eskalasyon mekanizmasıyla yönetimine olanak tanır. Olay yönetimi modülüne entegre olması sayesinde değişim ve bakım zamanı gelen işlemler için birer "olay kaydı" yaratılarak, Olay Yönetimi modülünün sağladığı geniş takip olanaklarından faydalanılmasını sağlar. (http://www.infratech.com.tr)

2.1.1.5. Sürüm Yönetimi

Sürüm yönetimi bir kurum içerisinde kullanımda olan yazılımların konfigürasyon bileşenlerinin yönetimidir. Sürüm yönetimi, kurum içerisinde hangi donanımların hangi yazılımları çalıştıracağı ile ilgilenir. Burada belirlenmesi gereken bu yazılımların birbirleri ve üzerinde çalıştıkları donanımlar ile ne kadar uyumlu çalıştıklarıdır. Bu kıstaslara bakılarak kurumlarda “Belirleyici Yazılım Kütüphanesi” oluşturulur. Bu hem fiziksel hem de mantıksal bir kütüphanedir. Fiziksel olarak kurumda kullanımda olan her yazılımın kullanım lisansları ve bir kopyası tek bir yerde tutulur. Mantıksal olarak da kurumda her donanımın çalıştırmakta olduğu yazılımların listesi çıkarılır, olması gerekenle karşılaştırılır ve uygun olarak düzenlenir. Yazılımların değişimi ihtiyacı olduğunda bunun süreçleri değişim

yönetimi basamaklarına göre yapılır ve her yazılım yapılandırmasına bir sürüm numarası verilir. (ISO/IEC 20000–1- 2005(E))

2.1.1.6. Yardım Masası

Yardım masası aynı zamanda "Tek İletişim Noktası" olarak da adlandırılır. Müşteri ya da kullanıcılar her türlü istek ya da sorunlarını kayıt numarası almak kaydı ile tek bir iletişim noktasına bırakırlar. Bu istekler bir sorun, vaka ya da değişim isteği olabilir. Buradaki kritik nokta kullanıcı ya da müşterinin ilgili kişiye kendisinin ulaşmak zorunda olmayışıdır. Kullanıcının tek bilmesi gereken, isteğinin hangi sınıflamaya girdiğini bilmek, isteğinin kabaca tanımını yapabilmek ve bunu tek iletişim noktasına iletmektir. İstekler, arka planda değerlendirilerek ilgili önlemler alınır ve kullanıcı gelişmelerden haberdar edilir. (ISO/IEC 20000–1- 2005(E))

2.1.1.7. Servis Seviyesi Anlaşmaları

Konfigürasyon bileşenlerinin işlevlerini yapamamaları ihtimaline karşı bu bileşenlerin uygun fiyat karşılığı bakım anlaşması altında tutulmaları esastır. Burada dikkat edilmesi gereken noktalar kullanıcı ihtiyaçları, hizmetin maliyet etkin tedariki, hizmetin güvenlik gereksinimlerini ihlal etmeden verilmesi ve hizmetin belirli bir kalite seviyesinin üzerinde tedarik edilmesidir. (ISO/IEC 20000–1- 2005(E))

2.1.1.8. Bilgi Teknolojileri Maliyet Yönetimi

Bilgi teknolojileri maliyet yönetimi, genel olarak bilgi teknolojileri hizmetlerinin en maliyet etkin yöntemlerle verilmesinin garanti altına alınmasıdır. Değişim planlama tablosundaki veriler yaklaşık maliyet hesaplamaları ile hesaplanarak kurumların bilgi teknolojileri yıllık maliyetleri ortaya konur. Bu maliyetler ortaya çıkarıldıktan sonra kurum yapısı elveriyor ise bu maliyetler müşteri ya da kullanıcılardan tahsil edilir. (ISO/IEC 20000–1- 2005(E))

2.1.1.9. Bilgi Teknolojileri Kapasite Yönetimi

Bilgi teknolojileri kapasite yönetimi, bilgi teknolojileri ürünlerinin kurumlarda doğru fiyata, doğru hacimde ve verimliliği en yüksek düzeyde tutarak yönetilmesidir. Bu planlama yapılırken hangi hizmetin hangi kaynakları kullandığı, bu kaynakların ne kadar yedekliliğe ihtiyaç duydukları ve bunların maliyeti ortaya konulur. Kapasite yönetimi, iş, hizmet, kaynak gibi üç bileşenin yönetimini yapar. (ISO/IEC 20000–1- 2005(E))

Kapasite yönetimi şu değişkenler izlenerek yapılır; (ISO/IEC 20000–1- 2005(E))

- Performans takibi
- İş yükü takibi
- Uygulama ölçeklenmesi
- Kaynak ihtiyacı tahmini
- İstek tahmini

2.1.1.10. Kullanılabilirlik (Mevcudiyet) Yönetimi

Konfigürasyon bileşenlerinin her birinin kullanıma hazır ve çalışır halde bulunurluğunu sağlayan süreçtir. Bu süreç dahilinde her konfigürasyon bileşeni için aşağıdaki değişkenler belirlenir; (ISO/IEC 20000–1- 2005(E))

- Hizmet Verilebilirlik: Hizmet üçüncü taraflar tarafından veriliyor ise hizmet ya da parçanın ulaşma süresi
- Güvenilirlik: Bileşenin hata vermeden çalışma süresi
- Geri Kazanım Süresi: Bileşen hata verdikten sonra geri çalıştırmak için gereken süre
- Bakım Kolaylığı: Bileşenin hem hata önleyici olarak, hem de hata verdikten sonra geri kazanımının ne kadar kolay olduğu kıstasları
- Dayanıklılık: Hataya vermeye karşı sağlamlığı
- Güvenlik: Sızmalara karşı ne kadar güvenli olduğu, gizliliğe ne kadar izin verdiği açılarından değerlendirilirler.

2.1.1.11. Hizmet Sürekliliği Yönetimi

Hizmet sürekliliği yönetimi bilgi teknoloji bileşenlerini etkileyen ciddi bir hata ya da etki olduğunda bilgi teknoloji hizmetlerinin en kısa sürede çalışır hale getirilmesi planlarının yapılmasıdır. Bu plana "İş Süreklilik Planı" denir. İş süreklilik planı hazırlanmasının aşamaları şu şekildedir. (ISO/IEC 20000–1- 2005(E))

1. Hangi işlerin daha önemli ve önce çalışır hale getirileceği "İş Etki Analizi" sonucunda belirlenir.
2. Her hizmet için tehdit, zafiyet ve önlem analizi (risk yönetimi) yapılır.
3. Kurtarma alternatifleri değerlendirilir.
4. Plan düzenli olarak test edilir, tatbikat yapılır ve gözden geçirilir.

2.1.1.12. Bilgi Teknolojileri Güvenlik Yönetimi

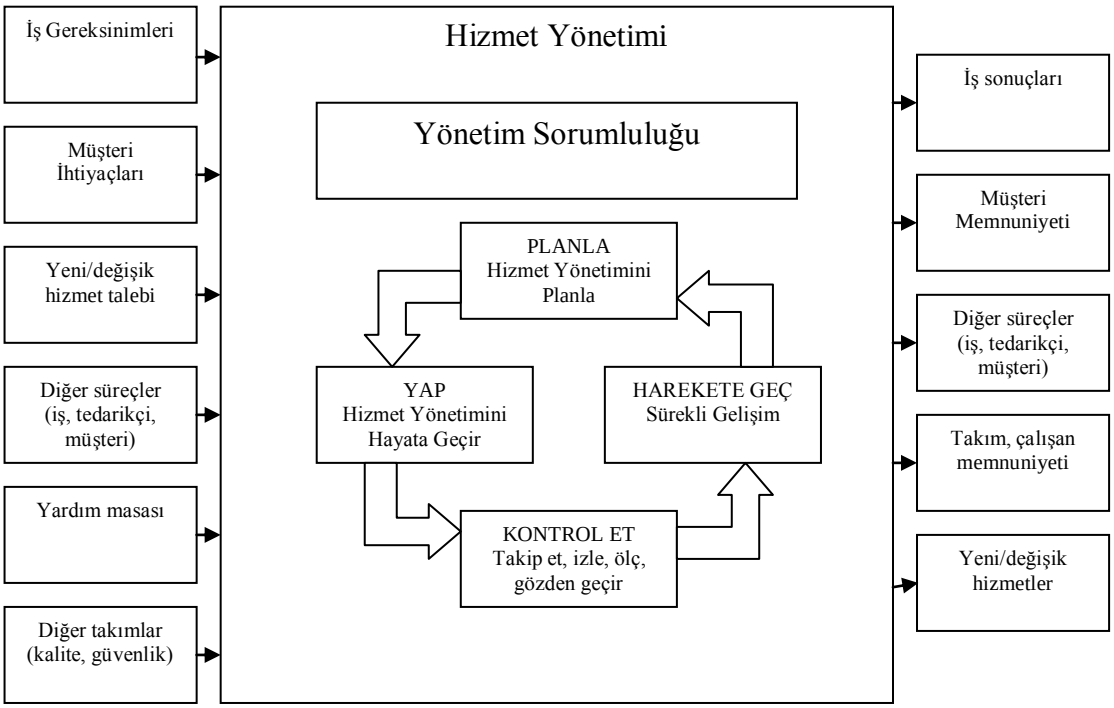
ISO 20000 güvenlik yönetimi için ISO 17799'u adres gösterir. Burada ki kritik nokta, güvenliğin bilgi teknoloji hizmetlerinden biri olmasıdır. Bilgi teknolojileri güvenlik yönetimi bu tezin ana konusudur ve ikinci ve üçüncü bölümlerde tüm detaylarıyla anlatılmıştır. ISO 20000 kapsamında bilgi güvenliği hakkında söylenmesi gereken, güvenliğin bilişim teknolojileri yönetimi konusunun küçük ve öteki bileşenlerden ayrılmaz bir parçası olduğudur. Bilgi teknolojisi yönetimi sisteminin diğer öğeleri olmadan, vaka ve olay yönetimi olmadan güvenlik olaylarının düzgün şekilde rapor edilmesi mümkün değildir. Konfigürasyon yönetimi olmadan hangi bileşenlerin güvenlik önlemi kapsamında olduğu, bu bileşenlerin kimin sorumluluğunda olduğu ve bileşenin fiziksel olarak nerede olduğu, teknik özellikleri bilinemeyecektir. Değişim yönetimi olmadan yapılacak değişimlerin güvenliğe etkileri analiz edilemez, yapılacak değişimlere göre güvenlik önlemleri de güncellenmelidir. Değişim yönetimi münferit değişimlere karşıdır, değişimler değerlendirilir ve planlanır. Bu planlama merkezi güvenlik önlemlerini belirli bir konfigürasyon üzerinde yapmayı kolaylaştırır. Hizmet masası yapılan tüm isteklerin ve olayların bir listesini tutarak kurumların bilgi teknolojileri güvenilirliğinin kolayca izlenmesini sağlar. Küçük parçalardan oluşan merkezi güvenlik açıklarının tespitini kolaylaştırır.Maliyet yönetimi olmadan güvenlik önlemlerinin belirli tehdit türlerine karşı alınması gerekip gerekmediği belirlenemez. Kural olarak önlem tehditten daha pahalıya mal olamaz. Kapasite yönetimi olmadan hizmetlerin ne kadar yedekli olması gerektiği tespit edilemez. İş süreklilik ve mevcudiyet yönetimi hangi hizmetin ne kadar önemli olduğunu ortaya koyar ve güvenlik konusunun da bir alt başlığıdır.

2.1.2. ISO 20000–2 Bilgi Teknolojileri – Hizmet Yönetimi – Uygulama Prensipleri

ISO 20000 standardının ikinci bölümünde yukarıda ana hatları ve birbirleri ile ilişkileri anlatılan hizmetlerin alt başlıkları detaylı olarak ele alınır ve olası durumlara karşı nasıl davranılması gerektiği konusunda prensipler yazılıdır. İzlenmesi gereken değişkenler, geri besleme süreçleri, maliyet hesaplama yöntemleri, planlamaların nasıl yapılacağı, risklerin nasıl hesaplanacağı vb. konular detayları ile irdelenir.

Şekil 2.2. de ISO 20000 sürecinin girdileri, çıktıları ve sürecin içeriği görülmektedir. Planla – yap – kontrol et – harekete geç döngüsü olarak adlandırılan

bu sistem, aynı zamanda ISO 27001 Bilgi Güvenliği Yönetim Sistemleri standardının da temelini oluşturmaktadır. ISO 20000 – 1,2 ve ISO 17799 – ISO 27001 ailesi standartların 2005 yılı sürümleri, özellikle birbirleri ile uyumlu çalışacak şekilde tasarlanmışlardır. Bu standartlar kurumların aynı döngü süreci içerisinde bilgi teknolojileri yönetim sistemlerini ve bilgi teknolojileri güvenlik sistemlerini beraber çalıştırabilecekleri bir çerçeve oluşturmaktadırlar (ISO/IEC 20000–1- 2005(E)).



Şekil 2. 2: ISO 20000 süreçlerini gözden geçirmek için kullanılan planla – yap-kontrol et – harekete geç döngüsü (ISO/IEC 20000-1:2005(E))

2.2. COBIT (Control Objectives for Information Technologies - Bilgi Teknolojileri için Denetim Hedefleri/Kıstasları)

İsmi İngilizce "bilgi teknolojileri için denetim hedefleri/kıstasları" olan bu standart, ISACA (Uluslararası Bilgi Teknolojileri Kontrol ve Denetim Birliği, Information Systems Audit and Control Association)[8] ve ITGI (Bilgi Teknolojileri Yönetim Enstitüsü, Information Technologies Governance Institude)[9] tarafından hazırlanmıştır. Şu anda üçüncü sürümü yürürlükte olan standardın uygulanması bir çok ekonomik skandaldan sonra yürürlüğe giren, şirketlerin mali denetim sistemi

[8] http://www.itgi.org/
[9] http://www.itgi.org/

kurmalarını zorunlu kılan Sarbanes-Oaxley kanunundan[10] sonra ABD'de yaygınlık kazanmıştır.

COBIT'in misyonu, standardın ilk bölümünde, "Yöneticiler ve denetçiler için otoriter, güncel ve uluslararası bir bilgi teknolojileri denetim hedefleri oluşturmak" (COBIT Framework, 2000) olarak ifade edilir. Bu misyondan anlaşılabileceği gibi bu standart yönetme ve disiplin altına almayı diğer hedeflerin önüne almaktadır. Bu standarttaki temel amaç, bilgi teknolojilerini yönetmek ve denetlemek için yöneticilerin eline bilgi teknolojileri yönetimi konusunda daha fazla araç ve sistematik bir yaklaşım vermektir. (COBIT Framework, 2000)

2.2.1. COBIT kitapları

COBIT şu altı yayınında yapılması gereken faaliyetleri özetler;

2.2.1.1. **Yönetici Özeti** (COBIT Executive, 2000):

Yönetici özeti, COBIT uygulamasını ve kavramlarını ve COBIT'i oluşturan 34 adımı herkesin anlayabileceği şekilde özetler. Bu yayının amacı COBIT süreçleri ve kavramlarını tanıtmak ve bunlar hakkında farkındalık yaratmaktır.

2.2.1.2. **COBIT Çatısı** (COBIT Framework, 2000):

COBIT çerçevesi de olarak Türkçe'ye çevrilebilecek bu yapı, kurumsal bilginin nasıl akması gerektiğinin, iş hedeflerine ulaşmak için bilginin hangi süreçlerde akacağının yapısıdır. Çerçeve yedi bilgi kıstasını (etkinlik, verimlilik, gizlilik, bütünlük, erişilebilirlik, uyumluluk ve güvenilirlik) ve bu bilginin ihtiyaç duyduğu kaynakları (insanlar, uygulamalar, teknoloji, tesis ve veri) ifade edip açıklar.

2.2.1.3. **Kontrol Hedefleri** (COBIT Control Objectives, 2000):

Bu yayın, bilgi teknolojileri sistemlerini kontrol edebilmek için, tanımlı 34 süreç adımından yola çıkarak 215 adet kontrol hedefi belirler. Bilgi teknolojileri, bu belirlenmiş hedefler aracılığı ile kontrol altında tutulur.

2.2.1.4. **Denetim Kılavuzları** (COBIT Audit Guidelines, 2000):

Bilgi teknolojileri, değer biç, incele, yorumla, karşı tedbiri belirle ve harekete geç sırasıyla sürekli bir döngü içinde denetlenmelidir. Denetçiler kararların ve

[10] "Sarbanes-Oaxley act of 2002" H.R. 3763,

uygulamaların COBIT'in 34 adımını takip edilerek yapılıp yapılmadığı ve kontrol hedeflerine ulaşılıp ulaşılmadığını denetim altında tutmaya çalışırlar.

2.2.1.5. **Uygulama Kılavuzu** (COBIT Implementation Tool Set, 2000):

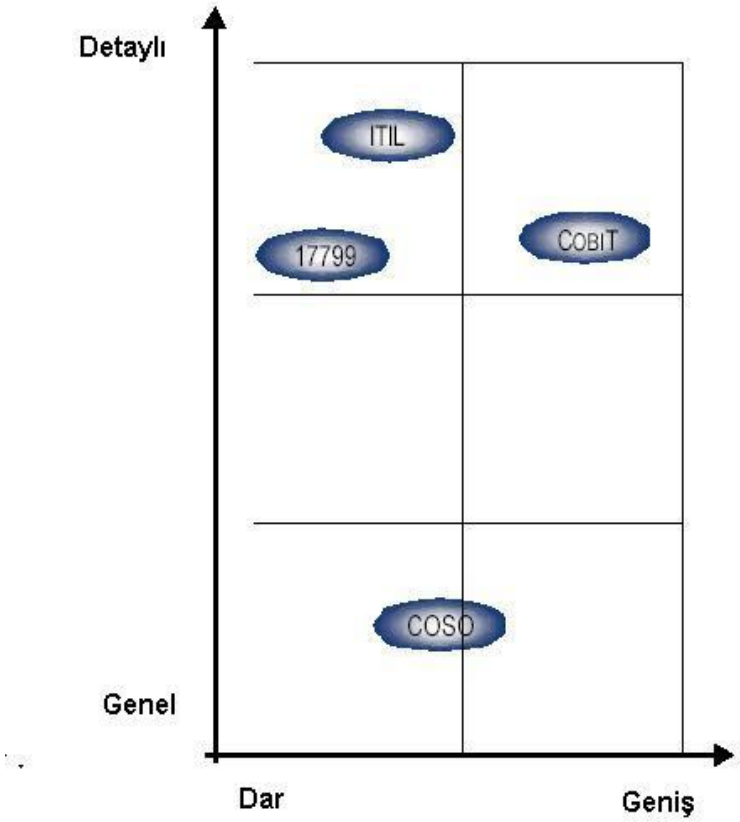
COBIT'in uygulaması esnasında doğabilecek alt seviye sorunların çözülebilmesi için en iyi uygulamalar, sıkça sorulan sorular, COBIT'i hızla ve başarıyla uygulamış kurumların edindiği dersler gibi konuların ele alındığı bir kılavuzdur. Diğer yüksek seviye kılavuzlarda ele alınmayan konular uygulama kılavuzunda yer alır. COBIT'in taktik ve operasyonel seviyede nasıl uygulanacağını anlatan kılavuzdur.

2.2.1.6. **Yönetim Kılavuzu** (COBIT Management Guidelines, 2000):

Kurumlar, başarılı olabilmek için süreçlerini bilgi teknolojilerini kullanarak en etkin şekilde otomatize etmelidirler. Yönetim kılavuzu bu otomatikleştirme işlemini izleyebilmek için olgunluk modellerini içerir. Bu modellere bakılarak belli bir anda ne durumda bulunulduğunu ve hangi adımları atmak gerektiğini belirlemek kolaylaşır. Yine bu modellere bakılarak anahtar başarı faktörleri ve performans kıstasları belirlenir. Bu faktörler ve kıstaslar kurumsal başarıda rolü olabilecek her bireyin aradığı soruların cevaplanmasını kolaylaştırır.

2.2.2. COBIT Yapısı

Yukarıda görüldüğü gibi tamamen aynı konular ile ilgilenmesine rağmen, ISO 20000 ve COBIT'in bilgi teknolojilerine bakış açısı çok farklıdır. Şekil 2.3'te COBİT'in göreceli kapsamı ve kapsanan COBİT alanları görülmektedir. Görüldüğü gibi BT Yönetiminde en geniş alan COBİT'tedir. COBİT en detaylı ve geniş standarttır. Bu standartların işleyişlerini ve kapsamlarını karşılaştırmak için pek çok tablo olsa da, bu iki standart arasındaki felsefi ve idari farkları açıklamak için yetersiz kalmaktadırlar. Farkı anlamak için bu iki standardın çıkış noktalarına bakmak yeterli olmaktadır.



	PO	AI	DS	M
ITIL	0	+	+	-
ISO/IEC 17799	0	+	+	0
COSO	+	+	0	-

(+): Değinilen Alanlar (O): Kısmen Değinilen Alanlar (-): Değinilmeyen alanlar

PO: Plan and Organise – Plan ve Organizasyon
AI: Acquire and Implement – Satınalma ve uygulama
DS: Deliver and Support – Ulaştırma ve Destek
M: Monitor - Gözlem

Şekil 2. 3: Kapsanan COBİT Alanları (http://www.bddk.org.tr)

ISO 20000 bilgi teknolojileri hizmetlerinin belirli bir hizmet seviyesinde, süreklilikte, kalitede, hızda, maliyette yürütülmesini hedeflerken, COBIT iş gereksinimlerini ve doğasını öne alarak her şeyden önce işin tarifini yapıp, bilgi teknolojileri ihtiyaçlarını buna göre şekillendirme açısından yaklaşırlar. ISO 20000'in kökeni en iyi bilgi teknolojileri uygulamaları iken COBIT bilgi

teknolojilerinin iş hedefleri hizmetinde en iyi nasıl kullanılacağını gösterir. COBIT tüm süreçlerini bilgi teknolojileri ortamına aktarmış ve iş hayatı bu bilgilerin sağlığına tamamen bağlı kurumlar tarafından tercih edilmektedir. Bankacılık Düzenleme ve Denetleme Kurumu COBIT'in tüm bankalarda uygulanması için çalışmalarına devam etmektedir.[11] COBIT, bilişim teknolojileri yönetimini bir proje yönetimi süreçlerine benzer şekilde ele almaktadır.

COBIT standardının her bir süreçte nasıl işlediği ve COBIT'in dört alanı ve bu alanlara bağlı 34 adımının nasıl işlediği daha önce anlatılanlar şu şekilde gösterilmektedir (COBIT Executive, 2000):

1. Planlama ve Organizasyon
2. Satınalma ve Uygulama
3. Ulaştırma ve Destek
4. Gözlem

2.2.2.1. Planlama ve Organizasyon

Planlama ve organizasyon aşamasında kurumların bilgi teknolojilerini kullanarak hedeflerine nasıl ulaşabileceklerine karar verilir. Bu kapsamda bilgi teknolojileri hedeflerine ulaşmak için nasıl bir organizasyon, nasıl bir altyapı ya da tesis gerektiği konuları aydınlığa kavuşturulur. Aşağıda COBIT'in 34 adımından planlama ve organizasyon bölümünde yer alan 10'u şunlardır (COBIT Executive, 2000):

1. BT stratejik planı belirlenmesi
2. Bilgi altyapısının belirlenmesi
3. Teknolojik gidişat hedeflerinin belirlenmesi
4. BT organizasyon ilişkilendirmesinin belirlenmesi
5. Yatırımın yönetilmesi
6. Yönetim hedeflerinin ve yönergelerinin paylaşılması, iletilmesi
7. İnsan kaynakları yönetimi
8. Dış gereksinimlerle uyumluluğun sağlanması

[11] http://www.bddk.org.tr/turkce/yayinlarveraporlar/sunumlar/IT_Audit_BDDK_Yaklasimi_20_4_2006.ppt

9. Risklere değer belirlenmesi
10. Proje yönetimi

2.2.2.2. Satın Alma ve Uygulama

Bir sonraki aşama, kurumların bilgi teknolojisi ihtiyaçlarını belirlemek ve iş süreçlerini bilgi teknolojileri ortamına aktarmaktır. Bu alan, aynı zamanda bilgi teknolojileri sistemlerinin bakımının doğru yapılmasını ve ömrünü uzatacak önlemleri de içerir. COBIT'in satın alma ve uygulama adımları şunlardır (COBIT Executive, 2000):

1. Çözümlerin belirlenmesi
2. Yazılımın satın alımı ve bakımı
3. Teknoloji altyapısının alımı ve bakımı
4. BT prosedürlerinin geliştirilmesi ve bakımı
5. Sistemlerin kurulumu ve yetkilendirilmesi
6. Değişikliklerin yönetimi
7. Çözüm ve değişikliklerin uygulanması

2.2.2.3. Ulaştırma ve Destek

Ulaştırma ve destek alanı bilgi teknolojilerinin kendine has özelliklerini barındırır. Bilgi teknolojisi sistemlerinde uygulamaların çalıştırılmasını, bu sistemlerin etkin ve verimli çalıştırılmalarını garanti altına almaya çalışır. Bu alan şu adımlardan oluşur (COBIT Executive, 2000):

1. Servis seviyelerinin belirlenmesi
2. Üçüncül kişi servislerinin yönetimi
3. Performans ve kapasite yönetimi
4. Servis devamlılığının sağlanması
5. Sistem güvenliğinin sağlanması
6. Harcamaların belirlenmesi ve dağıtılması
7. Kullanıcıların eğitilmesi
8. BT müşterilerinin yönlendirilmesi

9. Konfigürasyonun yönetilmesi
10. Olay ve problemlerin yönetimi
11. Verinin yönetimi
12. Araçların yönetimi
13. İşlemlerin yönetilmesi

2.2.2.4. Gözlem

Gözlem alanı belirlenmiş olan stratejik bilgi teknolojileri hedeflerine ulaşmak için mevcut altyapının hala yeterli olup olmadığını gözlemler. Gözlem aynı zamanda bağımsız olarak verimliliği ölçen bir alandır. Gözlem alanını oluşturan dört adım şu şekilde gibi sıralanmaktadır (COBIT Executive, 2000):

1. Süreçlerin izlenmesi
2. İç kontrol yeterliliğinin değerlendirilmesi
3. Bağımsız güvence temini
4. Bağımsız denetim için verilerin sunulması

2.2.3. COBIT Değerlendirmesi

COBIT özellikle denetimin ve kontrolün yasal zorunluluk olduğu kurumlarda önemlidir. Dünyada çoğu kurum, BT'nin denetlenebilir alanını tanımlamak için COBIT'ten yararlanmaktadır. COBIT, BT topluluğu tarafından anlaşılabilecek ve takip edilebilecek şekilde yazılmıştır. Sonuçta, etkili denetim kapsamını güvence altına alan stratejik planlar COBİT'le hazırlanabilir.

COBIT'in alan ve süreç yapısı, kontrol faaliyetlerini yönetilebilir ve tanımlanabilir bir yapı içinde sunuyor. Devlet gerekleri ve bilgisayar destekli denetim tekniklerinin kullanımı dahil olmak üzere, çeşitli alanları temel alan ayrıntılı denetim prosedürleri geliştiriliyor. BT alanında çalışan denetçiler uzmanlığa gereksinim duydukları için beceri değerlendirmeleri gerçekleştirmek ve denetimin başarılı şekilde yapılmasını güvence altına almak için COBIT'i kullanıyor.

Tablo 2.1'de COBİT'in BT ile ilgili alanlarda hangi süreçlerde kontrolü sağladığı açıklanmaktadır. Bütün bunların yanında COBİT ayrıca şu yaklaşımları da sergilemektedir (http://www.bddk.org.tr);

- Süreç tesisi ve denetimi odaklı
- Bütüncül yaklaşım
- Dengeli ve hiyerarşik yapılandırılmış alanlar
- Ölçme ve Derecelendirme Mekanizması
- Etkili Kurumsal Yönetişim aracı (Yönetilebilirliğin sağlaması)
- Teknolojiden bağımsız
- ISO 17799, ITIL, COSO yaklaşımlarına uygun
- AB Mevzuatında BS Denetimi çerçevesi olarak uygunluğuna onay veren düzenlemelerin olduğu bir yaklaşım sergiliyor. (http://www.bddk.org.tr)

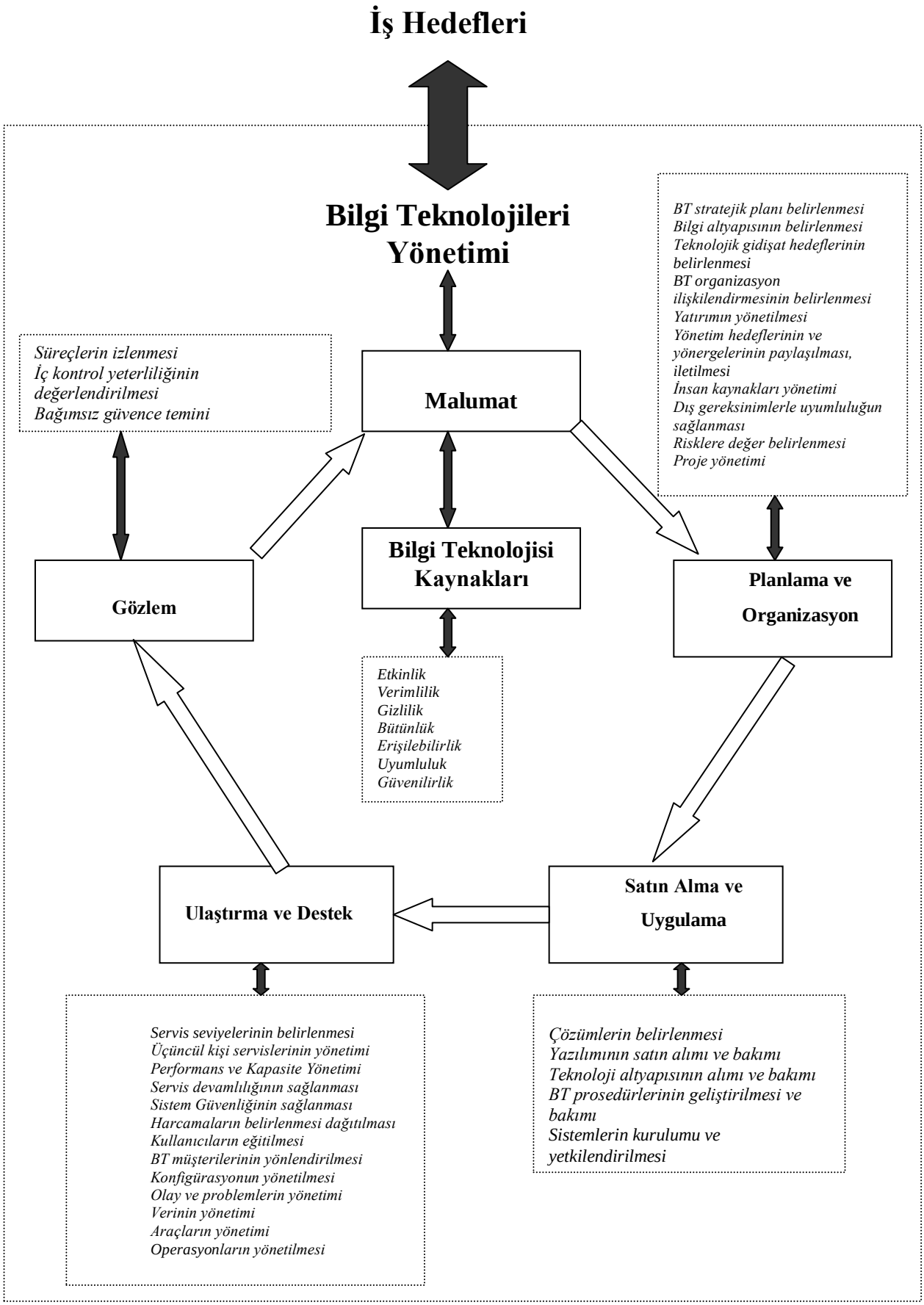
Basel II Olay Çeşitleri	BT ile ilgili alanlar	COBIT Süreçleri
İç Dolandırıcılık	• Programların kasıtlı değiştirilmesi • Değişiklik fonksiyonlarının yetkisiz kullanımı • Sistem yönergelerinin kasıtlı değiştirilmesi • Donanımın kasıtlı değiştirilmesi • Sistemin ve uygulama verilerinin Hackleme yoluyla kasıtlı değiştirilmesi • Lisansız yazılım kullanımı/kopyalanması • Erişim haklarının içeriden değiştirilmesi	• PO6 (Yönetimin amaçlarının ve talimatlarının iletilmesi) • DS5 (Sistem güvenliğinin sağlanması) • DS9 (Konfigürasyon yönetimi)
Dış Dolandırıcılık	• Sistemin ve uygulama verilerinin Hackleme yoluyla kasıtlı değiştirilmesi • Dışarıdan gelenlerin gizli fiziksel veya elektronik dökumanları görebilme imkanı bulabilmesi • Erişim haklarının dışarıdan değiştirilmesi • Haberleşme bağlantılarının kesilmesi veya dinlenmesi • Şifrelerin ele geçirilmesi • Virüsler	• DS5 (Sistem güvenliğinin sağlanması)
İstihdam Uygulamaları ve İş Ortamı Güvenliği	• BT kaynaklarının hatalı kullanımı • Güvenlik duyarlılığının düşüklüğü	• PO6 (Yönetimin amaçlarının ve talimatlarının iletilmesi) • PO7 (İnsan kaynakları yönetimi)
Fiziksel Değerlerin Zarar Görmesi	• Bilinçli veya kaza ile BT fiziksel altyapısına verilen zarar	• DS12 (Veri yönetimi)
İş Aksamaları ve Sistem Arızaları	• Donanım ve yazılım aksamaları • Haberleşme arızaları • Çalışanların sistemi sabote etmesi • Temel BT çalışanlarının işi bırakması • Yazılım/veri dosyalarının tahribi • Yazılımın veya hassas bilgilerin çalınması • Bilgisayar hataları • Sistemin geri yüklenememesi • DoS saldırısı • Konfigürasyon kontrol hatası	• DS3 (Performans ve kapasite yönetimi) • DS4 (Hizmet sürekliliğinin sağlanması) • DS5 (Sistem güvenliğinin sağlanması) • DS9 (Konfigürasyon yönetimi) • DS10 (Problem yönetimi)
Yürütme, Dağıtım ve Süreç Yönetimi	• Elektronik medyalara (CD, DVD,…) dokunma hatası • Kullanılmayan iş ortamları • Değişim kontrollerinde hata • Tamamlanmamış girdi veya transaction • Veri girdi/çıktısında hata • Programlama/deneme hatası • Operatör hatası, geri yükleme süreçlerinde mesela • Elle yapılan süreçlerde hata	• AI5 (Bilgi sistemleri kaynaklarının karşılanması) • AI6 (Değişiklik yönetimi) • DS5(Sistem güvenliğinin sağlanması) • DS10 (Problem yönetimi)

Tablo 2. 1: COBİT ve BT Denetimi

Kaynak: Information Systems Control Journal (http://www.bddk.org.tr)

COBIT standardının ülkemizde kamu kurumlarında uygulanması konusundaki en büyük risk, bu standardın bankalar gibi denetimin hayati önem taşıdığı sistemler için tasarlanmış olması, bürokratik yapının katı oluşu, güvenlik ve denetim ihtiyaçları yüzünden gerektiğinde işlevsellikten feragat edilen bir çatısı olmasıdır.

COBIT kamu kurumlarında uygulanmasa dahi, bilgi teknolojileri uygulama planlarının COBIT kontrol hedefleri ışığında değerlendirilmeleri yerinde olacaktır. COBIT şu anda uygulamada olan en geniş kapsamlı bilgi teknolojileri yönetim sistemidir. Şekil 2.4'de COBIT' in işleyişini görülmektedir. (COBİT, *Control Objective, 2000, s. 13)*



Şekil 2. 4 Dört COBIT Alanının İş hedeflerine Yönelik Akış (COBİT, *Control Objective, 2000, s. 13)*

3. 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. (Kovacich, 2003, s. 4) OODA döngüsü ismini İngilizce Observe-Orient-Decide-Act (Gözle-Yönlendir-Karar Ver-Harekete Geç) kelimelerinden alır.

Şekil 3. 1 Gözle-Yönlendir-Karar Ver-Harekete Geç Döngüsü (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 (Kovacich, 2003, s. 4).

Kurumların bilgi teknolojisi yatırımlarından hangi sonuçları bekledikleri konusunda yapılan bir araştırma güvenlik gereksinimlerine olan ihtiyacı açıklayabilecektir. Tablo 3.1'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.[12]

	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

Tablo 3. 1: Şirketlerin BT yatırımlarından beklentileri (konuların önemine 5 üzerinden verilen notlar) (ITGI, 2006)

Geleceğe yönelik bilgi teknolojileri iş planlaması ve güvenlik çalışmalarında Tablo 3.1'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)

3.1. Modern Kurum Yapısı

Her kurum bir ihtiyaçtan dolayı vardır ve bu ihtiyacı var eden de kurumların müşterileri, genel anlamda paydaşlarıdır. Çağımızın hızlı gelişen ve olaylara hızla tepki vermeyi gerektiren iş ortamının sebebi yüksek rekabet ortamında müşterilerin hizmet – mal sağlayıcılardan beklentilerinin oldukça yükselmiş olmasıdır. Bu gidiş yönünü değiştirmeyecek, ileride hizmetlerini zamanında ve istenen kalite düzeyinde veremeyen kurumlar rekabette diğer kurumların gerisinde kalacaklardır. Bu gerçek

[12] "IT Governance Global Status Report" PriceWaterhouseCoopers-ITGI, 2006

kâr amacı güden kurumlar kadar kamu ve hayır kurumları için de geçerlidir. Kâr amacı gütmeseler de bu kurumların müşterileri ve paydaşları da genel ekonomik ortamda isteklerini yükseltmektedirler. (Purser, 2004, s. 3)

Bilgiyi kullanma alışkanlıklarımızda hız faktörünü mutlaka hesaplarımızın içine katmamız gereklidir. Güvenlik klasik anlamda hız düşürücü, esnekliği engelleyici bir kavram izlenimi uyandırmaktadır. Bu, günlük işlem bazında doğru olsa da, uzun vadede risk tanımlamalarını yapmamış kurumlar beklenmedik iş kesintileri ile zor zamanlarında ayak uydurmaları gereken hızın ve rekabetin gerisinde kalacaklardır.

3.2. Bilgi Güvenliği Tanımı, 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 – Profosyonel 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.

3.2.1. Gizlilik

Gizlilik Uluslararası Standartlar Örgütü (ISO) tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" (http://en.wikipedia.org) olarak nitelenir. Bugün şifreleme altyapılarının olmasının sebebi temel olarak gizlilik, ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için eşit önemde olmayabilir. Gizlilik özellikle kamu kurumları ve bankalar gibi kuruluşlar için önemlidir.

Gizlilik, özellikle bir yasa ya da sözleşme dolayısıyla bir zorunluluk ise önemlidir. Örneğin avukat - müvekkil ilişkisi ya da doktor hasta ilişkisi gibi mesleki bilgiler kanun ile koruma altına alınmıştır. Bazı durumlarda ise taraflar birtakım bilgileri sözleşme ile birbirlerine verirlerken gizlilik anlaşmaları yaparlar. Her iki durumda da gizlilik büyük önem taşımaktadır.

3.2.2. Bütünlük

National Information Assurance'nin tanımına göre bütünlük (veri bütünlüğü) dar güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır (IA, 2006, s.34).

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 (IA, 2006, s.34);

1. Kesinlik
2. Doğruluk
3. Geçerlilik

3.2.3. Erişilebilirlik

Matematiksel olarak ifade edilirse, 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 (IA, 2006).

3.2.4. Hesap Verebilirlik

Hesap verebilirlik kişisel sorumluluğun bir ölçütüdür. 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 (IA, 2006).

Kamu kurumlarında hesap verebilirliğin en önemli yansıması şeffaflıktır. Kamu kaynaklarını kullanmakla görevli yetkililerden eylemlerini ve planlarını anlaşılabilir bir halde kamuoyu denetimine açmaları beklenmektedir.

3.2.5. 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"[13] teyit eder.

Yetkilendirme konusunda dikkat edilmesi gereken, bilgi sistemlerinde geçerli olan "en az bilgi"[14] kuralıdır. Başlangıçta askeri olan bu kural, kişilerin işlerini yapmaları için gereken en az bilgiyi bilmeleri gerektiği prensibini kurumlara benimsetmektedir.

3.2.6. 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 (ISO/IEC 13335-1);

- 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 13335-1[15] standardında da gösterilmektedir. Bu standardın tanımı itibariyle bilgi güvenliği, bilginin risk yönetimini yapmaktır.

---

[13] Bilgisayar grubunda kimlik yönetimi gibi merkezi işlevleri yapan bilgisayar sunucusu.
14 Bu kavram İngilizce olarak "Need to know" ya da "Principle of least privilege" olarak anılır.
15 ISO/IEC 13335-1 Guidelines for the management of IT Security Part 1: Concepts and models for IT Security

3.2.7. Bilgi Güvenliği İnceleme Alanları

Bilgi güvenliği kavramları CBK'da tanımlanan 10 alanda incelenir; (Hansche, 2003)

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

3.2.7.1. **Bilgi Güvenliği Yönetimi** (Hansche, 2003, S.3)

Bilgi güvenliği yönetimi başlığı isimlendirmeden de 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.[16] 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

[16] Strateji sözü eski Yunanistan'da generallere verilen "Stratagem" sıfatından gelir, güvenlik kavramlarının (şifreleme, fiziksel güvenlik, sürekli iletişim ihtiyacı vb.) hemen hepsinin kökeni askeridir.

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 "zaafiyet" 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 kaynağının yok edilmesi çoğu zaman mümkün olmadığından temel bir yöntem olarak kabul edilemez. 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.

Politikalardan bir aşağı seviyede standartlar bulunur. Bunlar kurum içerisinde hangi işin, nasıl yapılması gerektiğine dair bir kural setidir. Standartlarda temel nokta uyumluluktur. Tüm kurumun aynı işleri aynı yollar ve araçlar ile yapmasını

sağlamak için standartlar olmalıdır. Standartların kurum güvenlik politikası kadar kesin ve bağlayıcı olması gerekmemektedir. Daha aşağı seviyede ise rehberler gelmektedir. Rehberler özel bir işin nasıl yapılacağını açıklayan açıklayıcı eğitici dokümanlardır. Bu dokümanlar kurum çalışanlarının istedikleri zaman erişebilecekleri bir yerde depolanmalıdır. İşe alma ve işten çıkarma yöntemleri de güvenlik uygulamalarının bir parçasıdır. Araştırma yöntemleri uyuşturucu testi yaptırmaya kadar genişletilebilir. Kişileri işten çıkarırken ise ne yapılacağına önceden karar verilmiş ve prosedüre bağlanmış olmalıdır. Kişi işten çıkarıldığı anda tüm erişim hakları da aynı anda engellenmelidir.

Kişilerin iş tanımları kurumsal bilgi güvenliğinin önemli bir parçasıdır. Kişilerin iş adına ne yapmalarının beklendiği detaylı olarak tanımlanmalıdır. Bu tanımlamalar çerçevesinde kişilerin erişim yetkileri tanımlanır.

Kurumsal personel yönetimi ile ilgili bir diğer nokta da görev ve sorumlulukların ayrıştırılmasıdır. Kurumda çalışanlar arasındaki görev paylaşımları birbirlerini tamamlayacak şekilde yapılmalıdır. Bir konuda tüm sorumluluğun denetlenemeyecek şekilde tek kişiye verilmesi güvenlik ve işlevsellik sorunlarına yol açacaktır. Görev tanımlamaları kişilerin görevleri yedekli olacak şekilde yapılmalı, çalışanın izne ayrıldığı zamanlar, yedekliliğin ve yedekliliği sağlayacak dokümantasyonun ne kadar başarılı olduğu konusunun test edilebileceği fırsatlar olarak değerlendirilmelidir.

Güvenlik ihlalleri genellikle ihmalden kaynaklanır. Bu ihmalleri engellemek için güvenlik anlayışının çalışanlara eğitimler, seminerler, hatırlatıcı notlar olarak sürekli hatırlatılması gerekmektedir. Kurum içerisinde, sisteme girmeye yetkisi olduğu halde güvenlik politikalarının neler olduğu konusunda bilgisi olmayan bir kullanıcı olduğu sürece bu çalışmalar başarılı sayılamaz. Bu eğitim ve bilgilendirmenin içeriği ve tarzında, güvenliğin kurum işlevleri açısından gerekli olduğu bilinci uyandırılmalıdır. Çalışanlar güvenliğin kendilerine çok kuşkucu bir yaklaşımla sınırlandırmalar getirdiği inancına kapılırlar ise güvenlik politikalarına karşı çıkacaklardır. Bu tip tepkileri engellemenin en iyi yolu güvenlik çalışmalarını tabana yaymak, her türlü girdiyi değerlendirip mümkün ise olumlu ya da olumsuz karşılandığını girdi sahibine anlatmaktır. İnsanların "neden" sorusunu sıkça sormalarını teşvik etmek, her neden sorusunu güvenlik politikalarını anlatmak için

bir fırsat olarak görmek gerekmektedir. En başarılı güvenlik uygulamaları kurumun tümünün güvenlik politikalarına sahip çıktığı kurumlarda görülmektedir.

3.2.7.2. **Erişim Kontrol Sistemleri ve Yöntemleri** (Hansche, 2003, S.147)

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. Kablolama ve elektronik yayılım da fiziksel kontrol başlığı altında incelenirler. Veriyi elektrik akımı aracılığı ile taşıyan her türlü kablolama elektronik yayılım yapar ve bu elektrik yayılımının kontrol altına alınması gerekmektedir. Kurumda hizmette olan her kablolamanın ne ölçüde hassas veriler taşıdığına göre TEMPEST[17] değerlerinin düşürülmesi gerekmektedir. TEMPEST'in NATO karşılığı olan standart ise AMSG 720B'dir. Özellikle kurumlar içerisinde kritik bilginin depolandığı, önemli görüşmeler ve kararların alındığı merkezlerin TEMPEST değerleri düşürülmelidir. Ülkemizde TEMPEST ölçümleri konusunda uzman kurum, UEKAE'dir..

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

[17] TEMPEST Amerika Birleşik Devletleri'nin elektronik yayılım ile ilgili kurallar setidir

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.

Erişim kontrollerinde önemli bir nokta da gizlilik seviyeleridir. Her dokümanın veya genel anlamda kaynağın güvenlik seviyeleri olmalı ve sadece o güvenlik seviyesi için yetkisi olan kişiler o kaynağa ulaşabilmelidir.

Kişi bir kaynağa erişmeye çalıştığında sistem ilk olarak ulaşmaya çalışanın kim olduğunu anlamaya çalışır. Kişinin iddia ettiği kimse olup olmadığını kontrol etmek için sistem ya sadece o kişinin bilebileceği bir şeyi, sadece o kişinin olabileceği bir şeyi ya da sadece o kişinin taşıdığı bir şeyi ibraz etmesini bekler. Bilebileceği şeye örnek şifre ya da PIN (Personal Identification Number - Kişisel Tanımlama Sayısı) (http://en.wikipedia.org) numarası, olabileceği şeye örnek ses

veya göz retinası yetkilendirmesi, taşınan bir şeye örnek ise akıllı kartlardır. Basitçe yetkilendirme için kullanılan araçlar bunlardan oluşmaktadır.

Kaynaklara erişilirken yukarıdaki özellikleri kullanan ve yöneten denetleyici alt sistemleri incelemek gerekirse iki değişik yaygın kullanımlı ürünün özelliklerine bakmak yeterli olacaktır. Birincisi Microsoft Windows ürünlerinde de kullanılan Kerberos[18] sistemidir. Simetrik anahtar yapısı kullanan[19] bu sistem, kaynağa ulaşılmaya çalışıldığında kişinin iddia ettiği insan olduğunu onaylar ise, bu onaya binaen kişiye bir erişim bileti verir. Bu elektronik bilet ile kişi yetkisi çerçevesinde kaynaklara ulaşabilir. Bir diğer sistem ise adı SESAME (Avrupa Çok Kaynaklı Uygulamalar Ortamında Güvenlik Sistemi - Secure European System for Applications in a Multivendor Environments) olan ve Kerberos'tan daha güvenli olmak için yapılmış bir erişim kontrol sistemidir. SESAME, yetkilendirdiği kullanıcıya bir bilet anahtar yerine bir elektronik sertifika gönderir. Yukarıda sayılan iki sistem de bir kere yetki verdiği kişi başka kaynaklara ulaşmak istediğinde yeniden yetkilendirme istemeyecek şekilde programlanabilir. Bu programlamaya "Tek Giriş" (SSO - Single Sign On) özelliği denir.

Erişim sistemlerinde son olarak erişim saldırı sistemleri ele alınmalıdır. Saldırı tiplerinden en başta geleni kaba kuvvet saldırısıdır (brute force attack). Kaba kuvvet saldırısında bir kaynağın sahip olabileceği tüm şifre kombinasyonları denenir. Kaba kuvvet saldırısı yeterince uzun bir zaman içerisinde yüzde yüz başarı şansı olduğu için saldırganlar tarafından tercih edilmektedir. Bir diğer saldırı yöntemi ise sözlük saldırısıdır. Şifre olması muhtemel sözcükler belli bir kelime hazinesinden seçilip şifre tahmini yapılmaya çalışılmasıdır. Hizmet reddi saldırısı[20] ise pek çok sahte talep yapıp hizmet kaynaklarını sonuna dek sömürerek dolaylı yoldan hizmet verilmesini engellemektir. Ortadaki adam saldırısı[21] bir şifre mesajlaşmasında mesajın kaynaktan sunucuya gelmesini engelleyerek içeriğini değiştirerek mesajlaşmanın içeriğini çözmeye çalışmaktır.

Saldırıları engellemek için gözlem çok önemlidir. Her şifre girişi ve her kaynak kullanma isteminin kayıt altına alınması gözlemi kolaylaştıracaktır. Diğer bir

[18] Kerberos Yunan mitolojisinde ölüler dünyası ve yaşayanlar dünyası arasında bekçilik yapan üç başlı bekçi köpeğinin adıdır.
[19] Bkz. 3.2.7.5. s.41
[20] Denial of Service, DoS
[21] Man in the Middle Attack

yöntem ise bal çanağı denen, kolayca içine girilebilen sahte giriş sistemleri yapmaktır. Muhtemel saldırganlar gerçek sistem ile bu sahte sistem arasındaki farkı kısa sürede anlayamayıp oraya konulacak sahte kaynaklara eriştiklerini sanacaklar, bu sırada ise hareketleri ve niyetleri anlaşılabilecektir. Saldırılara verilebilecek bir diğer yanıt ise saldırı tespit sistemleridir. Giderek daha akıllı hale gelen bu sistemler şüpheli kaynaklardan gelen istekleri cevaplamayı reddetmekten, karşı saldırı yapmaya kadar pek çok cevap verebilmektedirler. Saldırılardan korunmak için en önemli pasif korunma ise zaafiyet testi analizleridir. "Zaafiyet testleri" kurumların sistemlerinde gerçek bir saldırı taklit edilerek zaafiyeti olup olmadığının anlaşılmasıdır.

3.2.7.3. Telekomünikasyon, Bilgisayar Ağları ve İnternet Güvenliği

(Hansche, 2003, S.515)

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. Modern iletişim sistemlerinin hemen hepsi OSI modelini referans almaktadır. 1984 yılında ISO'nun tanımladığı OSI modelinin detayları şu şekilde verilmektedir.[22] OSI kavramsal bir modeldir. Yani hiçbir yerde OSI programı veya OSI donanımı diye bir şey yoktur. Ancak yazılım ve donanım üreticileri bu modelin tanımladığı kurallar çerçevesinde üretim yaparlar ve ürünleri birbiri ile uyumlu olur.

OSI'nin yedi katmanı bulunmaktadır ve bu katmanların işlevleri aşağıdaki başlıklar halinde incelenmektedir. (ISO 7498:1984)

1. Katman : Fiziksel Katman:

1. katman veya fiziksel katman verinin kablo üzerinde alacağı fiziksel yapıyı tanımlar. Fiziksel katman bu tip çözülmesi gereken problemleri tanımlamıştır. Üreticiler (örneğin ağ kartı üreticileri) bu problemleri göz önüne alarak aynı değerleri kullanan ağ kartları üretirler. Böylece farklı üreticilerin ağ kartları birbirleriyle sorunsuz çalışırlar.

[22] ISO 7498:1984 Open Systems Interconnection - Basic Reference Model

Katman 2: Veri Bağlantısı Katmanı:

Veri bağlantısı katmanı fiziksel katmana erişmek ve kullanmak ile ilgili kuralları belirler. Veri bağlantısı katmanının büyük bir bölümü ağ kartı içinde gerçekleşir. Veri bağlantısı katmanı ağ üzerindeki diğer bilgisayarları tanımlama, kablonun o anda kimin tarafından kullanıldığının tespiti ve fiziksel katmandan gelen verinin hatalara karşı kontrolü görevini yerine getirir.

Veri bağlantısı katmanı iki alt bölüme ayrılır; MAC (Media Access Control) ve LLC (Logical Link Control).

MAC alt katmanı veriyi CRC (hata kontrol kodu, Cyclic Redundancy Check) ile alıcı ve gönderenin MAC adresleri ile beraber paketler ve fiziksel katmana aktarır. Alıcı tarafta da bu işlemleri tersine yapıp veriyi veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir.

LLC alt katmanı bir üst katman olan ağ katmanı (3. katman) için geçiş görevi görür. Protokole özel mantıksal portlar oluşturur (Service Access Points, SAPs). Böylece kaynak makinede ve hedef makinede aynı protokoller iletişime geçebilir (örneğin TCP/IP<-->TCP/IP). LLC ayrıca veri paketlerinden bozuk gidenlerin(veya karşı taraf için alınanların) tekrar gönderilmesinden sorumludur. Flow Control yani alıcının işleyebileceğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir.

Katman 3: Ağ Katmanı:

Ağ katmanı veri paketine farklı bir ağa gönderilmesi gerektiğinde yönlendiricilerin kullanacağı bilginin eklendiği katmandır. Örneğin IP (Internet Protocol – İnternet protokolü) protokolü bu katmanda görev yapar.

Katman 4: Taşıma Katmanı:

Taşıma katmanı üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler. NetBEUI (NetBIOS Extended User Interface – Uzatılmış Kullanıcı Arabirimi), TCP (Transmission Control Protocol – İletim Denetimi Protokolü) ve SPX (Sequenced Packet Exchange – Sıralanmış Paket Değişimi) gibi protokoller bu katmanda çalışır. Bu protokoller hata kontrolü gibi görevleri de yerine getirir.

Taşıma katmanı alt katmanlar (Transport Set) ve üst katmanlar (Application Set) arasında geçit görevini görür. Alt katmanlar verinin ne olduğuna bakmadan karşı

tarafa yollama işini yaparken üst katmanlarda kullanılan donanım ile ilgilenmeden verinin kendisi ile uğraşabilirler.

Katman 5: Oturum Katmanı:

Oturum katmanı bir bilgisayar birden fazla bilgisayarla aynı anda iletişim içinde olduğunda, gerektiğinde doğru bilgisayarla konuşabilmesini sağlar. Örneğin A bilgisayarı B üzerideki yazıcıya yazdırırken, C bilgisayarı B üzerindeki diske erişiyorsa, B hem A ile olan, hem de C ile olan iletişimini aynı anda sürdürmek zorundadır. Bu katmanda çalışan NetBIOS gibi protokoller farklı bilgisayarlarla aynı anda olan bağlantıları yönetme imkanı sağlarlar.

Katman 6: Sunum Katmanı:

Sunum katmanının en önemli görevi yollanan verinin karşı bilgisayar tarafından anlaşılabilir halde olmasını sağlamaktır. Böylece farklı programların birbirlerinin verisini kullanabilmesi mümkün olur. Dos ve Windows 9x metin tipli veriyi 8 bit ASCII olarak kaydederken (örneğin A harfini 01000001 olarak), NT tabanlı işletim sistemleri 16 bit Unicode'u kullanır (A harfi için 0000000001000001). Ancak kullanıcı tabii ki sadece A harfiyle ilgilenir. Sunum katmanı bu gibi farklılıkları ortadan kaldırır.

Sunum katmanı günümüzde çoğunlukla ağ ile ilgili değil, programlarla ilgili hale gelmiştir. Örneğin eğer siz iki tarafta da gif formatını açabilen bir resim gösterici kullanıyorsanız, bir makinenin diğeri üzerindeki bir GIF dosyayı açması esnasında sunum katmanına bir iş düşmez, daha doğrusu sunum katmanı olarak kastedilen şey, aynı dosyayı okuyabilen programları kullanmaktır.

Katman 7: Uygulama Katmanı

Uygulama katmanı programların ağı kullanabilmesi için araçlar sunar. Microsoft API'leri (Application Programming Interface - Uygulama Yazılım Arabirimi) uygulama katmanında çalışır. Bu API'leri kullanarak program yazan bir programcı, örneğin bir ağ sürücüsüne erişmek gerektiğinde API içindeki hazır aracı alıp kendi programında kullanır. Alt katmanlarda gerçekleşen onlarca farklı işlemin hiçbirisiyle uğraşmak zorunda kalmaz.

Uygulama katmanı için bir diğer örnek HTTP'dir. HTTP (HyperText Transport Protocol) çalıştırılan bir program değil bir protokoldür. Yani bir kurallar

dizesidir. Bu dizeye göre çalışan bir internet tarayıcı (İnternet Explorer gibi), aynı protokolü kullanan bir web sunucuya erişir.

Güvenlik önlemlerini alabilmek için bilişim ağlarının hangi sistemler ve yöntemlerle birbirleri ile haberleşmeleri gerektiğini anlamak önemlidir. Her gün kullanmakta olduğumuz bilgi ağlarından yararlanırken yukarıdaki katmanların hepsini kullanmaktayız. Bu katmanlarda gerçekleşen olayların anlaşılması ile güvenliğin hangi katmanda alınacağına karar verilebilir. Örneğin şifreleme yapılırken, IPsec (Internet Protocol Security - internet protokol güvenlik standardı) isimli şifreleme 3. katmanda yapılırken, banka işlemleri yaparken kullanılan SSL şifrelemesi 7. katmanda yapılmaktadır. Uluslararası internet altyapısı tamamen 3. ve 4. katmanlarda çalışmaktadır.

Kurumların ihtiyacına göre çalışan uygulamaların birbirleri ile iletişim katmanları göz önüne alınarak uygun güvenlik önlemleri alınmalıdır. Örneğin iki bina birbiri ile 3. katmanda bağlanacak ise IPSec protokolü kullanılarak şifreleme yapılması, kullanıcılar iş bilgisayar ağına bağlanacaklar ise VPN (Virtual Private Network - Sanal Özel Ağ) kullanılarak gene 3. katmanda internet üzerinden kurum ağına tünel açılması, kurumların internete ya da kurum dışı ağlara açıldığı noktalara ise ateş duvarları (firewall) tesis edilmesi gerekmektedir. Tüm bunlar ihtiyaca göre tasarlanması gereken yapılardır.

Ateş duvarı tanımlaması, binalar tasarlanırken yangın ihtimaline karşı binalarda korunaklı alanlar tasarlanmasından gelmektedir. Yangına dayanıklı duvarların oluşturulması ile binalarda yangın durumlarında insanların sığınabileceği alanlar oluşturulmaktadır. Binalardaki benzetme örnek alınarak bilgisayar ağları sınırlarında alınan güvenlik önlemine de ateş duvarı ismi verilmiştir. Ateş duvarlarının yapılandırması ve seçilecek teknoloji de dokümante edilerek tanımlanmış tehditlerin türüne göre seçilmelidir.

Bilgisayar ağlarının ne amaçla ne yoğunlukta kullanıldığı sürekli kontrol altında tutulmalı, bu raporlamalar otomatik hale getirilip değerlendirilmelidir. İletişim ağlarının hepsinin güvenlik kıstasları göz önüne alınarak tasarlanması gerekmektedir. Bilgi yollarında da aynı fiziksel yollarda olduğu gibi bazı trafik kuralları olması, yolları da ehliyetsiz kişilerin kullanmasının engellenmesi gerekmektedir. Bu ağlardan en önemlilerinden biri ses ağlarıdır. Kurumlarda ses

iletişimi için kullanılan telefon ağlarının aynı anda izin verilmeyen veri iletişimi için kullanılmamaları gerekmektedir. Örneğin kurumsal bilgisayar ağına bağlı bir bilgisayarın aynı anda modem aracılığı ile telefon üzerinden internete ulaşması, kurumsal bilgi ağını devre dışı bırakıp alınmış güvenlik önlemlerini etkisiz bırakarak önemli bir zaafiyet ortaya çıkaracaktır. Faks kullanımı da şifrelenmeyen güvensiz bir standart olması nedeni ile kullanımına ancak gizli sınıflamasının altındaki veriler için izin verilmelidir.

E-posta güvenliği, iletişim standartlarında önemli bir yer tutmaktadır. Giderek daha fazla iş amaçları için kullanılan e-posta standardı güvenlik standartları göz önüne alınarak tasarlanmadığı için fazladan güvenlik önlemlerini almak gerekmektedir. Bu fazladan güvenlik önlemlerinin amacı, inkar edilemezliği ve kaynağın gerçekten iddia edilen kaynak olduğunun temininin sağlanmasıdır. Bugün kullanılmakta olan e-mail standardı o kadar eskidir ki, internete bağlı her kullanıcı başka biri olduğunu iddia ederek üçüncü bir tarafa mail atabilmektedir. Uzman olmayan bir göz bu kaynağın kökenini anlamadan yanlış fikre kapılabilecektir. E-mail konusunda önemli bir husus da "spam" denilen gereksiz postaların süzülmesidir. Kurumlar gereksiz posta süzmek için mutlaka bir çözüm kullanmalıdırlar, Aksi halde kurum kaynaklar boşuna kullanılmış olacak ve verimlilik düşecektir.

İnternet saldırılarının hepsi bu alan kapsamında incelenmektedir. Saldırı olarak sayılmasa da bilgisayar ağlarının amaç dışı kullanımı altı seviyede incelenebilir.

- A tipi amaç dışı kullanım, yetki olmadan belli ağ kaynaklara ulaşılmasıdır.
- B tipi amaç dışı kullanım, iş dışı amaçlarla bilgisayar ağının kullanımıdır. Bu tip kullanım özellikle güvenlik politikalarına aykırı olarak yapılırsa ciddi sonuçlara yol açabilir.
- C tipi amaç dışı kullanım, başkalarının iletişimini dinlemektir.
- D tipi yanlış kullanım, belli bir hizmeti kesintiye uğratmaktır.
- E tipi yanlış kullanım, erişim kontrol sistemlerini atlatarak yetkisi olmadan ağ kaynaklarına ulaşmaktır. A sınıfından farkı, erişim kontrol sisteminin devre dışı bırakılmasıdır.

- F tipi yanlış kullanım ise bazı ağ kaynaklarının zaafiyet ararcasına taranmasıdır.

3.2.7.4. Uygulama Yazılımı Güvenliği

Günümüz bilişim ortamında pekçok 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. Yazılımlar geliştirilirken dikkat edilmesi gereken, uyumluluğu ve takip edilebilirliği teminen kabiliyet olgunluk modellerinin (Capability Maturity Model, CMM) ya da benzeri sistematik yaklaşımların kullanılmasıdır.

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.

Verilerin nerede tutulduğu, nasıl yedeklendiği ve kapasite yönetimi gene bu alanda incelenmektedir. Verinin depolanmak için hangi ortamlardan geçtiği tek tek incelenerek tehditler belirlenmelidir. Veri depolanırken alınması gereken temel önlem, veri depolandıktan sonra ihtiyaç olduğunda geri alınabileceğinden emin olunmasıdır. Veri depolama sistemleri hakkında ihtiyaçlar "İş Süreklilik Planı" bölümünde daha detaylı anlatılmaktadır.

3.2.7.5. Şifreleme (Kriptografi) (Hansche, 2003, S.377)

Şifreleme, bilişim güvenliğinin en önemli alt gereksinimlerinden birini oluşturmaktadır. Şifreleme, uygun anahtarı olmadan kimsenin çözemeyeceği şekilde mesajların dönüştürülmesidir. Şifreleme özellikle Avrupa Birliği'nin Amerika Birleşik Devletleri'nin o zamana kadar varlığı bile tartışılan iletişim dinleme ve şifre çözme sistemi ECHELON üzerine rapor yazması[23] ile her zamankinden daha önemli bir güvenlik gündem maddesi olmuştur. Bu raporunda Avrupa Birliği, ABD'yi diğer ülkelerin mesajlaşmalarını ABD şirketlerinin ticari avantajına kullanmakla suçlanmakta ve tüm Avrupa Birliği vatandaşlarına ve kurumlarına ECHELON sisteminin çözemeyeceği şifreler kullanılmasını tavsiye etmektedir. Bu rapor sonucunda Avrupa Birliği, herhangi bir dinlemenin iz bırakıp anlaşılabileceği "Kuantum Şifrelemesi Tekniklerini" (http://www.secoqc.net) araştırmaya başlamıştır. ECHELON sisteminin var olup olmaması bir yana, Avrupa Birliği gibi ciddi bir örgütün bu konuda önlem almaya başlayıp araştırmalarına hız vermesi dünyanın geri kalanında da şifreleme konusunu giderek daha güçlü şifreleme algoritmaları kullanmaya itmektedir.

Müttefik kuvvetlerin 2. Dünya Savaşı'nda merkez kuvvetlerin şifrelerini kırmayı başarmaları savaşı daha kolay kazanmalarını sağlamıştır. O zamandan bu yana şifre sistemleri çok gelişmiştir. Şifre sistemleri bugün bilgi sistemlerinin gizliliğini ve bütünlüğünü garanti altına almak için kullanılmaktadır. 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 "anahtardır". Anahtar bir dizi rasgele bir ve sıfırdan oluşmaktadır. İkili sistemde gösterilen bu anahtarın uzunluğu şifrenin gücünü belirler. Bu uzunluklar genelde ikinin üsleridir ve şifreleme algoritmaları ile özdeşleştirilmiştir. Her algoritmanın yanında kaç bit anahtar ile çalıştığı genelde belirtilir.

Pek çok şifreleme sistemi olmasına rağmen modern şifrelemeler genel olarak ikiye ayrılabilir. Birinci yöntem simetrik şifreleme yöntemleridir. Simetrik şifreleme yöntemlerinde aynı anahtar şifrelenmiş metni açmak hem de metni şifrelemek için

[23] European Parliment Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), 11 Temmuz 2001

kullanılır. Bu özel bir anahtardır ve şifrenin gizliliği özel anahtarın gizliliğine bağlıdır. Simetrik şifreleme hızı dolayısı ile tercih edilmesine rağmen esnek bir sistem değildir. Şifreleme gerçekleştikten sonra aynı şifrenin karşı taraftan çözülebilmesi için anahtarın da aktarılması ihtiyacı esnekliği ortadan kaldırmaktadır.

İkinci tür şifreleme tekniği açık anahtar altyapısını kullanır. Bu tip şifrelemede her kullanıcının bir genel bir de özel anahtarı vardır. Mesaj kime gönderilmek isteniyorsa onun genel anahtarı ile şifrelenir. Bu şifrelenen mesaj şifrelemek için kullanılan genel anahtar ile geri açılamaz, sadece kullanıcıda bulunan özel anahtar ile mesaj açılabilir. Genel anahtar altyapısı esnekliği büyük oranda artırsa da şifreleme hızı daha düşüktür.

Genel anahtar altyapısının inkâr edilemezliği sağlaması için sayısal sertifikalar kullanılmaktadır. Sayısal sertifikalar kişinin genel anahtarına kişi ile ilgili özel bilgileri de eklerler. Bu bilgiler kişinin açık ismi, adresi gibi bilgileri olabilir. Kişi sadece genel anahtarından ve özel bilgilerinden oluşan sertifikayı dağıtması için bir sertifika yetkilisinden hizmet almak zorundadır. Sertifika yetkilisi bu anahtarı isteyen her kullanıcıya dağıtmak ile yükümlüdür. Kişi özel anahtarını ise kimseye vermez, özel ve genel anahtarlarını tercihen kendisi oluşturur.

Özetleme algoritmaları da inkâr edilemezlikte[24] önemli görevler yapmaktadır. Özetleme algoritmalarının görevi mesajların bütününü şifrelemek değil, mesajın ya da özetlenen verinin uzunluğundan bağımsız olarak sabit uzunlukta ve sadece o veriden elde edilebilecek bir seri veri elde edilmesidir. Şifrelenen mesaj bir harf uzunluğunda ya da gigabaytlarca uzunlukta olsa da özetleri aynı uzunluktadır. Şifrelenen mesaj gigabaytlarca uzunlukta dahi olsa ve içinde sadece bir bayt değişmiş dahi olsa özet sonuçları tamamen farklı olacaktır. Birlikte çalışabilirlik esasları kamu tarafından SHA algoritmasının özetlemede kullanılmasını esas olarak belirlemiştir.

Şifreleme yöntemlerinin en önemlilerinden biri DES (Digital Encryption Standart) algoritmasıdır. 1977'de ABD yönetimi tarafından tüm kamu iletişiminde standart olarak belirlenen bu algoritma simetrik anahtar altyapısı kullanır. 64 bit anahtar kullansa da 8 bit kontrol paritesi olduğu için 56 bit olarak değerlendirilir. DES'in dört değişik çalışma modu vardır. Bu çalışma modlarını incelemek şifreleme

[24] Uluslararası literatürde bu kavramların İngilizce'lerini takip etmek daha kolay olacaktır. İnkar edilemezlik= Non-repudiation

sistemlerinin de nasıl çalıştığı konusunda fikir verecektir. Birinci mod, elektronik kod kitabı (ECB - Electronic Codebook) olarak adlandırılır ve en zayıf DES şifreleme modunu oluşturur. Bu modda her 64 blokluk mesaj alınıp anahtar ile DES'e özel algoritmik işlem yapılarak şifrelenir. Güvenlik bir aşama artırılmak istendiğinde şifre blok zincirlemesi (CBC - Cipher Block Chain) denilen mod kullanılabilir. CBC DES algoritması kullanılmadan önce mesajı "xor" mantıksal işleminden geçirir. Bir aşama daha yüksek şifreleme ise Şifre Geri Besleme Modu (CFB - Cipher Feedback Mode) denilen moddur. Bu modda bir önceki bloktaki şifrelenmiş mesaj ile şifrelenmemiş mesaj xor işlemine tabi tutulur ve daha sonra şifreleme algoritması bu veri üzerinde gerçekleştirilir. Son yöntem ise Çıktı Geri Besleme Modu'dur (OFB - Output Feedback Mode). Bu mod şifre geri besleme moduna benzemekle birlikte aradaki fark şifreleme için bir de çekirdekleme denilen ek bir yöntemin kullanılmasıdır. Tüm bu yöntemler şifreyi çözmeyi zorlaştırmak için alınan fazladan önlemlerdir.

Zaman içerisinde DES şifreleme yöntemi, artan bilgisayar hızları karşısında zayıf kalmıştır. Bu gelişmeye karşı güncel olarak DES değil, DES'in 3 kere aynı algoritma ile kullanılmasını sağlayan 3DES şifreleme yöntemi kullanılmaktadır. Üç defa 3 değişik simetrik anahtarın kullanımından dolayı 3DES 168 bitlik bir şifreleme yöntemi olarak ortaya çıkmaktadır.

DES'e alternatif bir çok şifreleme algoritması geliştirilmiştir. Bunlardan Uluslararası Veri Şifreleme Algoritması 128 bit anahtar kullanmaktadır. 128 bitlik anahtar 16 bitlik 52 adet anahtar[25] haline bir algoritma ile dönüştürülerek veri 64 bitlik bloklar halinde her defasında 16 bitlik şifrelerlerle tekrar tekrar şifrelemektedir. Blowfish ise 32 bitten 448 bite kadar şifreleme yapabilen DES'e alternatif olarak planlanmış bir diğer şifreleme algoritmasıdır. Skipjack olarak adlandırılan şifreleme algoritması ise 80 bitlik anahtarlar ile 64 bitlik mesaj bloklarını şifreleyen bir algoritmadır.

DES'e en büyük alternatif simetrik anahtarlı şifreleme ise AES'dir. Gelişmiş Şifreleme Sistemi anlamına gelen AES (Advanced Encryption Standart), Rijndael algoritmasına dayanmaktadır. 128, 192 ya da 256 bitlik anahtarlar kullanılır. Şifreleme mesajları üç defa, çizgisel olarak ve çizgisel olmayan şekilde dönüştürdükten sonra Rijndael algoritması ile anahtarı kullanarak mesajı dönüştürür.

[25] şifrenin gücü tek bir anahtarı algoritma ile çoğaltmasından kaynaklanmaktadır.

AES şu anda kullanılan en güçlü şifreleme sistemlerinden biridir. Birlikte çalışabilirlik esasları AES'yi standart kurumsal şifreleme algoritması olarak seçmiştir.

Asimetrik şifreleme algoritmalarının en ünlüleri ise RSA ve El Gamal şifreleme sistemleridir. RSA, şifreleme sistemini bulan bilim adamlarının adlarının baş harflerinden oluşmaktadır. Şifreleme için çok büyük asal sayılar kullanmaktadır. El Gamal şifreleme sistemi ise şifreleme için çok büyük tam sayılar ve modüler aritmetik kullanmaktadır. Yeniden hatırlatmak gerekirse asimetrik şifreleme sistemleri şifreleme için genel anahtarı kullanırlar, bu şifreleme ancak kullanıcının özel anahtarı ile açılabilmektedir.

Şifrelemenin ilgilendiği bir diğer alan ise sayısal imzalardır. Yukarıda anlatılan özetleme algoritmaları ve sayısal sertifikaların özel bir kullanımı olan sayısal imzalar asimetrik anahtar altyapısını kullanırlar. Kişi, arzu ettiği dokümanı kendi özel anahtarını barındıran sertifikası ile imzaladığında dokümana sertifikada bulunan bilgiler ve özel anahtar ile üretilmiş özet bilgisi eklenir. Bu dokümanın gerçekten iddia eden kişiler tarafından imzalandığından emin olmak isteyen bir kişi imza sahibinin sertifika otoritesinden temin ettiği genel anahtarını kullanarak bu kontrolü gerçekleştirebilir. 5070 sayılı elektronik İmza Kanunu[26] ülkemizde 2004 yılından itibaren yürürlüktedir ve bu kanuna göre elektronik imza, ıslak imza ile aynı kanuni bağlayıcılığa sahiptir.

3.2.7.6. **Kurumsal Güvenlik Mimarisi** (Hansche, 2003, S.79)

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 İngilizce baş harflerinden oluşan DMZ (DeMilitarized 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

[26] 5070 Sayılı "Elektronik İmza Kanunu" Kanun No. 5070 Resmi Gazete Sayı: 25355, 23/01/2004

tutulurlar. Bir diğer tanım ise Kaynak Gözlemleyicisi (Referance Monitor) 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.

Kurumların güvenliğe ne kadar önem verdikleri ve ne kadar güvenli olduklarını ölçmek için hazırlanmış bazı modeller vardır. Bunlardan birincisi Turuncu Kitap olarak anılmaktadır. Bu kitap kapağının turuncu basılmasından dolayı verilen bu isimlendirmenin dışında TCSEC[27] (Güvenilen Bilgisayar Sistemleri Değerlendirme Kıstasları - Trusted Computing Systems Evaluation Criteria) olarak daadlandırılmaktadır. 1985 basımlı ve ABD Savunma Bakanlığı kaynaklı bu kitabın amacı, bilgisayar sistemlerinin güvenilirliğini ve işlevselliğini ölçmektir. En düşük seviyeden başlamak gerekirse, Seviye D en az korumayı belirtir. Hiçbir gruba girmeyen sistemler bu seviyeye girerler. Bir sonraki seviye ise "Sağduyulu Koruma Seviyesi" (Discretionary Protection System) olarak adlandırılan C seviyesidir. C seviyesi kendi içinde de ikiye ayrılır. C1 seviyesi erişim haklarını kişi veya gruplara verirken, C2 seviyesi erişim haklarını sadece kişilere verir ve medyaları (kaydedilebilir diskler) temiz tutma zorunluluğu getirir. Seviye B "Zorunlu Seviye (Mandatory Protection) olarak adlandırılır. Bu kategori de kendi içinde üçe ayrılır. "Etiketli Güvenlik" (Labeled Security) olarak adlandırılan B1 seviyesi, C2'ye ek olarak her dökümana ve diskete bir güvenlik seviyesi etiketlemesi yapılmasını şart koşar. B2 seviyesi ise "Yapısal Koruma" olarak adlandırılır. B1 seviyesine ek olarak bilgisayarların normal bilgisayar ağı dışında hiçbir yolla dışarı ile bağlantı kuramaması kuralını getirir. B3 Seviyesi "Güvenlik Alanları" (Security Domains) ismini taşır ve iş ile ilgisi olmayan hiçbir sürecin sistemde olmamasını şart koşar. A1 seviyesinde güvenli bir bilgisayar sistemi "Kontrol Edilmiş Koruma" (Verified Protection) seviyesine sahiptir ve olabilecek en güvenli sistemdir. Bu sistem yapılandırmasında izin verilen dışında hiçbir yazılımın sisteme girmemesi şart koşulur.

[27] Department Of Defence Trusted Computer System Evaluation Criteria, 15/08/1983

TCSEC turuncu kitabına daha sonra bilgisayar ağları korunması kriterleri için kırmızı kitapda ve diğer başka kriterler için mavi ve sarı kitaplar eklenmiş ve tüm seriye gökkuşağı serisi (http://en.wikipedia.org) denmiştir. TCSEC karşılığında Avrupa'da ITSEC (Information Technology Security Evaluation Criteria) kıstasları oluşturulmuştur. ITSEC sadece bilgisayar sistemlerini değil, bir yazılımın da ne kadar güvenli yapıldığını derecelendiren bir kıstas sistemidir. Ancak ITSEC yerini bir süre sonra ISO 15408 - Ortak Kriterler'e bırakmıştır. ITSEC gibi Ortak Kriterler de yedi aşamalı güvenlik kıstasları ortaya koymuştur. Ortak kriterler bilgisayar ve ağ güvenliğinden çok bilgisayar ürünlerinin güvenli olup olmadıklarını sertifikalandırır. Ortak kriterlerin belirttiği kıstaslar bu tezin kapsamı dışında değerlendirildiğinden burada daha uzun bahsedilmeyecektir. Bu çalışmanın yapıldığı tarih itibariyle yedi ortak kriter seviyesinden en fazla 4. güvenlik seviyesinde ürünler bulunmaktadır.[28] Daha sonra ise güvenlik modelleri gelmektedir. Kurumlar, değişik ihtiyaçlardan kaynaklanan kurum içi güvenlik modelleri oluşturmuşlardır. Bu modellerden altısından burada bahsedilecektir.(http://www.commoncriteriaportal.org)

1. Makinesi (State Machine) modeli: Durum makinesi diğer modeller içinde temel oluşturduğu için anlaşılması önemlidir. Durum makinesi modeline göre bir sistemde tanımlı tüm nesneler farklı, fakat hepsi güvenli olan durumlarda bulunabilirler. Makinenin tek yapması gereken objelerin değişik güvenli durumlar arasında nasıl durum değiştireceğini bilmesidir. Aslında her gün kullandığımız bu durum belki de fazla basit bir mantığı anlatmaya çalıştığı için algılanması ilk başta zor olabilir. Burada anlatılmak istenen, örneğin bilgisayarda paylaşım verilen bir nesne erişilmeden dururken, bir kullanıcı eriştiğinde durum değiştirilmiş olur. Bu iki durumda güvenli durumlardır. Birinde zaten erişim yoktur, diğerinde yetkilendirilmiş bir kişi nesneye erişmiştir.

2. Bell-LaPadula modeli: Sadece güvenliğe önem veren bu model ABD Savunma Bakanlığı kaynaklıdır. Bu modelde hiç kimse yetki seviyesinden yukarıda bilgilere ulaşamaz (yukarı seviye okuma yasaktır). Yine hiç kimse kendi gizlilik seviyesindeki bilgileri daha aşağı güvenlik seviyesinde bulunan sistemlere gönderemez. Burada gizli belgelerin dışarı kaçırılmaması esas tutulmuştur.

3. Biba modeli: Özellikle veri bütünlüğünün bozulmasına karşı geliştirilmiş bir modeldir. Biba modeli verinin içeriğinin değiştirilmemesi için önlemler alır. Biba

[28] Bu ürünlerin neler olduğu ve listesi http://www.commoncriteriaportal.org adresinde bulunabilir.

modelinde ilk kural “hiç kimse daha aşağı güvenlik seviyesinde bulunan bilgileri okuyamazdır.” Hiç kimse de yukarı bilgi yazamaz. Bu modelin gereksinimlerini anlamak zaman alabilir. Anlaşılması gereken bu modelde gizlilik değil, verilerin içeriğinin değişmemesi esastır.

4. Clark-Wilson modeli: Ticari uygulamalar için geliştirilen bu model de Biba modeli gibi bütünlüğe önem verir. Durum makinesi kullanmayan bu sistem tek tek nesnelere erişimi kısıtlar. Makinelerde farklı güvenlik durumları, gizlilik konumları yoktur. Nesnelerin bütünlüğü düzenli olarak kontrol edilir ve nesnelerin güvenlik seviyeleri ancak belli bir prosedür sonucunda değiştirilebilir.

5. Bilgi akışı modeli: Bell-LaPadula ve Biba modelleri kısıtlanmış bilgi akışı modelleri iken, bilgi akışı modeli bilginin nereden nereye aktığına bakmaz. Baktığı tek yer, tanımlı bir matris yapısı içinde bilginin oraya aktarılıp aktarılamayacağıdır.

6. Model ise girişimsizlik modeli: Bu model güvenlik seviyelerinin birbirlerinden soyutlanmasını esas alır. Önem verdiği en kritik nokta bir güvenlik seviyesinde olan bitenlerin kesinlikle komşuları dâhil diğer güvenlik seviyelerini etkilememesidir.

Güvenlik modellerini anlamak, değişik güvenlik ihtiyaçlarını anlamak için önemlidir. Bu modellerin çoğu tam anlamı ile artık kullanılmasa da bu modellere esas oluşturan güvenlik ihtiyaçları yerinde durmaktadır.

3.2.7.7. 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 (“due care” ve “due diligence”). İtinalı olmak her güvenlik olayına ilgi ve detayla eğilmek iken, güvenlikte sebat kavramı politika ve olayların üzerinden tekrar 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.

Dosya silme de bir güvenlik sorunudur. İşletim sistemlerine dosya silme komutu verildiğinde yaptığı şey dosyanın bulunduğu bölgeyi dosya tablosunda yazılabilir olarak göstermektir. Dosya gerçekten silinmez. Dosyaların silinmesini temin etmek üzere silme ve üzerine yazma politikaları oluşturulmalıdır. ABD Savunma Bakanlığı dosyanın gerçekten silindiğinden emin olunması için üzerine 7-10 kere yazılmasını tavsiye etmektedir.[29]

Denetim sistemleri bu başlık altında incelenmektedir. Denetim, kurumun kendi politikalarına ve diğer mevzuata uygun davranıp davranmadığının kontrol edilmesidir. Denetim içerden veya dışardan olabilir. Kurum dışından denetleme yapan denetçilerin kurum ile bir ilişki içinde olmaması gerekmektedir. Denetimlerin bir kısmı zaman planlanmış iken bir kısmı beklenmeyen zamanlarda olmalıdır. Denetimlerin sağlıklı olabilmesi için denetçilere takip edebilecekleri mümkün oldukça çok kayıt bırakılmalıdır. Denetçiler işlerini bir rapor yazarak bitirirler. Raporda amaç, kapsam ve bulgular olmalıdır. Bu bölümlerin dışında rapor özel bir amaç için yazılıyor ise hitap ettiği kimselere yönelik bölümler de olmalıdır.

Denetim raporlarına güzel bir örnek Sayıştay'ın Hazine Müsteşarlığı bilgi sistemleri üzerine yazdığı rapordur.[30] Sayıştay, hazine mali girdi ve çıktıları üzerine TBMM'ne (Türkiye Büyük Millet Meclisi) ortalama yılda bir kere rapor verme yükümlülüğü olduğu halde, Hazine Müsteşarlığı'nın bilgi sistemlerinden sağlıklı bilgi alamadığını fark edince bu sistemler üzerinde 2003 yılında bulgularını gösterir

29 DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 01/1995
30 T.C. Sayıştay Başkanlığı, "Hazine Bilişim Sistemleri Denetim Raporu", Ekim 2003

bir rapor yayınlamış ve raporu TBMM'ne sunmuştur. Rapor sadece bulguları bildirmekle kalmamış, önerilerini de belirtmiştir. Önerilerden en önemlileri bilgi sistemlerinin yönetimini ve güvenliği sağlayıcı bir standarda uyulmayışı olmuştur. Kamuda bu tip denetimlerin kritik işlev gören kurumlarda yaygınlaşması beklenmelidir.

İşletim güvenliği konusunun son kısmı gözlemdir. Sistemin performansı, kullanıcı hareketleri ve hassas işlemlerin sağlığı özellikle gözlemlenmelidir. Gözlemin aynı zamanda caydırıcı bir önlem olduğu akıldan çıkarılmamalı, sistemin sürekli gözlemlenip raporlandığının herkes tarafından bilinmesi sağlanmalıdır. Gözlem sıklığı, gözlemler sonucunda yapılması gereken düzeltmelerin de küçük ve önleyici olmasını sağlayacaktır. Uzun aralıklarla yapılan gözlemlerde ise tepkisel kararlar verilmek zorunda kalınabilecektir.

Bilgisayarlarda ve sunucularda yüklü programların da sürekli gözlemlenmesi, bunların politikalarla uyumlu olup olmadığının kontrol edilmesi gerekmektedir. Gözlemlenmesi gereken başka bir önemli nokta ise bilgisayar ağı ve internet trafiğidir. Gözlemler sonucunda edinilecek en önemli bilgilerden biri eğilimlerdir. İhtiyaçlar konusunda gözlemler, çalışanların ifade ettiklerinden daha fazla bilgi verecektir.

3.2.7.8. 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. Pekçok 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 başlıcası 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.

3.2.7.9. Mevzuat, İnceleme ve Değerler

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.

Türk Ceza Kanunu'nda bilişim suçları; (5237 Sayılı Kanun, 2004.)

- 5237[31] sayılı "Yeni Türk Ceza Kanunu"nun "Bilişim Alanında Suçlar Bölümünde Düzenlenen Suç Tipleri"ni düzenleyen "Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu"nu tanımlayan 243. maddesi,
- "Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu"nu tanımlatan 244. maddesinin 1. ve 2. fıkraları,
- "Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu"nu tanımlayan 244. maddenin 4. fıkrası, "Banka veya kredi kartlarının kötüye kullanılması suçu"nu tanımlayan 245. maddesi,

[31] 5237 Sayılı Kanun, 26/09/2004

- "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri"ni tanımlayan alanlarda ise "Kişisel verilerin kaydedilmesi suçu"nu tanımlayan 135. maddesi,
- "Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu" nu tanımlayan 136. maddesi, "Verilerin yok edilmemesi suçu" nu düzenleyen 138. maddeleridir.

Bilişim sistemleri ile işlenebilecek diğer suçlar ise YTCK'da (Yeni Türk Ceza Kanunu) farklı bölümlerde düzenlenen ve bilişim sistemleri aracılığıyla işlenebilecek başka suç tiplerinde tanımlanmaktadır. Bu suç tipleri şunlardır; (5237 Sayılı Kanun, 2004.)

YTCK'nın 124. maddesinde düzenlenen "haberleşmenin engellenmesi suçu",

- 125. maddesinde yer alan "hakaret suçu",
- 132. maddesinde düzenlenen "haberleşmenin gizliliğini ihlal suçu",
- 142. maddesinin 2. fıkrasının 'e' bendinde yer alan "nitelikli hırsızlık suçu",
- 158. maddenin 1. fıkrasının 'f' bendinde yer alan "nitelikli dolandırıcılık suçu",
- 226. maddesinde düzenlenen "müstehcenlik suçu"
- 228. maddesinde düzenlenen "kumar oynanması için yer ve imkân sağlanması suçu".

Kurumlar yasal gereksinimlerin içini doldurmak istiyorlar ise kurum içi bilişim güvenliğini tüm alt gereksinimleri ile kurmak zorundadırlar. Kurum güvenliğinin yasal gereksinimleri sağlamak olduğu, güvenliğin kurum personelinin ahlaki ve etik davranışlarına da bir standart getirmesi gerektiği unutulmamalıdır. Bilişim suçlarıyla mücadelede alınması gereken önlemlerin ilki, kişilerin ve kurumların kullandıkları bilişim sistemlerinin güvenliğini sağlamalarıdır. Bununla kastedilen; sistemde bulunan verilerin ve sistemin kendisinin gizliliği, bütünlüğü ve kullanıma yönelik her türlü tehlikelere karşı güvenliğinin sağlanmasıdır. (Dülger, 2004, s.320)

Bir de özellikle büyük kurumların bilgi işlem merkezlerinde ancak yetkisi olan ve güvenilir personelin çalıştırılmasının sağlanmasıdır. (Dülger, 2004, s.321)

3.2.7.10. Fiziksel Güvenlik

Fiziksel güvenlik, bilişim güvenliğinin kapsamının sınırında olmasına rağmen önlemlerin fiziksel ortamdaki gerçekleri gözardı 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 tehditler temel olarak on iki bölüme ayrılırlar;

1. Yangın ve duman: Sadece dumanın kendisi dahi bir tehdit olabilir. Kurum binası yakınlarda alev aldığında zehirli ya da nefes almayı zorlaştırıcı duman çıkarabilecek malzemeler olup olmadığı araştırılmalıdır. Kurum içerisinde duman tespit ve söndürme cihazları olmalıdır. Su ile söndürmenin zararlı olacağı birimlerde gazlı yangın söndürme sistemleri kurulmalıdır.

2. Su: Kurum binasının su baskını tehdidi ile karşı karşıya olup olmadığı araştırılmalıdır. Özellikle bilgi sistemleri için bahse konu olabilecek su tehdidi muhtemel bir yangın sonrasında yangının su ile söndürülmesi ve tüm bilişim altyapısının söndürme suyu ile tahrip olmasıdır. Bilgi depolama odaları yapısal kablolama standartları gereği kurumların ne en üst, nede en alt katında değil, orta katların herhangi birinde, tercihen kablolama ergonomisi açısından kurumların tam ortasında bulunurlar.

3. Yer hareketleri: Kurum binasının bulunduğu coğrafi konumun deprem tehlikesi ile ne kadar tehdit edildiği araştırılmalı, engebeli arazilerde yer kayması ihtimali göz önünde bulundurulmalıdır. Binanın yıkılma ihtimali her zaman göz önünde bulundurulup yedekleme sistemleri kurulurken ihtimal göz önünde bulundurmalıdır.

4. Fırtınalar: Fırtınalar beraberlerinde yıldırım, sel, çamur yığını gibi tehditleri de getirirler. Yine bu tehdit de coğrafi konuma göre değerlendirilmelidir.

5. Sabotaj veya kurum mülkünün bilinçli olarak tahrip edilmesi: Bu tehditler kurumun çerçeve güvenliği alınarak önlenebilir.

6. Patlamalar: Kurum içerisinde ne tür bilişenlerin patlamaya yol açacağı incelenmeli ya da incelettirilmelidir. Bu kontroller düzenli aralıklarla yapılmalıdır.

7. Binanın yıkılma ihtimali: Binalar yer hareketleri olmadan da yıkılma tehlikesi ile karşı karşıya olabilirler. Bu tip bir tehdidin belirtileri görülür ise, her çatlağı sıvamak yerine bu konu analiz ettirilmelidir. Bina yıkılması diğer fiziksel tehditlerin sonucu da olabilir.

8. Zehirli malzemeler: Kurum içerisinde kullanılan, üretimde kullanılan bileşenlerin belli bir aşamada zehirli bir ürün oluşturup oluşturmayacağı araştırılmalıdır. Tuz ruhu ve çamaşır suyu gibi her evde bulunabilecek malzemelerin bileşiminin zehirli olduğu gibi analizler yapılmalıdır.

9. Kesintiler: Kurumun elektrik, su, doğalgaz kesilmesi gibi durumlarda faaliyetlerini sürdürebilmek için iş süreklilik planları olmalıdır.

10. İletişim kesintisidir. Kurum, veri veya ses iletişimi kesilir ise bundan ne kadar etkileneceğini iş süreklilik planlarındaki iş etki analizinde belirlemelidir.

11. Malzeme kaybı: Kurumda malzeme, araç ve gereçlerinin tümünün "eğer yarın yerinde bulamasam ne yaparım" analizi yapılmalıdır.

12. Personel kaybı: Personeller işten ayrılma, hastalanma veya ölüm gibi sebepler ile işlerini yarım bırakabilirler. Güvenlik bakış açısından her personelin kuruma ne kadar faydalı olduğunun analizinin yapılması gerekir. Tek bir personelin kaybı dışında grev gibi toplu personel kayıplarında neler yapılabileceği de önceden düşünülmelidir.

Fiziksel önlemler güvenliğin başlangıç noktasıdır. Kurumun en değerli varlıkları insanlarıdır. İnsanlar güven içinde olmadıkları sürece diğer varlıkların ne kadar güvende olduklarının anlamı yoktur. Fiziksel önlemler insanların yanında kurumun diğer varlıklarını da korurlar.

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

TS ISO/IEC 17799 standardı, bilgi güvenliği konusunda her kuruluşta uygulanabilecek bir güvenlik standardıdır. 1995 yılında İngiliz Standart Enstitüsünün çıkarttığı BS 7799, bugünkü kullanımda olan standardın kaynağını oluşturmaktadır. 1999 yılında BS 7799 standardı güncellenmiş ve uygulamada karşılaşılan kontrol standardı oluşturma zorluğuna istinaden orijinal standart BS 7799-1 olarak isimlendirilmiş, BS 7799'da konulan prensiplerin sorgulanabilmesi için BS 7799-2, kurumlarda standartlaşmış bir bilgi güvenliği yönetim sistemi kurmak üzere bir kontrol listesi olarak yürürlüğe konulmuştur. 2000 yılında BS 7799-1 ve 2 standartları içeriği hiç değiştirilmeden uluslararası standart olarak TS ISO/IEC 17799-1 ve 2 olarak kabul edilmiştir. 2005 yılında ise iki standart da yeniden gözden geçirilmiş, ISO/IEC 17799-1 standardının 2005 sürümü yürürlüğe konmuş, ISO/IEC 17799-2 standardının yeni sürümünün ise TS ISO/IEC 27001 olarak ismi değiştirilmiştir. 2007 yılında ISO/IEC 17799-1 standardının isminin yeni sürümle beraber TS ISO/IEC 27002 olarak değiştirilmesi, bilgi güvenliği ölçüm kıstasları için çıkarılması planlanan standardın kodunun ise ISO/IEC 27004 olması planlanmaktadır.

Güvenlik sertifikasyonunda bugün verilen sertifika ISO/IEC 27001 sertifikasıdır. Ancak ISO/IEC 27001 standardının koyduğu kuralları anlayabilmek için ISO/IEC 17799-1:2005 standardının anlattığı, tavsiye ettiği, zorunlu kıldığı her türlü önlemin gereklerini yapmış olmak şarttır. ISO/IEC 27001 standardının esasını oluşturan kontrol listesindeki her madde ISO/IEC 17799'da konunun ele alındığı başlıklara atıf yapar (ISO/IEC 27001). Tez'in bu aşamasına kadar yönetim ve güvenlik kavramlarının çoğu anlatıldığı için, bu aşamadan sonra kamu kurumlarının mevcut uygulamalarından örneklerden bahsedilecek ve ISO/IEC 17799 standardı detaylarında e-devlette bu standardın uygulanması konusu her bir detayla ilgili olarak değerlendirilecektir.

Giriş bölümünde de bahsedildiği gibi, "E-dönüşüm Türkiye" projesi Başbakanlık'ın 2003/12 sayılı genelgesi ile başlamış, 2003/48 sayılı genelge ile de DPT projenin koordinasyonu, izlenmesi, değerlendirilmesi ve yönlendirilmesi ile görevlendirilmiştir. Bu bağlamda çalışmalarına başlayan DPT Bilgi Toplumu Dairesi, "E-dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi"ni

yayınlamıştır. Rehber'de kamu kurumlarında bilgi güvenliği yönetim sistemlerinin kurulmasının önemi anlatılmıştır. Kamu kurumlarını bağlayıcı nitelikteki bu dokümanla, kamu kurumlarında uygulamalar başlanmış ama tüm kurumların entegresi gerçekleşmemiştir. Kurumlar kendi iletişim ağlarını kullanarak e-dönüşüme kısmen başlamıştır.

MERNİS PROJESİ:

Ülkemizde İçişleri Bakanlığı, Nüfus ve Vatandaşlık Genel Müdürlüğü tararından yürütülen, Merkezi Nüfus İdaresi (MERNİS) ve Kimlik Paylaşımı Sistemi (KPS) internetten gelebilecek saldırılara karşı firewall ile korunurken Atak Tespit ve Önleme Sistemi URL filtreleme, Antivirüs Gateway ve Antispam özelliklerini barındırmaktadır. Taşra bağlantısı ise Telekom'dan kiralanan özel hatlar ile sağlanıyor ve bu hatların internet ile hiçbir bağlantısı bulunmamaktadır. Tamamıyla kapalı bir ağ olan MERNİS yazılımına kullanıcı adı ve parola ile girilebilmektedir. Bütün yapılan işlemlerin geri izleme bilgisi tutulurken bir sorun çıkması halinde sistemin devamlılığı için veriler Felaket Yedekleme Merkezinde (FYM) güncellenmektedir. İki ayrı veri tabanı olan MERNİS ve KPS arasında IP tabanlı bir erişim bulunmamaktadır. KPS'ye kötü amaçlı bir erişim olsa bile MERNİS'e KPS üzerinde ulaşmak mümkün değildir. Sunulan web servislerinde Web Servis Güvenliği (WS-web Security) alt yapısı kullanılıyor. (İçişleri Bakanlığı, 2007)

MERNİS'in veri güvenliği, TÜİK'in (Türkiye İstatistik Kurumu) yürüttüğü adrese dayalı nüfus kayıt sistemi projesiyle bu yıl daha da güçlendirilecektir. MERNİS intranet, adres ve KPS'de yüksek performanslı ve genişleyebilir güvenlik ürünleri kullanacaktır. İnternette açık her ağ parçası Atak Tespit ve Önleme Sistemleri (IPS) ile dinlenecektir. İnternet üzerinde sunuculara gelecek trafik, SSL teknolojisi ile şifrelenecektir. Sunuculara yük paylaşımı yapılacak ve SSL trafiğinin hızlandırılması için özel cihazlar kullanılacaktır. Tüm güvenlik sistemi yıl içinde en az üç kere açıklara karşı taranarak raporlar oluşturulacaktır. Siteme girilen verilerin veri tabanında da güvenli bir şekilde saklanabilmesi için veri bütünlüğünün ve inkar edilemezliğin sağlanması, diğer bir deyişle, veri tabanına girilen her yeni veri ve güncellemenin imzalanarak saklanması için PKI imza sunucuları kullanılacaktır. (İçişleri Bakanlığı, 2007)

UYAP PROJESİ:

Adalet Bakanlığı'nın kullandığı İntranet içinde çalışan bir sistem olan Ulusal Yargı Ağı projesinde (UYAP), uygulama katmanı erişimi birden fazla güvenlik duvarı ve saldırı tespit sistemleri tarafından denetlenmektedir. Sistemin güvenliği dışarıdan gelebilecek saldırılara karşı donanım (Güvenlik Duvarı, Anahtar, Yönlendirici, Saldırı Tespit Sistemi (IDS) ve yazılımlar (Güvenlik Duvarı yazılımı, Saldırı Önleme Sistemi Yazılımı, Anti virüs Yazılımı, EPO yazılımı) ile sağlanmaktadır. (Adalet Bakanlığı, 2007)

Güvenlik internet üzerinden vatandaş ve avukat için verilen servislerde özel bir güvenlik bölgesinde yer alan yazılımsal bir gateway olarak çalışan bir sunucudan sağlanırken, internet erişimi UYAP iç kullanıcıları için kısıtlanmış ve belirli kurallar çerçevesinde merkezi Proxy üzerinde gerçekleştirilmektedir. Bakanlık personeli, kullanıcı adı ve şifresi ile sisteme girebilmektedir. Active Directory yapısı ile yönetilen projede kullanıcı yetkileri merkezden belirlenebilmektedir. Kullanıcılar sadece yetkileri olan uygulamalara, ekranlara ve veriye erişebilmektedir. (Adalet Bakanlığı, 2007)

Sistem dışından bir saldırı yapıldığında, saldırıyı yapanların yer ve kimlikleri tespit edilebilmektedir. Türk Ceza Kanunu'na göre suç teşkil eden bu tip eylemleri yapanların kimliklerinin saptanması caydırıcı bir rol oynamaktadır. İç kullanıcılardan gelebilecek saldırılara karşı hem sistemde hem de uygulama yazılımda kullanıcılar tarafından gerçekleştirilen işlemler loglanıyor. UYAP'ta Bilgi Güvenliği Yönetim Sistemi'nin kurularak uluslar arası bir standart olan ISO/IEC 17799-ISO/IEC 27001 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri Standardına sahip olma hedeflenmekte ve bu doğrultuda çalışmalar yapılmaktadır. (Adalet Bakanlığı, 2007)

POLNET PROJESİ:

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

Güvenli erişim protokolleriyle gerçekleştirilen sistem veri tabanına erişim izleri kayıt altına alınmaktadır. Personel, idari amirinin doğruladığı ve sistem

kullanıcısı olmanın sorumluluklarının hatırlatıldığı kullanıcı talep formunu imzalayarak sisteme giriş talebinde bulunabilmektedir. Herhangi bir nedenle birimden ayrılan kullanıcının erişim izinleri iptal edilir. Sistem kullanıcıları belirli periyotlarla şifrelerini değiştirmek zorundadır. Sistemin virüslere ve zararlı programlara karşı korunması otomatik güncelleme yapan antivirüs sistemiyle sağlanıyor. Oluşabilecek güvenlik açıklarının gönüne geçmek için otomatik yama sistemleri kullanılırken bilgi paylaşımları güvenlik duvarları üzerinden yapılmaktadır.

SAĞLIK BAKANLIĞI:

Sağlık Bakanlığı, bilgi sistemlerinde bilgi sistemlerinde paylaşılan idari, mali ve klinik verilerin güvenliğinin ve iş devamlılığının sağlanması, güvenlik ihlalinden kaynaklanabilecek kanuni risklerin en aza indirilmesi, yatırımların ve kurumun itibarının korunması için bütün kurumlarında bilgi sistemlerinin güvenliğinin sağlanması konusunda standartlar belirlenmiştir.

Bakanlığın Bilgi Güvenliği Politikası, genel olarak; e-posta güvenliği, antivirüs sistemleri, şifreleme gibi 23 ana başlık altında toplanan metot ve kurallardan oluşmaktadır. Ayrıca bilişim sistemlerinin fiziksel olarak nasıl korunacağına dair talimatlar da yayınlandı. Bakanlık, bütün sağlık kurumlarına, firewall, saldırı tespit ve önleme sistemleri, antivirüs gateway çözümleri, VPN çözümleri, yazılım güncelleme servisleri, sunucuların güvenliğinin sağlanması için alınması gereken önlemler, web filtreleme çözümleri, domain yapılarının oluşturulması denetleme ve izleme konularında zorunlu ve opsiyonel çözümler oluşturmaları talimatı vermiştir. Kimlik denetimi için güçlü mekanizmalar kullanılması yönündeki çalışmalar yapan Bakanlık aile hekimleri için sayısal imza ve kimlik denetiminde akıllı kartlar kullanılması çalışmalarını da sürdürmektedir. Hastanelerde bu sistemleri kullanmak üzere TUBİTAK-UEKAE ile çalışmalar yürüten Bakanlık, ISO/TSE 17799 bilgi güvenliği sertifikası alınmayı planlamaktadır.

Kurumlar için bağlayıcı olan genelgelerde, ISO/IEC 17799 standardının e-devlet çalışması yapan tüm kurumlarda uygulanması öngörülmektedir. ISO/TSE 17799-1:2005 standardını anlatmaya standardın sıfır – dördüncü bölümlerden başlanacaktır. Bu bölümler standardın temelini oluşturan bilgi güvenliği kavramlarını açıklığı kavuşturmak, güvenliğe neden ihtiyaç duyulduğunu anlatmak, işe nereden

başlanabileceğini belirlemek ve sonuncu ve en önemli olarak kritik başarı faktörlerini belirlemek ile standarda başlanır.

4.1. 17799-1:2005 Giriş Bölümü: Bilgi Güvenliğine Neden Gerek Vardır ve Kritik Başarı Unsurlar

Bu bölümde tez'in tüm bölümlerinde anlatılan kavramların üzerinden bir kere daha, bu defa bir standardın özetlemesi ile tekrar geçilecektir. Standart, her şeyden önce bilgi güvenliğine neden ihtiyaç bulunduğunu açıklamak ile işe başlar. Bilgi de her varlık gibi kurumun bir varlığıdır ve her varlık gibi parasal bir değeri vardır. Kâğıtta, kurum personelinde veya elektronik olarak depolanmış olarak bulunan bu bilginin risklere karşı korunması gerekmektedir.

Bilgi güvenliği kurumun rekabetçi gücünün korunması, para akışının sürekli kılınması, karlılığın artırılması, yasal uyumluluğun sağlanması ve kurumsal imajın zedelenmemesi için gereklidir. Bilgi iletişim ağları genellikle güvenlik değil, işlevsellik göz önünde bulundurularak tasarlanmıştır. Gittikçe daha fazla iş fonksiyonunun bu güvensiz ortamlarda yürüyor olması güvenliğe ihtiyacı artırmaktadır.

Kurumsal bilgi güvenliği bu riskleri kontrol etmek için kullanılan politikalar, organizasyon yapısı değişimleri, yazılım ve donanımlar ile korunmalıdır. Bu kontroller kurulmakla yetinilmeyip gözlemlenmeli, yeniden düşünülüp geliştirilmelidir. Bu geliştirme sürecindeki en önemli hedef kurumun iş hedeflerine ulaşılmasıdır. Güvenlik gereksinimleri için aşağıdaki üç kaynak temel alınmaktadır;

- Kurumun karşı karşıya olduğu risklerdir. Bu riskler kurumun hedeflerine ve bu hedeflere yönelik stratejilerine yönelik tehditlerdir.
- Kurumun uymak zorunda olduğu tüm mevzuat ve sözleşmelerdir.
- Kurumun destek faaliyetleri kapsamında kullanmakta olduğu bilgi işleme yöntemleridir. (arşiv kullanma ya da evrak dolaşım sistemi gibi)

Kurumların uymak zorunda olduğu mevzuat çerçevesinde yapılması gerekecek uygulamalardan en önemlileri ise şunlardır;

- Verileri ve özel hayatı ilgilendiren bilgileri korumak.
- Kurum kayıtlarını korumak.

- Fikri mülkiyet haklarını korumak

Koruma işlevini gerçekleştirmek için gereken kontrol ve önlemlere aşağıda belirtilen liste temel örnek olarak verilebilir;

- Bilgi güvenliği politika dokümanı
- Bilgi güvenliği sorumluluklarının belirlenmiş olması
- Bilgi güvenliği bilincinin varlığı ve ilgili eğitimler
- Uygulamaların doğru yapılandırılmış olmaları
- Zaafiyet yönetimi
- İş süreklilik planı
- Bilgi güvenliği olaylarının incelenip güvenliğin artırılması

Bilgi güvenliğini sağlamak için gereken kritik başarı faktörleri şu şekilde sıralanabilir;

- İş gereksinimlerini ön planda tutan güvenlik politikaları ve etkinliklerin olması
- Bilgi güvenliğini uygulayan, yöneten, gözlemleyen ve geliştiren kurum kültürü ile uyumlu genel bir güvenlik anlayışının olması
- Yönetimin görünür desteği ve güvenliğe adanmışlığı
- Bilgi güvenliği, risk analizi ve risk yönetimi gereksinimleri hakkında doğru bir anlayış
- Bilgi güvenliğinin yönetime çalışanlara ve tüm ilgililerine etkili pazarlanması (anlatılması)
- Tüm çalışanlara ve yöneticilere güvenlik politikalarının uygulanması konusunda yönlendirmeler yapılması
- Bilgi güvenliği etkinlikleri için yeterli bütçe ayrılması
- Yeterli güvenlik farkındalığı ve eğitimin verilmiş olması
- Bilgi güvenliği olayları için etkili bir olay yönetimi mekanizması kurulmuş olması

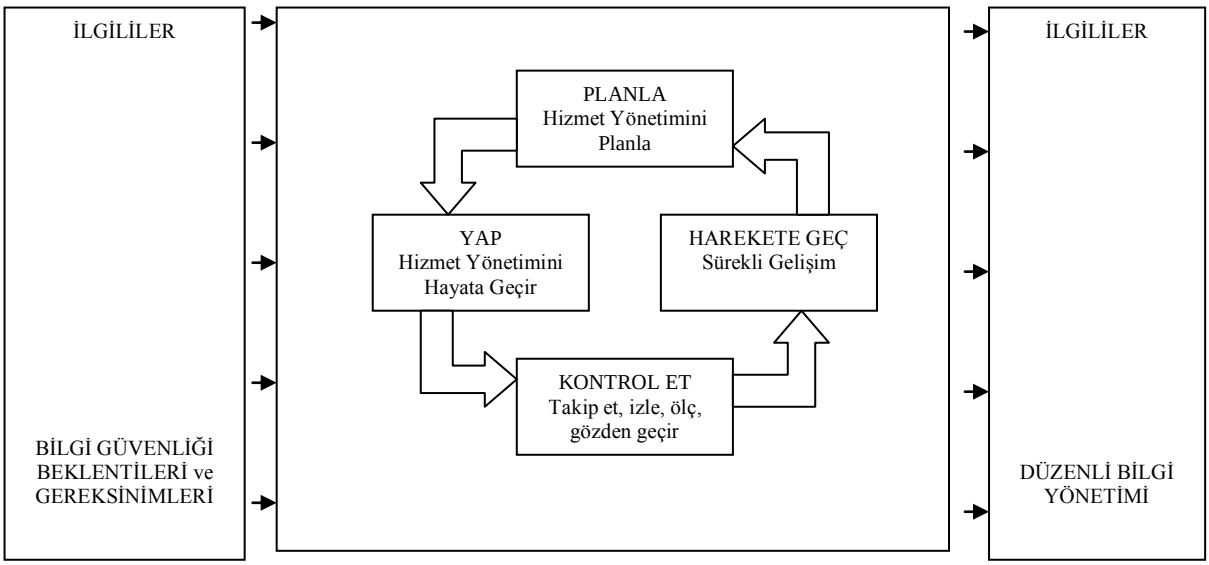
- Bilgi güvenliği için ölçülebilir performans kıstasları konulmuş olması (bu madde bu standart kapsamında değildir, bu madde için 27004 standardı ileri bir tarihte yürürlüğe girecektir)

Yukarıda sayılan belirtiler güvenlik uygulamalarının sağlıklı çalıştığı kurumların ortak özelliklerinden seçilmişlerdir.

4.2. TS ISO/IEC 17799 Bilgi Güvenliği Yönetim Sistemi

17799 ve 27001 standartlarının kurmaya çalıştığı kurumsal güvenlik altyapısı "Bilgi Güvenliği Yönetim Sistemi"[32] (BGYS) olarak adlandırılır. BGYS'de ISO 20000 standardı gibi planla – yap- kontrol et – harekete geç döngüsünü kullanmaktadır.

Şekil 4. 1'deki döngüde de görüldüğü gibi güvenlik gereksinimleri statik değil, zamanla değişen ve gelişen bir yapıdır. Her yapılan değişimin yapıyı daha da güçlendirmesi öngörülür.



Şekil 4. 1 Bilgi Güvenliği Yönetim Sistemi planla – yap- kontrol et – harekete geç döngüsü (ISO/IEC 20000-1:2005(E))

BGYS sisteminin kurulması şu adımlar atılarak gerçekleştirilir:

- Bilgi güvenliği yönetim sistemini kurmak için ilk adım BGYS amaç ve sınırlarının belirlenmesidir. Bu aşamada kurumun yeri, çalışma alanı, kullanmakta olduğu teknolojiler, varlıklarının listesi gibi bilgiler

[32] Orijinal metindeki yazılışı ile "Information Technology Management System", ISMS (ISO/IEC 27001)

yazılarak kayıt altına alınır. Kapsam dışı bırakılan bir alan var ise bunun nedeni de açıklanır.

- Kurumların yerleri, çalışma alanları, kullanmakta oldukları teknolojiler, varlıklarının listesi, değişkenleri göz önünde tutularak güvenlik yönergesi hazırlanır. Bu yönerge kurumların stratejilerini, hedeflerini, kültürünü ve yükümlülük altında bulunduğu kanuni gereksinimler göz önüne alınarak hazırlanır.
- Risk'ler belirlenir ve incelenir. Kurumlardaki varlık listesi oluşturulur. Bu varlıkların zaafları, oluşabilecek tehditler ve tehditlerin olasılıkları tespit edilir.
- Varlıkların kurumlar için değerine göre, yönetim tarafından istenebilecek güvenlik düzeyi belirlenir.
- Kullanılacak önlemlerin belirlenmesi. Tehditlere karşı hangi önlemin, ne amaçla kullanılacağı belirlenir.
- Uygunluk ifadesi hazırlanır. Uygunluk ifadesi, risklerin belirlenmesi sonrasında bu risklere karşı alınan önlemlerin (kontrollerin) amacının ne olduğuna, eğer önlem alınmayan riskler var ise bunun sebeplerinin neler olduğuna dair bir gerekçelendirme belgesidir.

BGYS'nin faaliyete geçirilmesi aşamasında ise riskler için öngörülen önlemlerin maliyet ve etkinlik yönetimi aşamaları gelir. Bu önlemlerin ne kadar etkin olduğu ve maliyetleri kontrol altında tutulur. Daha sonra ise BGYS'nin gözlemlenmesi, bakımı ve geliştirilmesi aşamaları gelir. Bilgi güvenliğinin aksayan noktaları, güvenlik olaylarının doğru kanallardan incelenip incelenmemesi gibi etkenler gözlem altında tutulup sürekli geliştirilmeleri için kaydedilirler.

ISO/IEC 17799 ve ISO/IEC 27001 standartları risk incelemelerini on bir alanda incelerler. Bilgi güvenliği bu on bir alanda sınırlı kalmayabilir ve bu alanlar kurum ihtiyacına göre artırılabilir. Bu alanlar ve önerilen önlemler standart içinde sıralandığı şekilde aşağıda incelenmektedir;

1. Güvenlik politikası
2. Örgütsel güvenlik
3. Varlık sınıflandırması ve denetimi

4. Personel güvenliği
5. Fiziki ve çevresel güvenlik
6. İletişim ve işletim yönetimi
7. Erişim denetimi
8. Sistem geliştirilmesi ve idamesi
9. Bilgi güvenliği olay yönetimi
10. İş sürekliliği planı (Ticari süreklilik yönetimi)
11. Uyum

4.2.1. Güvenlik Politikası

BGYS'nin en önemli dokümanı güvenlik politikası dokümanıdır. Bu doküman kurum hedefleri, ihtiyaçları, ilgili mevzuat göz önünde tutularak hazırlanır ve belli aralıklar ile gözden geçirilir. Güvenlik politikası dokümanı temel olarak aşağıdaki konuları içermelidir;

- Bilgi güvenliğinin tanımı, hedefleri, kapsamı ve bilgi güvenliğinin bilgi paylaşımındaki önemi,
- Yönetimin bilgi güvenliğinin kurum hedeflerine ulaşılması için bilgi güvenliğinin önemini vurgular ifadesi,
- Risk analizinin nasıl yapılacağına ve uygun önlemlerin nasıl alınacağına dair bir yöntemi,
- Kurumlar için önemli prensip, politika ve uyumluluk gereksinimleri, (mevzuat, iş süreklilik planı, eğitim ve farkındalık gereksinimleri ya da disiplin ve kovuşturma sistemi gibi)
- Güvenlik sorumlulukları,
- Uyulması gereken ek standartlar var ise bu dokümanları.

Güvenlik politikası dokümanı kurum paydaşları tarafından yapılan geri beslemeler, bağımsız denetleme raporları, yönetim istekleri, güvenlik politikasının ölçülmüş etkinliği, politikaya temel oluşturan bazı unsurların değişmiş olması (konum, yasalar, sözleşmeler, iş hedeflerinin değişimi gibi durumlar), tehdit veya zafiyetlerin değişimi, bilgi güvenliği vakalarının raporları ve ilgili yetkili kurumların

(emniyet teşkilatı veya itfaiye gibi) önerileri - girdileri göz önünde tutularak belli aralıklar ile gözden geçirilmelidir.

Bu anlamda bizdeki kamu kurumları kendi sistemlerinin güvenliği için bir dizi önlemler almaktadır. Kurumların geçerli olan bilgi güvenliği politika dokümanlarında, kamu hizmetlerinin kaliteli sunumu, bilgilerin ve mahremiyetin korunması ile ilgili gereken standartlar ve sorumluluklar belirlenmeli, bu süreçte olabilecek riskleri değerlendirilmelidir. Mevzuatların kurum hedeflerine yönelik olarak yapılacak risk incelemelerinden sonra değiştirilmesi ve düzenli aralıklar ile gözden geçirilmesi gerekmektedir.

4.2.2. Örgütsel Güvenlik

Örgütsel güvenlik kurumların bilgi güvenliği sistemini oturtmak için kurmaları gereken personel organizasyonunun veya kurum içi örgütlenmenin adıdır. Güvenlik örgütlenmesi yönetimden başlar. Yönetim güvenlik faaliyetlerinin yönünü belirler, etkinliğini ölçer, politikaları belirler, güvenlik gereksinimlerinin ilgili personel tarafından anlaşıldığından ve gereğince uygulandığından emin olur, denetleme işini bizzat ya da görevlendirmeler yaparak gerçekleştirir ve güvenlik farkındalığının her zaman yüksek olması için her türlü etkinliğin gerçekleşmesi ve kaynağın ayrılmasını sağlar. Kısaca kurumlarda bilgi güvenliği yönetim ister ise vardır, diğer herhangi bir koşulda ise yoktur.

Eğitim, risk incelemesi, tatbikat gibi güvenlik etkinlikleri kurumun değişik birimlerinden katılım ile gerçekleşmelidir. Bu birimlerin arasında özellikle üst yönetim, insan kaynakları, hukuk, güvenlik birimi, bilgi teknolojilerinden sorumlu birim temsilcilerinin ve kurumun asli işlevlerinden sorumlu personelin olması gereklidir.

Kurum içinde kullanıma girecek her yeni bilgi işleme aracı yönetimin onayına tabi olmalıdır. Her yeni bilgi işleme aygıtı, sistemi, kısaca kurumsal bilginin ilişkiye girdiği her tür cihaz diğer aygıtlarla uyumluluğu gibi alanlarda test edilmeden kullanıma alınmamalıdır. Kişisel bilgisayarlar veya kuruma ait olmayan donanımlarda kullanım için ayrı politikalar olmalıdır.

Kurumlar bilgi alışverişi yaptığı tüm kuruluşlar ile gizlilik anlaşmaları yapmalıdır. Bu anlaşmalarda korunması gereken bilginin neler olabileceği, anlaşma bittiği zaman gizlilik koşulunun devam edip etmeyeceği, bilginin hangi koşullarda

kullanılabileceği ve tarafların gizlilik koşulunun sağlanıp sağlanmadığı konusunda birbirlerini nasıl gözlemleyecekleri veya denetleyebilecekleri hususları yer almalıdır.

Kurumlar acil durumlar ya da güvenlik olayları gibi durumlarda hangi otorite ile hangi şekilde bağlantı kuracağının bilgilerini önceden tutmalıdır. Örneğin altyapıda yer alabilecek sorunlarda (kanalizasyon, su, elektrik, iletişim vs.) veya emniyet teşkilatı, itfaiye ve acil sağlık hizmetleri gibi ihtiyaçlarda kimin aranması gerektiği konusu önceden tanımlanmış olmalıdır. Kurumlar güvenlik konularında en son ve güncel bilgilendirmelerin alınabileceği kaynaklar ile bağlantı kurmalıdır. Güvenlik konusunun ilgilileri bu konuda uzmanların üye olduğu organizasyonlarda görev almalı, eğitimlere katılmalı, en güncel tehdit ve zafiyetlerin tartışıldığı her ortamdan haberdar olmaya çalışmalıdırlar. İnternet güvenlik portalları, ulusal ve uluslar arası güvenlik etkinliklerine katılım bu tip bilgilenme için kullanılmalıdır.

Kurumlar güvenlik zafiyetlerini ve uygulamalarını bağımsız kaynaklara denetlettirmelidir. TS ISO/IEC 27001 sertifikasının alınması dış denetim işlevi için en etkin çözümdür.

Kurumlar bilgi güvenlik örgütlenmesinin en önemli ayaklarından biri de kurumun dış paydaşları ile olan ilişkileridir. Bu paydaşlar kurumların hizmet sunduğu kişiler, mal hizmet aldığı kişiler, şirketler, kurumun müşterileri ya da kurumun müşterisi olduğu üçüncü bir taraf olabilir. Kurum bu şirket/örgütlerin personellerinin kurum bilgi ağlarına erişimlerini ayrı politika ve prosedürlere bağlamalıdır. Bu personelin kuruma fiziksel erişimleri ve kurum bilgi ağlarına erişimleri konusu bu erişimlerin kurumda mı uzaktan mı olduğuna, erişilen bilgi düzeyinin hassasiyetine ve bu erişimlerin sıklığına göre düzenlenmelidir. Erişimlerin kesintiye uğramasının kurumlara zararı hesaplanmalıdır.

Kurumlar içerisinde geçici ya da sürekli görev yapmakta olan kurum personeli olmayan proje çalışanlarının erişim yetkileri alınacak özel onaylar ile belirlenmeli kayıt altına alınıp gözlemlenmelidir.

Kurumlar, bilgi altyapısını kullanan üçüncü taraflar ile yapılan sözleşmelerde, bilgi güvenliği gereksinimlerine, varlıklarının korunmasına (bilgi, yazılım, donanım), Üçüncü taraf personelinin kurumların varlıklarını kullanmak için gerekli eğitimleri almış olmalarına, Üçüncü taraf personelinin kurumların güvenlik mevzuatı bilgilendirilmiş olmalarına, Kurumlar arası raporlamalar için şablonlara, Erişim ile

ilgili olarak, rollere göre personel erişim yetkilerine, erişim ile ilgili olarak, açıkça izin verilmemiş tüm erişimlerin yasak olduğuna dair bir maddelere, kullanıcı erişim ve yetkilendirilmesi için bir süreç tanımı yapılmasına, (örneğin üçüncü taraf personeline kullanıcı hesabı açılması gerekiyor ise bu aradaki sözleşmede yer almalıdır) aradaki erişim yetkilerinin kaldırılması için bir süreç tanımı yapılmasına, güvenlik vakalarının incelenmesi, raporlanması, bildirilmesi ve araştırılması ile ilgili bir süreç tanımlarına, üçüncü taraf personelinin hangi gizlilik düzeyinde bilgiye erişebileceklerinin tanımının yapılmasına, hedeflenen hizmet seviyesi ve kabul edilemeyecek hizmet seviyesi tanımlamalarına, (Hizmetten beklenilen kalite seviyesi tanımlanmalıdır), performans kıstaslarının tanımına ve raporlanma sürecinin tanımına, kurumların gözlemleme, denetleme yapma, verdiği hakları kaldırma haklarının garanti altına alınmasına dikkat etmeli ve bu konularda son derece itinalı davranmalıdır.

Yukarıda sayılan maddeler mümkün ise arada anlaşma olmamasına rağmen diğer paydaşlara da uygulanmalıdır.

4.2.3. Varlık Yönetimi

Kurumlar bilgi varlıklarını koruma altına almalıdırlar. Bu varlıklar veritabanları, dosyalar, arşivler, yazılımlar, donanımlar, ısıtma-soğutma-elektrik gibi hizmetler, insanlar ve saygınlık gibi değerlerdir. Bu sayılanların herhangi birinin zarar görmesi kuruma para ve eşdeğeri zararlar verecektir. Kurum tüm varlıklarının listesini çıkarmalıdır.

Kurumdaki her bilgi, her donanım, her varlık bir personelin üzerine zimmetli olmalıdır. Kurum sahip olduğu bilgiyi yedekli olarak kurum personeline dağıtmalı, kurum personeli kurumu hedeflerine götürecek olan kurumsal bilgileri bilmekle yükümlü olmalıdır. Kurum personeline bu bilgilere erişmek, gizli tutmak ya da paylaşmak için gerekli altyapıyı sağlamalıdır.

Kurumlar, her bir varlığının kullanımı için detaylı kullanım kılavuzlarını, kullanma yöntemlerini ve kabul edilebilir kullanım şekillerini tüm personelin ulaşabileceği bir ortama koymalıdır. Kurumlar, bilgilerinin nasıl sınıflandırılacağı konusunda detaylı olarak görevlendirmeler yapmalıdır.

4.2.4. Personel Güvenliği

Personel güvenliği üç bölümde incelenmektedir, işe alınmadan önce, işe alındıktan sonra ve işin sona ermesi sürecinde. İşe alınmadan evvel kurum kişi hakkında mümkün olan tüm güvenlik araştırmalarını yapmalı, işe alınma sırasında ise kişiden kurumun tüm kural ve politikalarına uyacağı, kurumdan ayrılacağı zaman ise kurum hakkında gizli kalması gereken bilgileri açığa çıkarmayacağı konusunda güvenceler alınmalıdır.

İşe alındıktan sonra ise kişinin işe alınmasına sebep olan özelliklerinin kaybolmaması ve gelişmesi için gereken önlemler alınmalıdır. Kişinin kurumda rolü ve yetkilerinin ne olduğu, kurumun hangi davranışları hoş gördüğü, hangilerinin ise yasak olduğu konularında hiçbir kuşkuya yer bırakmayacak şekilde bilgilendirilmesi gerekmektedir.

İşten ayrılma sırasında ise kişinin üzerine zimmetli her türlü kurum varlığını teslim etmiş olduğundan emin olmak gerekmektedir. Özellikle yaptığı işten memnun kalınmayan bir kişinin işine son verildiğinde yapılması gereken ilk iş kişinin kurum içi erişim haklarının kaldırılması ve kurum varlıklarının kişiden geri alınmasının güvenlik görevlileri eşliğinde yapılmasıdır. Kişiler görevlerinden ayrıldıkları zaman bilgi hizmetleri ile ilişki kesmeli, kurumdan geçici ya da kalıcı olarak ayrılan bu kişilerin erişim hakları konusunda düzenlemeler yapılmalıdır.

4.2.5. Fiziki ve Çevresel Güvenlik

Bu tezin 3.2.7.10 bölümünde fiziksel güvenlik ile ilgili bilgilendirme yapılmıştır. İlgili bölümde kurum personelinin çevresel risklerden nasıl korunacağından bahsedilmiştir.

Bunlara ek olarak kurumların bilgilerinin kurum sınırlarından girişi ve çıkışı da fiziksel güvenlik çerçevesinde değerlendirilmektedir. Kurum bilgi işleme cihazları kurum sınırları dışına sadece yetkili izin ile çıkabilmelidir. İçerisinde kurum bilgisi taşıyan disk, teyp gibi birimler elden çıkarılacakları, el değiştirecekleri veya atılacakları zaman önce içerisindeki bilgilerin kurtarılamayacak şekilde silindiğinden emin olunmalıdır.

4.2.6. İletişim ve İşletim Yönetimi

Tezin 3.2.7.3 (**Telekomünikasyon, bilgisayar ağları ve internet güvenliği)** ve 3.2.7.7 (**İşletme güvenliği)** numaralı başlıklarında iletişim ve işletim yönetimi konularına değinilmiştir. 2.1.1.5 (**Sürüm yönetimi)** ve 2.1.1.9 (**Bilgi teknolojileri kapasite yönetimi)** başlıklarıda 17799'un bu alt başlığı altında değerlendirilmektedir.

Kurumlarda çalışır halde bulunan iletişim altyapılarının ne ölçüde güvenliğe ihtiyacı olduğunun kurumun tüm birimlerinden gelecek görüşler ile belirlenmesi gerekmektedir. Bunun nedeni her birimin bilgilerinin gizlilik derecesini kendisinin tayin etmesi, bu bilgilerin ne kadar korumaya ihtiyaç duyduğuna da ancak kendisinin karar verebilmesidir. Kurumun iletişim altyapısının ne kadar güvenli olması gerektiğini kestirmek bu tür geri besleme ve birimler arası iletişim olmadan mümkün görülmemektedir.

Güvenlik işletimi kapsamı içerisinde değerlendirilen değişim yönetimi kapsamında, kamu kurumlarının tüm bilişim isteklerinin toplanacağı bir havuz kurulması önerilmektedir. Halihazırda kullanılmakta olan yardım masası yazılımı bu amaçla kullanılmalıdır. Kurum ihtiyacı olan personel, bunu herhangi bir izin ya da onay almadan yardım masasına bu durumu "istekler" bölümünde bildirmelidir. Kurum personeli elden geldiğince çok istek yapmaya teşvik edilmeli, gelen bu istekler sınıflandırılıp belli aralıklar ile değerlendirilmelidir. Kişilerin isteklerine ya da isteklerine temel olan sebeplere çözüm olabilecek sistemler önerilip, yönetim onaylar ise tedariki planlanmalıdır. Kurumda temel prensip, kişilerin rollerine bakılarak konfigürasyonlarının (bilgi, eğitim, donanım gibi konfigürasyonlar) yapılmasıdır. Kişiler bu konfigürasyona ulaşmak için istek yapmak zorunda kalmamalıdırlar. İstek belli bir roldeki personelden geldiğinde, isteğin tedariki onaylanıyor ise planlama bu tedarikin (yönetimin onayladığı istisnalar hariç olmak üzere) o roldeki tüm personel için yapılması planlanmalıdır.

Kurumlarda bilişim alanında yapılması istenen değişimlerin bir değişim planlama tablosunda tutulması gerekmektedir. Bilişim planlamalarında tedarik edilecek sistemler, teknik şartnameleri, yaklaşık maliyet hesapları ve tedarik sırasında ki sorumluluk dağılımı bir yıl önceden hazırlanmalı ve sürüm yönetimi yapılarak güncellenmelidir.

Kapasite yönetimi de bu alanda incelenmelidir. Kurum kapasite planlanması güvenlik açısından önemlidir. Kullanıcıların kullanmakta olduğu uygulamaların hacmi hesaplanmalı, her ihtiyacın disk alanı, işlemci yükü ve bilgisayar ağı gibi ihtiyaçları hesaplanarak bu sürecin çıktıları değişim planlama tablosuna girdi olarak kaydedilmelidir. Kurumlarda planlanan her önemli değişim (sürüm değişimi gibi) önce test ortamında test edilmelidir. Test sürecinin sonunda da değişimler her an eski bir duruma dönülebilecek önlemler alındıktan sonra yapılmalıdır.

Kurumlarda yerleşik bir yedekleme politikası olmalıdır. Kurumun bilgi varlığı listesinden alınan çıktılar göz önüne alınarak her varlığın yedeklendiğinden emin olunmalı, bu konuda verilecek sorumluluklar hiçbir kuşkuya yer verilmeyecek şekilde ilgili personele tebliğ edilip yedekliliğin kontrolü düzenli olarak yapılmalıdır. Yedekler, çalışıp çalışmadıkları konusunda düzenli olarak test edilmelidirler. Yedeklenmiş bilgiler detaylı olarak etiketlenmeli, yedekler güvenli merkezlerde tutulup fiziksel erişim kısıtlanmalıdır.

Kurumların bilgisayar ağlarında, internete erişimde, dosya sunuculara erişimde mümkün olduğunca çok kayıt tutulmalı, tüm personel bu kayıtların tutulduğu konusunda (önleyici tedbir) bilgilendirilmelidir. Kurumlar bilgilerini üçüncü taraflar ile paylaşma konusunda kurallar yetki ve sorumluluklar tanımlamalıdır.

Ek bir önlem olarak kurumlarda, inkar edilemezliği sağlamak üzere, resmi olarak teslim edilen tüm elektronik dokümanların sayısal imzalı olması talep edilmelidir. Elektronik İmza Kanunu[33] yürürlüktedir ve elektronik imza ıslak imza ile kanunen eşdeğerdir.

Kurumların bilgi sistemlerinde üretilen her bilginin kurum malı olduğu, kurumun kendi sisteminde üretilmese de herhangi bir şekilde sistemin içerisinde kayıtlı bulunan tüm veriler üzerinde her türlü tasarrufa hakkı olduğu prensibinin tüm bilgi sistemi kullanıcıları tarafından bilinmesi sağlanmalıdır.

[33] 5070 Sayılı Kanun, 17/01/2004

4.2.7. Erişim denetimi

Tezin **2.2.7.2. Erişim kontrol sistemleri ve yöntemleri** bölümünde detayları ile incelenmiştir.

Çalışanların şifrelerinin gizli kalmasının kendi sorumlulukları olduğuna dair bir belgeyi imzalamalarının yerinde olacağı değerlendirilmektedir. Kurum bilgi ağlarına erişimin sadece şifre ile değil, akıllı kartlar da kullanılarak yapılması güvenliği artıracaktır. Kurumda kullanıcı hesabı açmak gibi işlemler belli bir istek – cevaplama süreci takip edilerek yapılmalıdır. Bu tip isteklerin resmi yollardan yapılması ve resmi yollardan cevap verilmesi gerekmektedir.

Kurumlar, bilişim ağlarında gerçekleşen mümkün olduğunca çok kaydın merkezi kayıt sunucularında tutulması ve belirli aralıklarla yedeklenmesi gerekmektedir. Bu yedeklemelerin inkar edilemezliği sağlamak üzere yedeğin ne zaman kimin tarafından alındığı gibi bilgiler medyaların üzerine yazılarak alınması güvenilirliği artıracaktır. Bu medyanın zarar görmeyecekleri şekilde saklanmaları (manyetik etkileşim veya fiziksel hasar almayacakları ortamlarda) gerekmektedir.

Kurum bilgi ağlarının tümünün saat ayarları birbiri ile eşit olmalıdır. Kurum telefon, bilgisayar ağlarının zaman senkronizasyonunun aynı sunuculardan belirli aralıklar ile yapılması gerekmektedir. Erişim kontrolün bir ayağı da ayrıcalık yönetimidir. Kurum yönetimi eğer erişimler konusunda istisnalar yapmak isterse bu istisnalar yazılı ve imzalı olmalıdır.

4.2.8. Sistem Geliştirilmesi ve İdamesi

Sistem tedarikini de içeren bu başlığın hedefi güvenliğin tüm sistemlerin bir parçası olmasıdır. Tedarik edilen, kurum için özel geliştirilen yazılım ve donanımların güvenlik ilkeleri ile uyuşmaları gerekir. Bu güvenlik ilkeleri bilginin gizliliğini, erişilebilirliğini ve bütünlüğünü ön plana almalıdır.

Kurumlarda hangi verilerin şifrelenerek saklanması veya iletilmesi gerektiği risk incelemesi yapılarak belirlenmelidir. Verilerin belirlenmesinden sonra yetkiler belirlenmelidir. Şifre anahtarlarının oluşturulması ve bu anahtarların güvenli olarak saklanması gerekmektedir. Kurumlarda şifreleme uygulamasında, anahtar oluşturma ve saklanmasında, anahtarların dağıtılmasında, anahtarlar kaybolduğu zaman inceleme yapılmasında kimlerin yetkili olacağı görevler ayrılığı prensipleri göz önüne alınarak belirlenmelidir.

E-dönüşüm kapsamında, kurumlarda kullanımda olan bilgi sistemlerinin yazılım konfigürasyonlarının standart olması, resmi konfigürasyonun dışında sistemlere yazılım yüklenmemesi gereklidir. Aksi takdirde zararlı yazılımların sisteme zarar vermesini engellemek mümkün olmayacaktır. Kurumlarda yazılım sürüm yönetimi yapılıp, donanımlara özel yazılım kütüphaneleri oluşturulmalı, yazılımların ihtiyacı karşılamadığı belirlenince değişim yönetimi 2.1.1.4 gereklerince yazılımlar değiştirilmelidir.

Şifreleme algoritmaları dosya sunucusunda, iletişim hatlarında uygulanmalıdır. Şifrelemede TÜBİTAK UEKAE'nin milli algoritmaları kullanılmalı, şifreleme ve anahtar dağıtımı sistemlerinin kurulumunda UEKAE desteği alınmalıdır.

4.2.9. Bilgi Güvenliği Olay Yönetimi

Güvenlik politikasına ya da uyulması gereken mevzuata aykırı her bilgi güvenliği durumuna bilgi güvenliği olayı olarak adlandırılır. Bilgi güvenliği olay yönetiminin parametreleri ISO 20000 standardında bulunan olay yönetimi ile aynıdır ve kurumda iki standart da uygulanıyor ise iki süreç paralel işletilmelidir.

Güvenlik olaylarına örnek olarak, zararlı yazılımların sistemi etkilemesi, bilgi gizliliğinin ya da bütünlüğünün bozulmuş olması, bilgi sistemlerinin kullanılamaması veya bilgi sistemlerinin amaç dışı kullanımı sayılabilir. Bu veya benzeri bir olay olduğunda, önceden kimlerden oluştuğu tanımlanmış bir müdahale ekibinin olay yerinde tespit yapması, delilleri toplaması (örneğin sistemin sabit disk kopyasını alması) ve olayı önceden formatı belli bir rapor halinde yönetime bildirmesi gereklidir.

Güvenlik olaylarının sonucunda yazılan raporlar değerlendirilmeli, bu tip olayların bir daha olmaması için nelerin gerektiği tartışılmalıdır. Bilgi güvenliği olayı olduğunda hangi adımların atılması gerektiği konusu ayrıntılı mevzuat hazırlanmalı, bu mevzuat çerçevesinde; fiziksel evraklar için önlemler öngörülmeli, kurum personelinin fiziksel olarak bırakabileceği izleri takip amacıyla parmak izlerini ve el yazı örneklerini toplanması konusunda kurallar getirilmeli, güvenlik sızıntıları dikkate alınmalıdır. Kişiler nasıl fiziksel ortamda parmak izi bırakıyorlarsa, bilişim ortamlarında da izler bırakmaktadırlar. Bilişim ortamında sorumlulukların ve güvenlik soruşturmasının takibi süreci de mevzuatta ayrıntılı yer almalıdır.

4.2.10. İş Sürekliliği Planı (Ticari Süreklilik Yönetimi)

Tezin 3.2.7.8. **İş sürekliliği planı** bölümünde detayları ile incelenmiştir.

Kurumlarda iş sürekliliği kesintilerinin sebep-sonuç ilişkilerinin irdelenmesi gereklidir. Kurum süreçlerinin birbirleri ile ilişkileri, bu süreçlerin bazılarının kesilmesinin kurum işleyişine verebileceği zararlar ortaya konulmalıdır. Bu konuda nasıl bir çalışma yapılması gerektiği 3.2.7.8. İş sürekliliği planı konusunda anlatılmıştır. İlgili konuda belirtilen özelliklere sahip bir komisyonun iş süreklilik ve felaket kurtarma planlarını hazırlaması gerekmektedir. Kurumun en değerli varlıkları olan insanların bu planlarda 3.2.7.10. Fiziksel Güvenlik konusunda tarif edilen felaketlere karşı korunması öncelikle değerlendirilmelidir. Bu öncelik kurumun geneline anlatılarak, kurum çalışanlarının güvenlik çalışmalarına daha içten katkı yapmaları sağlanmalıdır.

4.2.11. Uyumluluk

Kurumlar ilgili mevzuata (kanun, yönetmelik) ve imzalamış olduğu sözleşme hükümlerine uymakla yükümlüdürler. Bu yükümlülüklerin ihlal edilmemesini sağlamak üzere yükümlülüklerin sıralanıp, kurum güvenlik politikalarına eklenmeleri gerekmektedir. Kanunlardan kaynaklanan riskler bu şekilde azaltılmış olur.

Kanuni yükümlülüklerin başında fikri mülkiyet hakları gelmektedir. Kurumlar diğer kişi ve kuruluşların fikri haklarını ihlal etmekten uzak durmalı, kurum bilişim ağlarında fikri hakların ihlal edilmesini yasaklamalıdırlar. Kişisel bilgiler ve kurumsal bilgilerin kaybedilmesi kanuni risklere yol açabilecektir. Özellikle hukuk ve sağlık sektörü gibi alanlarda bu risk artmaktadır.

Mevzuatın takibi sonucu kurumları ilgilendirebilecek her kanun, tüzük ve yönetmelik bir araya getirilip kurumun yükümlülükler listesi çıkarılmalıdır. Süreçler içerisinde bu yükümlülüklere uyum gerekiyor ise, kurum iç yönetmeliklerinde ve yönergelerinde değişiklikler yaparak kanuni uyumsuzluk risklerini azaltmalıdır. 2.2.7.9. Uyumluluk başlığında uyulması gereken başlıca kanunlar sıralanmıştır.

Kurum kullanmakta olduğu yazılım lisanslarını takip etmeli, lisansı olmayan yazılımların kullanımını önlemelidir. T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi'nin yayınlamış olduğu e-dönüşüm Türkiye

Projesi Birlikte Çalışabilirlik Esasları Rehberi[34] kamu kurumlarının bilişim ağları yönetimi ve yazılım kıstasları konusunda bağlayıcı niteliktedir. Bilgi Toplumu Dairesi'nin bu kapsamdaki tüm yayınları takip edilmelidir.

Birlikte çalışabilirlik esasları tüm kamu kurumlarını bağlayıcı nitelikte bir rehber dokümandır. Dokümanda dikkati çeken en önemli husus kullanımı ücret gerektirmeyen açık standartlara yönelten ifadelerdir. Rehberin kullanılmasını öngördüğü dosya ve iletişim standartlarının en önemlisi olarak açık OASIS[35] (Organization for the Advancement of Structured Information Standards) projesi görülmektedir. OASIS projesi değişik ofis yazılımlarının aynı dosya türü standartlarını kullanarak birbirleri ile uyumlu çalışmalarını sağlayan ortak ofis dosya türü ve iletişim standartlarının hepsidir. OASIS kelime işlem dosyalarının sonu ".odt", elektronik çizelge dosyalarının sonu ".ods" ve sunum dosyalarının sonu ".odp" ile bitmektedir. Rehber, OASIS standardının elektronik imza kullanımı da dâhil olmak üzere kamuda genel standart olmasının öngörüldüğünü belirtmektedir. Bir başka deyişle, kamuda resmi geçerliliği olan elektronik dokümanlar OASIS standardında olacaktır. Microsoft kendi sitesinde yapmış olduğu basın açıklamasında OASIS standardını destekleyeceğini açıklasa da bu desteğin standart Microsoft Office yazılımı ile gelmeyeceği, sonradan bir eklenti olarak yükleneceği belirtilmiştir. Desteğin standardın iletişim boyutlarını da tam olarak destekleyip desteklemeyeceği konusu da açık değildir. Kurumlar teknoloji seçimlerinde rehberin öngördüğü standardı desteklemeyebilecek yazılımları tedarik etmemelidir.

Açık kaynak kodlu yazılımların kullanımının kamu kurumlarındaki bilgi sistemlerinde denenmesi, maliyet etkinliklerinin lisans ücretli rakipleri ile karşılaştırılmasının kanuni uyumluluğun sağlanması için gerekli olduğu değerlendirilmektedir.

[34] DPT e-dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi, Temmuz 2005
[35] http://www.oasis-open.org/

5. SONUÇ

E-devlet Projesi kapsamında, kurumların bilgi güvenliği konusunda atması gereken adımları tanımlamadan önce, kamuda bu konuda ki gelişmeleri incelemek gereklidir. Bu konuda kaynak doküman DPT Bilgi Toplumu Dairesi'nin 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bilgi Toplumu Stratejisi ve ekli "2006-2010 Eylem Planı"dır. Planda kamu kurumlarının e-devlet ihtiyaçlarına istinaden yapılması gereken eylemler kurumlara görev olarak verilmekte, zaman planları oluşturulmakta ve beklentiler ortaya konmaktadır. Kurumların bilişim ihtiyaçları, bu çalışmalar takip edilerek belirlenmelidir. Güvenlik açısından önemli bulunan maddeler: (Eylem Planı, 2006-2010)

1. Yetmişaltıncı eylem kapsamında kamu kurumlarının ortak kullanımına açık "Bilgi Sistemleri Olağanüstü Durum Yönetim Merkezi"nin Türksat tarafından kurulması,
2. Seksenikinci eylem kapsamında fikri mülkiyet haklarının sayısal ortamda korunmasını sağlayacak yasal düzenlemelerin Kültür Bakanlığı tarafından hazırlanması,
3. Seksenyedinci eylem kapsamında kişisel verilerin korunması için Adalet Bakanlığı tarafından düzenleme yapılması ve,
4. Seksensekizinci eylem kapsamında UEKAE tarafından "Ulusal Bilgi Sistemleri Güvenlik Programı" hazırlanarak bilgisayar olaylarına acil müdahele merkezi kurulması ve kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanması, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilmesi ve eksikliklerin giderilmesi yönünde öneriler oluşturulmasıdır.

Özellikle seksensekizinci eylemin kapsamının anlaşılması kurumların bilişim güvenliği politikalarının belirlenmesinde etkili olacaktır. Bu eylem kapsamında hangi çalışmaların yapılacağı, UEKAE'nin DPT 2005 yılı eylem planında kendisine verilen kamu kurumlarında güvenlik taraması yapılması görevini bitirdiğinde sonuçları açıkladığı sunumda ortaya konmuştur. (Eriş, 2006, s. 15) UEKAE bu sunumunda aşağıda ki tespitlerde bulunmaktadır:

1. Kurum birimleri personel yetki ve sorumluluklarının belli olmaması.
2. Dış kaynak kullanımı ve satın alma kurallarının belli olmaması.
3. Bilgi güvenliği rollerinin belli olmaması.
4. Üst yönetimlerin bilgi güvenliği konusunda bilgisiz ve konuya ilgisiz olması.
5. Kamu kurumlarının kritik hizmetleri alabileceği yetkin bir güvenlik merkezinin olmayışı.
6. Bilgi sistem personelinin yeterli eğitime sahip olmaması.
7. Bilgi güvenliğinden sorumlu üst yöneticinin belli olmaması.

Tespitlerinde bulunmaktadır.

Bu tespitlerden yola çıkarak UEKAE aşağıdaki adımları sırasıyla atmaya karar vermiştir: (Eriş, 2006, s. 16)

1. Kamu kurumlarının az kritik, kritik ve çok kritik olarak sınıflandırılması.
2. Kamu bilgi sistemi yöneticileri günü hazırlanması.
3. Kamu kurumlarında "Bilgisayar güvenlik olaylarına müdahele" yeteneği kazanılması (müdahele sorumlularının tespiti, UEKAE ile iletişim kanalı kurulması vb.)
4. Çalıştay hazırlanması.
5. Kamu kurumları bilgi sistemleri güvenlik dokümanlarının hazırlanması.
6. Çok kritik kurumların "Asgari güvenlik önlemleri"ni uygulamaları ve denetlemeleri.
7. Çok kritik kurumların bilgi güvenliği eğitimleri hazırlamaları

olarak belirlenmiştir.

Kamu kurumları kendisi içinde de değişik yapıları olan birimleriyle çeşitlilik gösteren bir yapıya sahiptir. Çok gizli belge ve bilgileri ve çok hassas konuları barındıran kurumların bilgi güvenliği sorunu ulusal güvenlik sorunu haline gelebilmektedir. Bu anlamda kurumları bilişim stratejilerinin kritik düzeyde ele alınması gerekir. Bu konuda, ayrıntılı mevzuat düzenlemenin yanında, bilgi güvenliğini ve yönetimini sağlamak üzere hareket planı oluşturmalıdır. Planlama

değil icra makamlarına bağlı, Hareket Planını yürütmek üzere kurumun tüm birimlerini temsil eden değişik düzeylerde iki sürekli komisyon oluşturulmalıdır. Birinci komisyon, bilgi güvenliğinden sorumlu daire başkanı başkanlığında kurulacak olan sözleşmeli personel, uzman yardımcıları, uzmanlar ve şube müdürlerinden oluşan bir komisyon olmalıdır. Komisyon her daire başkanlığı seviyesinde birimi temsilen bir asil bir de yedek üyeden oluşmalıdır. İkinci komisyon ise bakanlıklar düzeyinde müsteşar başkanlığında toplanan, içerisinde müsteşar yardımcıları, daire başkanları veya hukuk müşaviri olan üst düzey bir komisyon olmalıdır. Alt komisyonun gerçekleştirdiği çalışmalar daha sonra görüş ve onay için üst komisyona sunulmalıdır. Alt komisyon, bilgi teknolojileri sistemlerinin kurumda etkinlik, verimlilik, gizlilik, bütünlük, erişilebilirlik, uyumluluk ve güvenilirlik esaslarına uygun olarak kurulabilmesi için gerekli eğitimleri almalıdır.

Alt komisyonların çalışma alanları ISO 20000 yapısının kurumlarda kurulması olmalıdır. Güvenlikten önce kurum bilişim sistemlerinden beklentilerini ve bu beklentilerin düzenli olarak karşılandığını planlamalıdır. ISO 20000 uygulaması çalışmalarında planlanması gereken alt çalışmalar şunlardır:

- Kurumların hangi iş süreçlerinin bilişim ortamında yürümesi gerektiğine karar verilmelidir. Bilgi sistemlerinin kullanım amaçları, bilgi sistemlerinden kurumun beklentileri yazılarak dokümante edilmelidir.
- Kurum varlık sınıflaması yapılmalıdır. kurum yazılım – donanım – bilgi envanteri çıkarılmalı, bu envanterin her birisinin sorumlusu belirlenmelidir. Fiziksel varlıkların etiketlenmesi gerekmektedir.
- Kurumlarda konfigürasyon yönetimine geçilmelidir. Kullanıcıların rollerine göre hangi yazılım – donanım'a sahip olmaları gerektiğine karar verilmelidir. Aynı rollere ve ünvana sahip kullanıcıların konfigürasyonu aynı olmalıdır.
- Konfigürasyonları belirlenmiş kullanıcıların işlerini yapabilmeleri için ne kadar kapasiteye ihtiyaçları bulunduğu tespit edilmelidir. Kurumda kapasite yönetimine geçilmelidir.
- Kurum varlıklarının ne tür bakıma ihtiyacı olduğuna karar verilip mümkün olan tüm yazılım ve donanımlar için hizmet seviyesi bakım anlaşmaları yapılmalıdır.

- Kurumlarda sürüm yönetimine geçilmelidir. Donanımlara yüklenecek yazılımlara konfigürasyon yönetimi ile karar verildikten sonra her donanım için "belirleyici yazılım kütüphanesi" oluşturulmalıdır. Donanımlara bu kütüphane dışında yazılımların yüklenmesi engellenmelidir. Belli bir sürüm yazılım veya donanım seviyesinden diğerine "Değişim Yönetimi" mekanizmalarınca geçilmelidir.
- Değişim yönetimi mekanizması kurulmalıdır. Kullanıcılar isteklerini belirlenmiş bir bilgi havuzuna göndermeli, bu istekler belli aralıklar ile derlenerek değerlendirilmelidir. Uygun bulunan istekler tedarik programına alınmalı, bulunmayanlar için gerekçeler yazılarak kayıt altına alınmalıdır. Kurumlar değişim yönetimi mekanizmaları ile planladığı tedarikler için en az altı ay öncesinden teknik şartname ve yaklaşık maliyet hesaplarını yapmış olmalıdır. Bu şekilde maliyet yönetimi sistemi de kurulmuş olacaktır. Değişim yönetimi mekanizmalarının dışında bilişim tedariki yapılmamalıdır. İstisnalar en üst seviyelerden onaylı olmalıdır.

Bu maddelerin uygulanması ile kamuda Bilgi Teknolojileri Yönetim Sistemi'nin temel adımları atılmış olacaktır. İlgili kurullar -olağanüstü durumlar dışında- yılda iki defa toplanmasının yeterli olacağı değerlendirilmektedir. Toplantıların özellikle bütçe belirleme dönemlerine uygun gelecek şekilde planlanmaları gerekmektedir.

Bir sonraki aşamada alt kurul kurumlarda, güvenlik politikası revize etme çalışmalarına başlamalıdır. Bu çalışmalarda 3.2.7.1. "güvenlik yönetimi" başlığında tarif edilen adımlar takip edilmelidir. Güvenlik çalışmalarında aşağıdaki hususlar özellikle gündeme gelmeli ve sonuca vardırılmalıdır:

- Fiziksel ve çevre güvenliği tehditlerinin kurum varlıkları üzerinde yarattığı riskler tanımlanmalıdır. Bu kapsamda kurumun bilgi varlıklarının kurum sınırlarından giriş – çıkışı, kuruma ait olmayan bilgi varlıklarının kurum ağına bağlı olması konularında politikalar üretilmelidir.

- Kurum personelinin ulaşmaya yetkili olduğu ve ihtiyacı olan bilgilere ulaşabilmesi için nasıl sistemler kurulması gerektiği (örneğin arşivde bulunan evraklar sayısallaştırılmalı mıdır vb.) karara bağlanmalıdır.
- Kurum personelinin işten ayrılması sırasında bilgi ayniyatı devri ve bilişim hizmetleri ilişik kesilmesi açısından hangi adımların atılması gerektiğine karar verilmelidir.
- Kurum ile üçüncü taraflar arasında imzalanmış sözleşmelerde bilgi paylaşımını ve koşullarını gerektiren maddeler incelenmelidir. Bilgi paylaşımı koşullarının 17799:2005 koşullarına uyup uymadığı raporlanmalı ve gerekirse anlaşma yenilenmelidir. (bkz. 2.2.2.1.)
- Kurumlarda iş sürekliliği planı hazırlanmalıdır. İş sürekliliği planı 3.2.7.8. İş sürekliliği planı konusundaki adımlar takip edilerek yapılmalıdır.
- Mevzuat takip edilerek, kurumların uyması gereken mevzuat, güvenlik politikası dokümanlarına belirli aralılar ile işlenmelidir.

Bilgi teknolojileri güvenliği ve yönetimi konusunda verilecek kararlar yılda iki defa tartışılarak karara bağlanmalıdır. Kurum personellerinin geniş katılımı ile verilecek bilgi teknolojileri hareket planı kararları, birimlerinin ortak ihtiyaçlarını belirleyebilmelerini sağlayacaktır. Bilgi teknolojileri kurumun iç işleyişini hızlandırırken, güvenlik süreçleri rollerin tanımlanmasını gerektirdiği için yetki kargaşası olmayacaktır. Sınırlı sayıda personel ile çok ve önemli işler yapmak zorunda olan kamu kurumları, bilgi teknolojilerini kullanarak iş gücünü en verimli ve etkin yöntemlerle kullanabilirken, bilişim dünyasının kendine has risklerinde de kendini korumuş olacaktır.

ÖZGEÇMİŞ

Bünyamin YILDIZ

09 Eylül 1975 yılında Adana-Aladağ ilçesinde doğdu. İlk ve Orta Öğrenimini burada tamamladı. Lisans eğitimini, Kırıkkale Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Kamu Yönetimi Bölümünde tamamladı. 2000 yılında Kaymakamlık sınavını kazanarak, Mersin Kaymakam Adayı olarak göreve başladı. Sırasıyla, Mersin Kaymakam Adaylığı, Sakarya-Taraklı Kaymakam V., Eskişehir-Alpu Kaymakam V., Çankırı-Kurşunlu - Bayramören Kaymakam V., Denizli-Güney Kaymakam V., Tokat-Yeşilyurt Kaymakamlığı görevlerinde bulundu. Halen Van-Bahçesaray Kaymakamlığı görevini yürütmektedir. İngilizce bilmektedir. Hobileri kitap okuma, müzik, spor, ağaç dikmektir. Evli ve bir çocuk babasıdır.

KAYNAKÇA

2003/12 No'lu "e-dönüşüm Türkiye" Projesi konulu T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü Genelgesi, 27/02/2003.

2003/48 No'lu e-dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı konulu T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü Genelgesi, 03/11/2003.

2005/20 No'lu Birlikte Çalışabilirlik Esasları Rehberi konulu T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü Genelgesi, 04/08/2005.

2005/05 No'lu e-Dönüşüm Türkiye Projesi 2005 Eylem Planı konulu Yüksek Planlama Kurulu Kararı (01/04/2005 tarih, 25578 sayılı T.C. Resmi Gazete).

5070 Sayılı "Elektronik İmza Kanunu" Kanun No. 5070 Resmi Gazete Sayı: 25355, 23/01/2004.

5237 No'lu Türk Ceza Kanunu (12/10/2004 tarih, 25611 sayılı T.C. Resmi Gazete).

Adalet Bakanlığı, Bilgi İşlem Dairesi Başkanlığı, 2007.

ANDRESS, Amanda, "Surviving Security: How to Integrate People, Process, and Technology, Second Edition", *Auerbach Publications,* 2004.

Bilgi Toplumu Stratejisi Eylem Planı (2006-2010) (28/07/2006 tarihli ve 26242 sayılı Resmi Gazete).

COBIT Audit Guidelines, *ISACA* ,Temmuz 2000.

COBIT Control Objectives, *ISACA*, Temmuz 2000.

COBIT Executive Summary, *ISACA*, Temmuz 2000.

COBIT Framework, *ISACA*, Temmuz 2000.

COBIT Implementation Tool Set, *ISACA*,Temmuz 2000.

COBIT Management Guidelines, *ISACA*,Temmuz 2000.

Department Of Defence Trusted Computer System Evaluation Criteria, 15/08/1983

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 01/1995, ISBN 0-16-045560-X.

DoD Standart, "TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA", CSC-STD-00l-83, l5/08/1983.

DÜLGER, Murat Volkan, "Bilişim Suçları", Seçkin Yayıncılık, 2004.

Emniyet Genel Müdürlüğü, Bilgi İşlem Dairesi Başkanlığı, 2007.

ERİŞ, Mehmet, "Türkiye Kamu Kurumları BT Güvenlik Analiz Sonuçları Çözüm Önerileri", Sunum Dokümanı, Tübitak Feza Gürsey Salonu, 13/06/2006.

European Parliment,"European Parliment Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)", 11/08/2001.

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

HERRMANN, Debra S., "A Practical Guide To Security Engineering and Information Assurance", *CRC Press,* 2001.

http://www.bilgitoplumu.gov.tr, 2007.

http://www.commoncriteriaportal.org, 2007.

http://www.isc2.org, 2007.

http://www.itgi.org, 2007.

http://www.oasis-open.org, 2007.

http://www.secoqc.net, 2007.

http://www.uekae.tubitak.gov.tr, 2007.

http://en.wikipedia.org/wiki/Information_technologies, 2007.

http://en.wikipedia.org/wiki/Confidentiality, 2007.

http://en.wikipedia.org/wiki/Rainbow_Series, 2007.

http://en.wikipedia.org/wiki/Personal_identification_number, 2007.

ISO/IEC 13335-1 Guidelines for the management of IT Security Part 1: Concepts and models for IT Security.

ISO/IEC 17799:2005, "Information Technology – Code of practice for information security management".

ISO/IEC 27001:2005, "Information Technology – Security Techniques – Information Security Management Systems – Requirements".

ISO 7498:1984, "Open Systems Interconnection - Basic Reference Model.

"IT Governance Global Status Report" PriceWaterhouseCoopers-ITGI, 2006.

İçişleri Bakanlığı, Bilgi İşlem Dairesi Başkanlığı, 2007.

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

National Information Assurance (IA) Glossary, 06/2006.

National System for Information Sysytems Protection, An invitation to a Dialogue, *The White House 2000*.

Presidential Decision Directive NSC/63, Critical Infrastructure Protection, 23/05/1998.

PURSER, Steve, "A Practical Guide To Managing Information Security", *Artech House*, 2004.

RFC 4301 , "Security Architecture for the Internet Protocol".

RFC 4309, "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)".

Sağlık Bakanlığı, Bilgi İşlem Dairesi Başkanlığı, 2007.

Sarbanes-Oaxley act of 2002.

T.C. Sayıştay Başkanlığı, "Hazine Bilişim Sistemleri Denetim Raporu", Ekim 2003

TIPTON, Harold F., KRAUSE, Micki, "Information Security Management Handbook, Fifth Edition", *CRC Press*, 2004.

VARLI, Ahmet Türkay, "Bilgi Sistemleri Denetiminde BDDK Yaklaşımı", Bankacılık düzenleme ve Denetleme Kurulu İnternet Sitesi, http://www.bddk.org.tr/turkce/yayinlarveraporlar/sunumlar/IT_Audit_BDDK_Yaklasimi_20_4_2006.ppt.

WYLDER, John, "Strategic Information Security", *Auerbach Publications*, 2004.