T.C.
BEYKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÖNETİMİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ BİLİM DALI

ITIL VE COBIT YÖNETİM STANDARTLARI VE BİR UYGULAMA

Yüksek Lisans Tezi

Tezi Hazırlayan

Orhan YILMAZ

İSTANBUL, 2014

T.C.
BEYKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÖNETİMİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ BİLİM DALI

ITIL VE COBIT YÖNETİM STANDARTLARI VE BİR UYGULAMA

Yüksek Lisans Tezi

Tezi Hazırlayan

Orhan YILMAZ

Öğrenci No:
120785005

Danışman
Asist. Prof. Dr. Talat FIRLAR

İSTANBUL, 2014

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "**Itil ve Cobit Yönetim Standartları ve Bir Uygulama"** başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. 15/08/2014

(İmza)

Aday: **Orhan YILMAZ**

Adı ve Soyadı : Orhan YILMAZ
Danışmanı : Asist. Prof. Dr. Talat FIRLAR
Türü ve Tarihi : Yüksek Lisans, 2014
Alanı : Yönetim Bilişim Sistemleri
Anahtar Kelimeler : ITIL, COBIT, Bilgi Güvenliği

ÖZ

Gelişen teknoloji ile birlikte bilgiler hızla çoğalmakta ve bu bilgileri eski yöntemlerdeki gibi basılı dokümanlarla takip etmek, depolamak ve geliştirmek günümüzde artık tercih edilmemektedir. Bilginin böylesine hızlı artması bilgi teknolojilerini de beraberinde geliştirmiştir. Böylece eski yöntemler bırakılıp bilgi teknolojileri kullanılmış ve artık bilgiye çok daha hızlı erişim kolaylığı getirilmiştir. Erişim kolaylığının yanı sıra özellikle organizasyonel olarak birçok bilgi ve verinin düzenli bir şekilde saklanması, bunların güvenliliğinin sağlanması iş hayatında büyük bir kolaylık sağlamıştır. Fakat bilgi teknolojilerinin getirdiği faydaların yanı sıra bilinçli bilinçsiz yapılan hatalar büyük sonuçlara mal olabilir. Bu durumda bilgiyle ilgili birçok düzenleme yapılması gerekebilir. Bu bağlamda Literatürde ITIL ve COBIT konuları sıklıkla araştırılan konular arasındadır. Fakat bu iki konunun bir arada incelendiği araştırma sayısı oldukça azdır. Bu eksiklikten yola çıkarak bu çalışma planlanmış ve literatüre katkıda bulunulması amaçlanmıştır. İncelemede, işletmelerin bilgi güvenliği yönetim sistemi kapsamında varlık ve risk yönetimlerinin yapılmasının önemli olduğu görülmüştür.

Name and Surname : Orhan YILMAZ
Advisor : Asist. Prof. Dr. Talat FIRLAR
Degree and Date : Yüksek Lisans, 2014
Area : Management Information Systems
KeyWords : ITIL, COBIT, Information Security

ABSTRACT

With improving information technology informations are increasing and the way they followed, storing and improving those informationsa are not the same as they are in the past. With the spread of information, information technology is raise and improve itself. Thereby, the trend of old techniques is decreased and it make informations to be easily achieved. Beside the accessibility opportunities, it provides many advanteges for many business area. In this way they can esaily keep many informations and organize it. Although information Technologies bring lots of advantages, they can also arise some problems. With or without intention, some mistakes can result in many lose for organizations. In that situation, there can be need of many readjustment about the informations. In that area, in the literatüre ITIL and COBIT are the two of the most investigated topic. However, there are few research that investigate these three topics. Due to low number of the research about that topic this investigation is prepared and desires to contribute in literature. In the survey, the information security management system as part of business assets and performing risk management was observed that be important.

İÇİNDEKİLER

Sayfa No.

İKİNCİ BÖLÜM
ITIL KÜTÜPHANESİ

ÜÇÜNCÜ BÖLÜM
COBIT STANDARTI VE MİMARİSİ

DÖRDÜNCÜ BÖLÜM
TEKNOLOJİ YÖNETİMİ

BEŞİNCİ BÖLÜM
RİSK ANALİZİ METODOLOJİSİ

ALTINCI BÖLÜM
GENEL KABUL GÖRMÜŞ DENETİM KONTROL VE UYGULAMA YÖNTEMLERİ

YEDİNCİ BÖLÜM
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN BİR FİNANS KURUMU ÜZERİNDE UYGULANMASI

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

AICPA :Yetkili Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants)

BDDK : Bankacılık Düzenleme ve Denetleme Kurumu

BGYS : Bilgi Güvenliği Yönetim Sistemi

BS : İngiliz Standartları ((British Standards)

BSI : İngiliz Standartları Enstitüsü (British Standards Instutie)

BT : Bilgi Teknolojileri

CBK : Bilginin Ortak Vücudu (Common Body Knowledge)

CISSP : Profesyonel Sertifikalı Bilgi Güvenliği Sistemleri (Certified Information Security Systems Professional)

CEO : İcra Kurulu Başkanı (Chief Executive Officer):

CIO : Bilgi Sistemleri Grubu Başkanı (Chief Information Officer)

CFO : Finans Grubu Başkanı (Chief Financial Officer)

CMDB : Konfigürasyon Yönetim Veritabanı (Configuration Management Database)

CMMI : Yetenek Olgunluk Model Entegrasyonu (Capability Maturity Model Integration)

COBIT : Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology)

ITIL : Bilgi Teknolojileri Altyapı Kütüphanesi (The Information Technology Infrastructure Library)

COSO :Treadway Komisyonu Sponsor Organizasyonlar Birliği (The Committee on Sponsoring Organizations Of The Treadway Commission)

DVD : Çok Amaçlı Sayısal Disk (Digital Versatile Disc)

DMZ : Askerden Arındırılmış Tarafsız Bölge (De Militarized Zone)

CD : Yoğun Disk (Compact Disk)

DS : Teslimat ve Destek (Deliver and Support)

DSS : Karar Destek Sistemi (Decision Support System)

E-Devlet : Yöneten İle Yönetilenler Arasındaki Yükümlülüğün Dijital Ortamda Gerçekleşmesi

EFQM : Avrupa Kalite Yönetimi Vakfı (European Foundation for Quality Management)

E-Posta : Elektronik Posta

IEC : Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)

GAO : US Merkezi Muhasebe Dairesi(The US General Accounting Office)

ISC : İnternet sistemleri konsorsiyumu (Internet Systems Consortium)

İSYS : İş süreci yönetim sistemi

ISACA : Bilgi Sistemleri Denetim ve Kontrol Birliği (Information Systems Audit and Control Association)

ISO : Uluslararası Standardizasyon Örgütü (International Organization for Standardization)

ISS : Internet Servis Sağlayıcı

IT : Bilgi Teknolojileri (Information Tecnology)

ITGI : BT Yönetim Enstitüsü (The IT Governance Institute)

ITSM : Bilgi Teknolojileri Hizmet Yönetimi (Information Technology Service Management)

KYS : Kalite Yönetim Sistemi

ME : İzleme ve Değerlendirme (Monitor and Evaluate)

ODM : Olağanüstü Durum Merkezi

OLA : Operasyonel Seviye Anlaşması (Operational Level Agreement)

PC : Kişisel Bilgisayar (Personal Computer)

PCAOB : Özel Şirketler Muhasebe Gözetim Kurulu (Public Company Accounting Oversight Board)

PO : Planla ve Organize Et (Plan and Organize)

RACI : İşi Yapmaktan Sorumlu, İşin yapılmasından Sorımlu, İş yapılırken danışılan kişi , Bilgi verilen kişi (Responsible, Accountable, Consulted, Informed)

SLA : Hizmet Seviye Taahhütnamesi (Service Level Agreement)

TBD : Türkiye Bilişim Derneği

TCB : Güvenilir Bilgi Temeli (Trusted Computing Base)

TTS : Talep Takip Sistemi

TS : Türk Standartları

TSE : Türk Standartları Enstitüsü

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

GİRİŞ

“Bilgi teknolojisi”, “bilgi ve iletişim teknolojisi” ve "bilgi ve telekomünikasyon teknolojisi" terimleri eş anlamlı olarak sıklıkla kullanılmaktadır. Günümüz modern dünyasında teknoloji ve zamanın ilerlemesiyle birlikte mevcut bilgi kaynaklarımız da yaşadığımız her an katlanarak artmaktadır. Bu bilgilerin artması kullanım alanlarının da gelişmesini sağlamakta ve artık bilgiye ulaşmak yaşamın birçok anında kritik hale gelmektedir. Bilgi teknolojileri gelişen bu ihtiyaçlar doğrultusunda güvenilir bilgi saklama ve geliştirme hizmetlerini kullanıcılarına sunmaktadır. Bilgiyi yaşamımızın her anında güvenli bir şekilde saklar ve geliştirir. Özellikle iş dünyasında kritik bir pozisyona sahip bilgi teknolojileri organizasyonlara iş hedefleri doğrultusunda ilerleme yolunda mevcut bilgileri depolama, analiz etme, geliştirme, güvenliğini sağlama, risk analizi yapma gibi birçok hizmet sunmaktadır. Diğer bir deyişle bilgi teknolojileri toplumda var olan bilgileri toplama, işlem yapma, depolama ve dağıtma işlerini yapan bir disiplindir. Elektronik bir işlem yapıldığında, bilgiler bir kayıt üzerinde ya da bir elektronik ortam üzerinde işlenmiş olsa bile yaşamımızın hemen her alanının bir parçasıdır ve tekrar kullanılması gerekebilmektedir. Bu nedenle, daha kapsamlı olmasından dolayı ‘bilgi teknoloji güvenliği’ teriminin yerine ‘bilgi güvenliği’ terimi kullanılmaya başlanmıştır. Ancak, ‘Bilgi teknoloji güvenliği’ terimi halen kaynakçada aynı anlamı taşımakta ve kullanılmaktadır

Bilgi böylesine hızla büyüyen bir toplumda kurumlar açısından büyük bir önem taşımakta ve yöneticiler de bu alana iş hedefleri yolunda ilerlemek adına büyük bir önem vermektedir. Bu kadar önemsenen bir konu olduğu için bilginin uygun şekillerde korunması gerekmektedir. Geçmişten günümüze, savaş dönemlerinde komutanların bilgi saklamak istemeleri örneğinde olduğu gibi bilginin muhafazası ve yönetimi hep önemli olmuştur. Özellikle organizasyonlara interdisipliner iş süreçlerinde bilginin alanlar arası aktarılması, anlaşılması ve risklerin değerlendirilmesi açısından çok kritiktir.

Bilgi, baskılı veya kâğıt üzerinde yazılı, elektronik olarak saklanan, posta veya elektronik postasıyla gönderilen, filmlerde veya konuşmalarda sözlü olarak ifade edilen birçok farklı biçimde bulunabilmektedir. Bilginin tekrar kullanılabilmesi

için uygun bir şekilde korunması gerekmektedir. Bu bilgileri ihtiyaçlar doğrultusunda toplamak ve istediğimiz zaman erişebilmek için öncelikle onların güvenliği sağlanmalıdır. Bilgi güvenliği bilgi teknolojileri oluşumun temel yapısını oluşturur. Güvenilir olmayan, hedeflerin dışındaki bilgi fayda sağlamaktan çok organizasyonları iş hedeflerinden ayırır ve büyük krizler yaşamasına sebep olur. Bilgi güvenliği sağlamak demek bilgileri çeşitli risklerden korumak, güvenliğini, iş sürekliliğini sağlamak ve riskleri en aza indirgeyerek iş kazançlarını yükseltmek anlamına gelir. Örneğin; bir şirketin müşteri bilgisi, finansal durumu veya yeni ürün dizini gibi mahrem bilgileri, iş kaybına, hukuki sorunlara ve hatta iflasa götürebilecek bir güvenlik açığı sebebiyle rakip firmaların eline geçmemelidir.

Kuramlarda BGYS (Bilgi Güvenliği Yönetim Sistemi) uygulanabilmesi için bilgi güvenliği kavramlarından önce bilgi teknolojileri sistemlerinin yönetim stratejilerinin neler olacağının belirlenmesi gerekmektedir. "Bilgi Teknolojileri Yönetim Sistemleri" olarak anılan COBIT, ITIL ve ISO27001 gibi standartların amacı, bilgi teknoloji hizmetlerinin müşterilere arzu edilen seviyede ulaşmasını sağlamak, bilgi teknolojileri sistemlerinin denetimini, gözlemlenebilirliğini, ölçeklenebilirliğini, işlevselliğini, verimliliğini, güvenilirliğini ve sürekliliğini sağlamaktır. Bilgi Güvenliği Yönetim Sistemi ise temel olarak aynı hedeflere atıflar yapsa da bilginin gizliliği, bütünlüğü ve kullanılabilirliği ile ilgilidir.

Bu çalışanın amacı işletmelerde bilgi güvenliğini araştırmaktır. Günümüzde işletmeler açısından en değerli varlığın bilgi olduğu bir dönemde bu bilgilerin güvenliğinin sağlanması büyük önem arz etmektedir. Bu çalışma işletmelerde bilgi güvenliği ile ilgili konuları detaylı açıklaması ve bu alanda ülkemizde kısıtlı çalışma yapılması açısından da önem taşımaktadır.

Bu araştırmanın literatür kısmındaki bilgiler tarama modeli kullanılarak konu ile ilgili kaynaklardan derlenmiştir. Araştırmanın uygulama kısmında ise nitel araştırma yöntemleri kullanılarak oluşturulan bir işletmenin bilgi güvenliği uygulamalarına yer verilmiştir.

Araştırmanın birinci bölümünde bilgi güveliği kavramı, ikinci bölümde ITIL kütüphanesi, üçüncü bölümde COBIT standardı ve mimarisi, dördüncü bölümde teknoloji yönetimi, beşinci bölümde risk analizi ve metodolojisi, altıncı bölümde genel kabul görmüş denetim kontrol ve uygulama yöntemleri konularına değinilerek

yedinci bölümde bilgi güvenliği yönetim standardının bir finans kurumu üzerine uygulanması gerçekleştirilmiştir.

BİRİNCİ BÖLÜM
BİLGİ GÜVENLİĞİ KAVRAMI

1. BİLGİ GÜVENLİĞİ

Bilgi güvenliği; bilginin gizliliğinin, güvenilirliğinin ve elverişliliğinin korunmasıdır. (TSISO /IEC 27001: 2006) Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır (Canber ve Sağıroğlu 2006, ss.7-10).

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

Şekil 1.Gözle-Yönlendir-Karar Ver-Harekete Geç Döngüsü

Kaynak: Kovacich, G. L., The information Systems Security Officer's Guide: Establishing and Managing an İnformation Protection Program. 2003, 4, 4

Model, idari olarak doğru verilmiş kararların kurumlan, 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.

1.1 Bilgi Güvenliği Tanımı

Güvenlik; tehlikelerden korunma, emniyet, korku ve endişeden korunma olarak tanımlanmaktadır (Maiwald 2003, 4). "Bilgi güvenliği; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaç ve doğru şekilde kullanılarak bilginin her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanır" (Sağıroğlu vd. 2004, ss.499-507).

Başka bir tanıma göre bilgi güvenliği: "Bilgi ve bilgi sistemlerinin yetkisiz erişimlerden, kullanımdan, ifşa edilmesinden, hasar görmesinden, değiştirilmesinden ve yok edilmesinden korunmasıdır. (http://www.ubak.gov.tr/ Erişim: 18.09.2014). "Bilgi güvenliği, kurumların bilgi envanterindeki varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini tehdit eden risklerin tanımlanıp, bu konuda risk yönetimi gereklerinin yapılmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olabilirliğine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir; riskin azaltılması, riskin kabul edilmesi, tamamen üçüncü bir tarafa devredilmesi (sigorta etmek gibi) veya risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir. Risklerin tanımlanması ISO 13335-115 standardında da gösterilmektedir. Bu standardın tanımı itibariyle bilgi güvenliği, bilginin risk yönetimini yapmaktır" (Yıldız 2007, 25).

1.1.1.Bilgi Güvenliğinin İlkeleri

1.1.1.1.Gizlilik

"Bilgi güvenliği sağlamadaki en temel unsur ebetteki gizliliktir (confidentiality). Bilişim sistemlerindeki gizlilik konsepti bilginin korunması ve yetkisiz erişimlerden ya da ifşa edilmesinin önlenmesiyle ilgilidir" (Lehtinen 2006,

110- 117).” Bilginin ve ilerleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesidir. Örneğin; ABC uygulamasının sadece yetkili kişilerce değiştirilebilir olmasıdır” (Alberts and Dorofee 2003, 102). Gizliliğin ihlali yetkilendirilmemiş kişilerin bilgiye erişmesi, bilgiyi görmesi, kullanması ve kopyalaması durumunda ortaya çıkar. Bilginin gizliliği bir mektubu (bilgiyi) kilitli bir kutuya koyarak göndermek ile ifade edilebilir. Kutuyu açmak için o kilidin anahtarına ulaşmak gerekir. Gizlilik Uluslararası Standartlar Örgütü (ISO) tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi olarak nitelenir. Günümüzde birçok bilişim ve telekomünikasyon firmasında şifreleme alt yapılarının kullanılmasının sebebi temel olarak bilgi gizliğinin sağlanılmasının gerekliliğidir. Gizlilik genel bir tanım olarak ise; bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir” (Önel ve Dinçkan, 2007, 6). Gizlilik, özellikle bir yasa, kanun veya standart dolayısıyla kurum için 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 (Yıldız 2007, 25).

National Information Assurance ’in tanımına göre bütünlük (veri bütünlüğü) dar güvenlik anlamında verinin yahut bilginin yetkisiz kişilerce değiştirilmesine veya yok edilmesine karşı korunmasıdır (IA, 2006, 34). “Bilginin göndericiden çıktığı haliyle bir bütün olarak alıcısına ulaştırılmasıyla bütünlük ilkesi sağlanır. Bilgi, alıcısına iletişim esnasında takip ettiği yollarda değiştirilmemiş, aralara yeni veriler eklenmemiş ve sıraları değiştirilmemiş şekilde ulaşır. Özetleme algoritmaları ise veri bütünlüğü sağlaması açısından kullanılır” (Tekerek, 2008, ss.132-137).

1.1.1.2.Erişilebilirlik

Erişilebilirlik bir sistem veya özkaynağın gereksinildiğinde kullanıma elverişli olma derecesi olarak tanımlanır (Kumas, 2007, 50). Bilginin gizliliği ile bilginin erişilebilirliği birbirini engellememelidir fakat bunun yanında erişilen bilginin bütünlüğünün sağlanması da önemlidir. Eğer bir bilginin sadece gizliliğini sağlayıp bilgiye erişimi kısıtlayıp engelliyorsak kullanım açısından bir fonksiyonu

olmayan bu bilgi bir şey ifade etmeyecektir. Aynı şekilde eğer erişimini sağlıyor fakat bütünlük sağlamıyor ise yanlış ve eksik bilgi aktarıp olumsuz sonuçlara sebep olabilir. Dolayısıyla bilgi güvenliği kavramı temel olarak bu üç unsurun bir arada sağlanması demektir (Doğantimur 2009, 52-56).

1.1.1.3.Hesap verilebilirlik

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, http://ia.net/, Erişim: 16.06.2014).

"Hesap verebilirlik ilkesi; alınan bir takım kararların doğru olup olmadığını kanıtlama ve sorumluluğunu kabullenme zorunluluğuna işaret etmektedir. Hesap verebilirlik ilkesi, yönetim işlevi ve sorumluluklarının belirtilmesini, hissedar ve yöneticilerin taleplerinin sıraya konulması ve nesnel kararlar verildiği yönetim kurullarınca izlenmesini öngörür" (Dinç ve Abdioğlu 2009,160). Hesap verebilirlik ilkesi, menfaat sahipleri ile ilgili hususlara değinmekte ve firma ile menfaat sahipleri arasında kurulan ilişkilerin düzenlenmesine dair ilkeleri açıklamaktadır. Bu ilişkiler içinde firmaların sorumlu olduğu kişilere karşı bilgi güvenilirliğini sağlamak ve bunun hesabını vermek gibi bir sorumluluğu vardır

1.1.1.4.Yetkilendirme

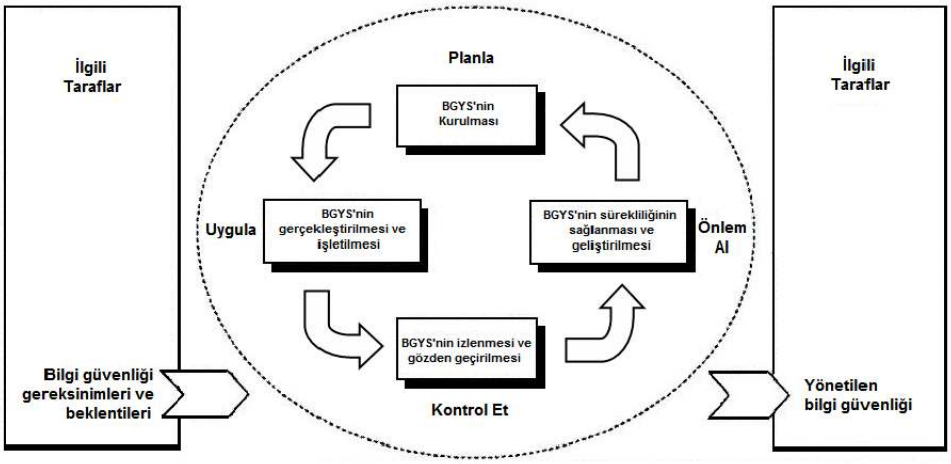
Bilgi güvenliği bakış açısından yetkilendirme kimlik doğrulama sistemidir. Bilgiye erişim sürecinde yetkilendirme, bilgiye doğru kişinin ulaşıp ulaşmadığını kontrol eden alt sistemdir (Yıldız. 2007, 64-68).

1.1.2.Bilgi Güvenliği İnceleme Alanları

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

- Bilgi Güvenliği Yönetimi
- Erişim Kontrol Sistemleri ve Yöntemleri
- Telekomünikasyon, Bilgisayar Ağları ve internet Güvenliği
- Uygulama Yazılımı Güvenliği
- Şifreleme
- Kurumsal Güvenlik Mimarisi
- Operasyon Güvenliği
- İş Sürekliliği Planı
- Mevzuat, İnceleme ve Değerler
- Fiziksel Güvenlik

2.Bilgi Güvenliği Yönetimi



Şekil 2. Bilgi Güvenliği Yönetimi Döngüsü (TBD Kamu-BİB 2008, 15-16)

Kaynak: TBD, **Kamu-BİB, Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri**, Kamu Bilişim Platformu, Sürüm 1.0, 2008.

Bilgi Güvenliği yönetiminde aşağıdaki süreçler izlenmektedir (TBD Kamu-BİB 2008, ss.15-16):

Planla (BGYS' nin kurulması): Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin oluşturulması.

Uygula (BGYS' nin gerçekleştirilmesi ve işletilmesi): BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi.

Kontrol Et (BGYS' nin izlenmesi ve gözden geçirilmesi) : BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.

Önlem al (BGYS' nin sürekliliğinin sağlanması ve iyileştirilmesi) : BGYS' nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi.

2.1.Erişim Kontrol Sistemleri ve Yöntemleri

Bilişim güvenliğinde en önemli konularda biri, kaynaklara kimin nasıl eriştiğini kontrol etmek, bu sayede bilgi üzerinde yetkisiz değiştirme ve açığa çıkarma olaylarını engellemektir. Bu amaçla yapılan faaliyetlere genel olarak erişim denetimi denir. Bir kullanıcı bilgisayarından ağ üzerindeki bir dizine ulaşmak istediğinde ona kullanıcı adı ve parola soran bir ekranla karşılaşması, erişim denetimine örnek olarak verilebilir. Erişim denetimi, yazılım ve donanım tabanlı olarak sağlanabilir

"İnterpol Computer Crime Manual" esas olmak üzere, 11.06.1999 tarihinde hazırlanan Emniyet Genel Müdürlüğü "Bilişim Suçları" raporunda suç tipleri aşağıdaki gibi ele alınmıştır (http://www.egm.gov.tr/Sayfalar/default.aspx, Erişim: 20.04.2014).

- **Yetkisiz Erişim**: Bir bilgisayar sistemine ya da bilgisayar ağına yetkisi olmaksızın erişmektir. Burada, suçun hedefi bir bilgisayar sistemi ya da ağıdır. "Erişim" sistemin bir kısmına ya da bütününe ve programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli değildir. Bu bir kişi tarafından bir bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de olabilir.

- **Yetkisiz Dinleme**: Bir bilgisayar veya ağ sistemine, sisteminden veya sistemi içinde yapılan iletişimin yetkisi olmaksızın teknik anlamda dinlenmesidir.

Burada, suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferinin teknik olarak takip edilmesi ve dinlenmesidir. Teknik anlamda dinleme, iletişim içeriğinin izlenmesi, verilerin kapsamının ya direk olarak (bilgisayar sistemini kullanma ya da erişme yoluyla) ya da dolaylı olarak (elektronik dinleme cihazlarının kullanma yoluyla) elde edilmesi ile ilgilidir. Suçun oluşması için hareket yetkisiz ve niyet edilmiş olarak işlenmesi gerekir. Uygun yasal şartlar çerçevesinde soruşturma yetkililerinin yaptıkları bu kategoriye girmez.

- **Hesap İhlali**: Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının bilgisayar sistemlerinde bulanan hesabını kanunsuz olarak kullanmaktır. Bir kişinin, İnternet, telefon veya benzer bir sistemdeki hesabının kişinin rızası olmaksızın kanunsuz olarak kullanılmasıdır

2.2.Telekomünikasyon, Bilgisayar Ağları ve Internet Güvenliği

Günümüzde, dünyada çok sayıda internet üzerinden bilgisayar kullanıcısı olduğu bilinmektedir. "Türkiye'de de 15-20 milyona ulaşmış durumdadır. Gelişen mobil ve kablosuz sistemler kullanıcılarına birçok hizmet sunarken berberinde pek çok güvenlik problemleri de getirmektedir. Bu da hizmet sağlayıcılarına mobil ve internet ortamında güvenli bir hizmet verebilmek için bazı sorumluluklar yüklemektedir. Sağlayıcılar bu amaçla çeşitli güvenlik politikaları belirleyip bu stratejileri güvenli bir hizmet için sağlamaktadır" (Sağıroğlu ve Bulut 2009, ss.499-507).

2.3.Uygulama Yazılımı Güvenliği

Yazılımlarda ortaya çıkan güvenlik eksikliklerinin ana nedeni genellikle yazılım geliştirilirken her aşamada güvenliliğin aynı titizlikle ele alınmamasıdır. Bu konuyla ilgili sayabileceğimiz en temel özelliklerden biri yazılımın tehdit modellemesi yapılmamasıdır. Tehdit modellemesi yapılmayan bu yazılımlar ileriki süreçlerde daha büyük problemler olarak ortaya çıkar. Bunun yanında gereksinim

analizi yapılırken ortaya çıkan hatalar da bunun sebeplerindendir. Ayrıca yazılımın sadece fonksiyonellik özelliğinin üstünde durulup güvenlik testlerini ihmal etmek de bu problemlerden biridir. Yazılım geliştirme sürecinin ilk yıllarından beri kaliteli ve kullanılabilir yazılımlar üretmek için çalışmalar yapılmaktadır. Fakat günümüzde güvenli yazılım geliştirmek amacı daha önce tutuluyor ve bu amaç doğrultusunda bir çok model ve ana çatı üzerinde çalışılmıştır.

"Yazılımların kaliteli olarak geliştirilmesi amacıyla CMMI (Capability Maturity Model Integration) gibi standartlar ortaya konmuştur fakat yine de bu standarda uygun geliştirilen yazılımların güvenlik sorumluluğu bir güvence vermemektedir. Güvenli yazılım geliştirme döngüsü oluşturma ile ilgili çeşitli standartlar geliştirilmektedir. Microsoft tarafından geliştirilen SDL (Security Development Lifecycle) metodu ve OpenSAMM metodolojisi bu tür standart çalışmalarına örnektir. Bu alandaki çalışmaların daha olgunlaşarak devam etmesi beklenmektedir" (Sağıroğlu ve Bulut 2009, 499-507).

Şifreleme

Şifreleme, bilişim güvenliğinin en önemli alt gereksinimlerinden birini oluşturmaktadır. Şifreleme, uygun anahtarı olmadan kimsenin çözemeyeceği şekilde mesajların dönüştürülmesidir. Şifreleme depolanan ve kullanılan bilgileri istenmeyen kişilere karşı matematiksel kodlarla korur. Şifreleme işlemi sayesinde yetkisiz kişilerin bilgi erişimi engellenir, bu kişiler dosyalar erişseler dahi bilgiyi anlaşılmaz hale getirir ve kullanılmasını engeller (Kahraman 2006, 22-28). İletişimde de şifreleme önemli bir rol oynamaktadır. İletişimde şifreleme hem üçüncü bir kişinin mesajı okuyamamasını hem de mesajı gönderen kişinin mesajı gönderdiğini inkâr edememesini sağlamaktadır. Şifreleme sistemlerinde şifrenin gücünü belirleyen en önemli parametre olan anahtar, bir dizi rastgele bir ve sıfırdan oluşmaktadır. İkili sistemde gösterilen bu anahtarın uzunluğu şifrenin gücünü belirler. Bu uzunluklar genelde ikinin üsleridir ve şifreleme algoritmaları ile özdeşleştirilmiştir. Şifreleme günümüzde birçok devlet tarafından ilgi görmektedir ve Amerika Birleşik Devletleri, Küba, Irak, İran, Libya, Kuzey Kore, Sudan ve Suriye'ye şifreleme teknolojisinde

ihraç yasağı uygulamaktadır. Bir çok ülkenin şifrelemeye olan bu ilgisinin artmasıyla birlikte hükümet kısıtlamalarının artması beklenmektedir. (Kahraman 2006, 22-28).

2.4.Kurumsal Güvenlik Mimarisi

Kurumsal güvenlik mimarisinin amacı, ağ güvenlik altyapısı, ilgili güvenlik mekanizmaları ve ilgili güvenlik politikaları ve prosedürleri kavramsal tasarı sağlamak için belli bir düzen içinde tutmaktır. Kurumsal güvenlik mimarisi bileşenleri farklı konuları içinde bulundurup tek amaca hizmet eder. Bu bileşenler uyumlu bir birim oluşturarak güvenlik mimarisini oluşturur. Bu bileşenler kavramsal bir tasarım sağlayarak güvenlik hizmetini organizasyonun bir problemle karşılaşmayacak şekilde düzenler.

Bilgi veya Veri Aldatmacası (Data Diddling): Veri aldatmacası, verinin bilgisayara veya hafızasına kaydında değiştirilmesi veya bu yöntemle bilgisayara yanlış veri girilmesi veya bazı verilerin kasten bırakılması anlamına gelmektedir. Böylelikle fail, bilgisayara girdiği veya bilgisayarda bıraktığı bilgilerle var olan veriler üzerinde istediği yönde değişiklik yapma veya ekipmanı istediği yönde kullanma imkanına kavuşmaktadır(Yazıcıoğlu ve Yılmaz 2005, 2). **"**Verilerin şifrelenmesi, dosyalanması, ulaştırılması, kontrolü ve bilgisayara girilmek üzere dönüştürülmesi ancak bu verilere erişme imkanı olan çalışan tarafından değiştirilebilir. Bu işlem dokümanların tahrif edilmesi, veri ortamlarının (manyetik bant, disk veya disket) özel olarak hazırlanmış materyallerle değiştirilmesi, kartlara ek karakter kaydı, bazı kayıtların iptali veya manuel kontrolden kaçınılması gibi metotlarla yapılabilir" (Doğan 1992, 156).

Truva Atı (Trojan Horse): Truva atları bilişim sistemlerine herkesin kullanımına açık ağlardan, internet üzerinden herhangi bir web sayfasından kopyalanarak sistemlere girmektedirler. Truva atları genellikle kullanıcıları cezp ettirecek adlar altında bulunduklarından ötürü kullanıcılar kolayca programları sistemlerine bulaştırabilmektedirler. Kullanıcı farkında olmadan onun yerine kendiliğinden süreç başlatan bir fonksiyondur. (Kurt 2005, 63). Birçok bilgisayar kullanıcısı tarafından

edinilmek istenebilecek faydalı bir yazılıma Truva atı yazılımı da ilave edilmekte ve herkese bulaşması istediğinden ötürü internet üzerinden ücretsiz olarak dağıtılmakta veya elektronik posta aracılığıyla kullanıcılara ulaştırılmaktadır. Kullanıcı programın faydalı işlevlerinden istifade etmektedir ve hiçbir şeyden kuşku duymamaktadır. Bu yazılımı bilgisayarına yükleyen kullanıcı, yazılımın görünüşte faydalı olan tarafından yararlanmaktadır. Bu arada Truva atı yazılımı da kurulmuş olduğu bilgisayarın işletim sistemi açıklarından yararlanarak, kendisini gönderenin bütün komutlarını yapmaktadır.

Salam Tekniği (Salami Techniques): Genellikle bankacılık sektöründe yapılan bir bilişim suçudur. Bu yöntemle banka hesaplarına yatırılan paraların küsuratlı kısmı başka bir başka hesabına aktarılır ve küçük miktardaki paralar başka bir hesapta birikerek büyük bir meblağ olur. Bu yöntem Truva atı programı ile kullanılır. Bu suç türünde hesaplardaki rakamların virgülden sonraki rakamların ya son rakamı ya da son iki rakamı failin belirlediği bir hesaba transfer edilerek orada biriktirilmektedir. Bankalar, mevduat faizlerini değiştirdiğinde veya hesaplarda işlem gerçekleştirdiklerinde ortaya çıkan kuruşların ondalık hanelerini hesaba ilave etmekte veya etseler bile şahıslar için önemsenmeyen bu rakamların saptanması ve izlenmesi oldukça güçleşmektedir (Yazıcıoğlu ve Yılmaz 2005, 4).

Süper Darbe (Super Zapping): Süper darbe, bilgisayar sistemlerinin çeşitli nedenlerle işlemez duruma gelmesi yani kilitlenmesi halinde çok kısa bir zamanda sistemin yeniden çalışmasını sağlamak üzere güvenlik kontrollerini aşarak sistemde değişiklik yapılabilmesi için geliştirilmiş bir programdır. Bu program geliştirilme maksadına uygun olarak kullanıldığında çok yararlı olmasına karşın kötü niyetli insanlar tarafından kötü amaçlar için kullanıldığında çok tehlikeli olabilmektedir. Bir Amerikan bankası veri-işlem görevlisi, sistemde oluşan bir hatayı düzeltmek için kullandığı süper darbe programının güvenlik önlemlerini ortadan kaldırdığının farkına varmış ve arkadaşlarının hesaplarına yüklü miktarlarda para aktarmıştır. Bu olay bir banka müşterisinin hesabında meydana gelen azalmayı fark etmesi durumunda ortaya çıkmıştır (Turhan 2006, 12).

Gizli Kapı veya Hile Kapısı (Trap Doors): İşletim sistemleri veya çok işlevli ve kullanıcılı sistemleri hazırlayan bilgisayar programcılarının ileride ortaya çıkabilecek

durumlara göre, sistem şifrelerinde değişiklik yapabilmeyi veya yeni şifreler girebilmeyi sağlamak üzere sisteme bıraktıkları çeşitli giriş imkanlarına denilmektedir. Böyle bir değişikliğe kapalı olan şifreler üzerinde, ortaya çıkan yeni koşullara göre ayarlama yapabilme imkanı yaratılmak istenmektedir (Yazıcıoğlu ve Yılmaz 2005, 4). Bu metotta kötü niyetli kullanıma olanak sağladığından bilişim suçlarının işlenmesinde kullanılabilmektedir.

Bug-Ware: "Bug-ware tam anlamıyla bilişim suçu sayılamayacağı ileri sürülmektedir. Belirli fonksiyon kümelerini düzenlemek için tasarlanan bilgisayar programlarını temsil eden bir terimdir. Fakat uygun olmayan ve zor anlaşılır, karışık programlanmaları sebebiyle sistem yazılımlarına ve donanımlarına zarar verebilirler. Yanlış mantık akışı ve program parçalarının, uygun olmayan bir biçimde toplanması sebebiyle istemeyerek bile olsa donanımlara ve verilere zarar verebilirler" (Doğan 1992, 156).

Mantık Bombaları (Logic Bombs): Mantık bombaları Truva atı yazılımının bir alt türüdür. Sisteme çok büyük yıkım ve hasarlar veren mantık bombaları bilişim sistemini çeşitli yolarla yanıltarak bozmaktadırlar. Mantık dışı ve yapılan işlemin aksine sisteme sürekli yanlış bilgi gönderir ve bunlarla sistemi doldurur (Yazıcıoğlu, R. Yılmaz 2005, 4).

Eş zamanlı Saldırılar (Asynchronous Attacks): Çok işlevli program teknikleri, bilgisayarda varolan birçok programın, bilgisayar kaynaklarını çeşitli usullerle kullanmak maksadıyla işlem yapmalarına imkan sağlamaktadır. İşte birçok sistemin varolan programları eş zamanlı kullanamamasından hareket eden bazı failler, geliştirdikleri eş zamanlı saldırı teknikleriyle bilgisayar işletim sistemlerinde, daha doğrusu programdaki veriler üzerinde çeşitli ihlâller oluşturmaktadır(Yazıcıoğlu ve Yılmaz 2005, 4).

Artık Toplama (Scavenging): Artık toplama da denilen bu teknikte bir bilgisayar sisteminin çalışmasında geriye kalan veri ve bulguların toplanması işlemi ifade edilmektedir.

Saatli Bombalar (Time Bombs): "Nümerik veya zamana bağlı çevresel değişkenlerin aldıkları duruma göre koşulsal olarak, zararlı bilgisayar komutlarını

yerine getiren programlardır. Genelde mantık bombaları ile aynı yapıya sahiptirler ve belirli bir sayıda çalıştırıldıktan sonra, belli bir tarihte örneğin 1 Nisanda patlayacak şekilde programlanabilirler"(Doğan 1992, 156).

Bilgisayar Virüsleri: Bulundukları bilgisayarlar çalıştığında kendini diğer sistemlere kopyalayarak uygun ortam oluştuğunda çeşitli işlemler gerçekleştirerek sistemlere zarar vermektedirler. Yerleştikleri yerlere göre boot virüsleri ve dosya (file) virüsleri ve daha sonra Microsoft firmasının ürünlerinde ortaya çıkan virüs biçimi olan makro/mail virüslerinin de eklenmesiyle üçe ayrılmaktadırlar. Boot Virüsleri, disketlerin veya sabit disklerin açılırken çalıştırıldıkları boot (açılış) sektörlerine yerleşirler. Bilgisayarlar açıldıklarında ilk olarak disklerin "boot" adı verilen sektöründe bulunan komutları çalıştırırlar. Boot virüsleride buralara yerleşerek sistem daha çalışır çalışmaz kendilerini aktif hale getirirler. Dosya virüsleri de dosyalara bulaşırlar. Dosya çalıştırıldığında devreye girerler. Bilgisayar açık kaldığı müddetçe çalıştırılan her dosyaya kendini kopyalar. Makro virüsleri ise özellikle Word, excel gibi programlara bulaşarak makroyu çalıştırırlar. Mail virüsleri, en hızlı yayılan ve zarar verme olasılığı yüksek olan bir virüs türüdür. 1948 yılında geliştirilen ve kendi kendini kopyalama özelliği bulunan auto isimli program virüslerin ilk atası olarak kabul edilmektedir. Bu programlar ilk yapıldıklarında sistemlerde dolaşarak kendileri için belirlenen legal işlemleri gerçekleştiriyorlardı (Çekiç 2006, 25). Bilgisayar virüsleri, yazılımdan yazılıma, dosyadan dosyaya, sistemden sisteme kolaylıkla kopyalanabilmektedirler. Bu kopyalanma işlemine günlük kullanımda "virüs bulaşması" denilmektedir. Bilgisayar virüsleri bulaştıkları bilişim sisteminde bulunan yazılımları çökerterek, sisteme olası en fazla zararı verecek şekilde tasarlanmışlardır. Bilgisayar virüsleri bir yazılıma ya da dosyaya fark edilmeyecek şekilde yerleşirler ve sonra kendi kendilerini kopyalayarak çoğaltırlar. Son olarak sistemleri veri depolama üniteleri basta olmak üzere kullanılamaz hale getirirler. Bilgisayar virüsleri, bilgisayarda yerleştikleri yerlere göre "boot virüsleri" ve "dosya (file) virüsleri" olmak üzere iki gruba ayrılmaktaydılar. Ancak Microsoft firmasının 1995 makro komutları yazmak için programlama dili olan "WordBasic"i geliştirmesinden sonra "makro/mail virüsleri" de oldukça fazla yaygınlaşmış ve üçüncü grup olarak kabul edilmiştir

Yazılım Bombaları (Software Bombs): Bir virüs çeşidi olan yazılım bombaları, kütük organizasyonunu tahrip etmek için kullanılır ve sisteme girdiklerinde verilere çarparak yok ederler. Bu durumda ne bir uyarı ne de önceden bir belirti söz konusudur.

Solucanlar (Worms): "Ağ solucanları kendi kendilerine çoğalırlar başka bir programa ihtiyaç duymazlar. Herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve tam bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programdır" (Kurt 2005, 63).

Tavşanlar (Rabbits): Bilgisayar virüslerinden biri olan tavşanlar, adlarına yakışır bir şekilde çok hızlı ürerler. Bellekte veya diskte alan tükeninceye kadar kolonileşirler. Burada amaç, özellikle çok kullanıcılı sistemlerin, iletişim ağ ortamlarında ana sistem bilgi isleme gücünü yitirinceye kadar sistemin kaynaklarını kurutmaktır. Tavşanlar ile virüsler arasındaki en belirgin fark, tavşanların kullanıcı veri kütüklerinin sonuna eklenmemeleri, asalak özelliklere sahip olmamaları ve kendi kendilerine yetebilmeleridir(Doğan 1992, 156).

Bukalemun (Chameleon): Çoklu ağ sistemlerinde kullanıcılara ait bilgileri gizli bir dosya içerisine kaydederek, kendini belli etmeden arka planda çalışan sistem yazılımıdır. Bilgisayar bağlantısının geçici bir süre mantıklı bir sebep yüzünden tekrar açılıp kapanacağı veya sistemin kapanması gerektiğini kullanıcıya ileterek bilgisayar bağlantısının kapanması sağlayan bu yazılım, kullanıcı tarafından bilgisayar yeniden işlem görürken gizli dosyalama yaptığı kullanıcılara ait bilgileri ilgili kişiye iletir. Böylece fail kişisel bilgi hırsızlığı yöntemi ile dolandırıcılıktan hırsızlığa her çeşit suç türünü işleyebilir.

Tarama (Scanning): Bilişim sistemlerine, değeri her seferinde değişen verilerin hızlı bir şekilde girilmesi suretiyle, sistemin olumlu cevap verdiği durumların tespit edilmesine yönelik bir tekniktir. Tarama, bilişim sistemlerinin telefon numaralarını veya Internet'e bağlı sistemlerin İP numaralarını bulmaya yönelik olabileceği gibi numarası belli olan, fakat şifre ile korunmuş sistemler için bu şifreleri bulmaya yönelik de olabilir(Kurt 2005, 63).

İstem Dışı Alınan İletiler-Yığın İleti (SPAM): Spam eylemine "spamming", bunu gerçekleştirene ise "spammer" denilmekte olup spam kelimesi yerine Türkçe' de "istem dışı ileti" veya "yığın ileti" terimleri kullanılmaktadır. Spam tanımında dikkati çeken nokta istem dışı, zararlı, zaman kaybettirici ve çok sayıda olma özelliğidir. Spamın içeriğini, ürün-hizmet reklâmları, ilaç-kozmetik ürünleri, illegal içerik-pornografi, hemen zengin ol-evinden para kazan yöntemleri oluşturmaktadır. Fransız Ulusal Enformasyon ve Özgürlük Komisyonu'na göre spam, hiçbir temas olmaksızın tartımsa forumlarından, dağıtılan listelerden ve web sayfalarından elde edilen elektronik adreslere alıcının talebi olmaksızın ara sıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalardır. Amerika Birleşik Devletleri'nin çeşitli eyaletlerinde e-posta yoluyla reklâm yapılması kanunlarla yasaklanmış(Memiş,http://hukukcu.com/modules/smartsection/item.php?itemid=29,2013, Erişim: 18/08/2014) ve ABD'de 2004 yılında "Can Spam Act of 2003" adlı spam ile mücadele amaçlı bir yasa çıkarılmıştır.

Ülkemizde de artık ticari reklâmların yanında siyasal reklâmların dahi cep telefonlarına kısa mesaj göndermek suretiyle yapıldığı görülmektedir. Spam faaliyetleri ilk bakışta önemsiz gibi görünse de 2004 yılı itibariyle Amerika Birleşik Devletleri'nde meydana çıkardığı zararın 10 milyar Dolar290, Avrupa şirketleri için ise yıllık 2.5 milyar Euro üretkenlik kaybına sebep olduğu nazara alınırsa önemi ve tehdit boyutu ortaya çıkmaktadır. Yığın ileti faaliyeti (spamming) zamanla çeşitlenmekte ve farklı isimlerle anılmaktadır ki örnek olarak "phishing" (olta atmak) ve "vishing" gösterilebilir. "webpage spoofing" olarak da bilinen "phishing" örneğin bir bankanın web sitesinde olduğunu sanarak güvenle şifre bilgilerinin elde edilmesi yöntemidir. Bu yöntemlerle aldatmak suretiyle önemli bilgiler elde edilmektedir.

Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme: Amerika ve Almanya'da çok sık olarak görülen bu suç tipinde, kendisine internet adresi (domain name) almak isteyen kişinin, bir İSS'ye yaptığı müracaat, sisteme müdahale eden bilişim korsanı veya bu bilgiye ulasan çalışan tarafından kendileri veya üçüncü bir kişi adına daha hızlı davranılarak kaydettirilir. Daha sonra bu internet adresi yüksek ücretlerle satılır. Web sayfası yönlendirme ise, Avrupa, Orta doğu, Asya'nın bazı bölümleri ile Afrika'nın kuzey bölümlerinin internet adreslerini dağıtmaktan sorumlu olan

“Reseaux IP Europeens Network Coordination Center” (RIPE) adlı organizasyonun veri bankasında bulunan web sayfalarına, internet üzerinden nasıl ulaşılacağına dair “routing” kurallarının yapılan müdahalelerle değiştirilerek internet kullanıcılarının farklı internet adreslerine çekilmesi suretiyle işlenmektedir.

Yerine Geçme (Masquerading): Bir ağa bağlı olan bilgisayarlara tanınan erişim imkanları sınıflara ayrılabilir. Bazı bilgisayarlara daha geniş erişim imkânı tanınırken diğer bilgisayarlar için bu imkân sınırlandırılabilir. Bu gibi durumlarda, herkesin erişim hakkı, erişim kodu ve parolasıyla belirlenir. Ama sistemde yapılacak ufak hileler ile erişim hakkı olmayan ya da sınırlı olan şahıslara erişim hakkı sağlanabilmektedir. Sistemde yapılan hile, erişim yetkisi olan bir kişinin parola veya erişim şifresinin yazılması yoluyla yapılıyorsa bu "yerine geçme" olarak isimlendirilmektedir

Gizlice Dinleme (Eavesdropping): Antik Anglo-Sakson hukukunda, “eaves” adı verilen komsu evin saçağına “eavesdrip” olarak ifade edilen, bir mesafeye bir kimsenin gizlice yaklaşması eylemi sonucunda para cezası ile cezalandırılması söz konusu idi. Kaynak terimini anılan suçtan alan gizlice dinleme eylemi, telefon hatları, e-mail, anlık mesajlar ve diğer iletişim araçları üzerinde yapılan özel görüşmelerin gizlice dinlenmesi anlamına gelmekte fakat kamuya açık yapılan yayınlar bu kapsama girmemektedir. (acikarsiv.atilim.edu.tr/browse/280/ fatma_burcu_nacar.pdf Erişim: 18.09.2014). Bu eylem telefon hattı üzerinde gerçekleştirilirse “telephone tapping”, optik fiber hattı üzerinde gerçekleştirilirse “fiber tapping” adını almaktadır. Bu son yöntemin mümkün olduğuna çoğu kimse tarafından inanılmamaktadır. Bu eylem bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek veya bilişim sistemlerinin az da olsa yaydığı elektromanyetik dalgaların yakalanarak verilerin tekrar elde edilmesi tekniğidir. Gizlice dinleme tekniği, özellikle bilgisayar ekranlarının yaydığı elektromanyetik dalgaların yakalanması ve tekrar ekran görüntüsüne çevrilmesi suretiyle işlenebileceği gibi bilgisayarlar arasında veri naklinde kullanılan ağlara yapılan fiziksel müdahaleler sonucu, ağda nakledilen verinin elde edilmesi seklinde de islenmektedir.

Sahte Elektronik Posta (Fake Mail): E-posta adreslerini yığın e-posta gönderen şahıs ve kurumlara temin etmek için hazırlanan sahte içerikli e-postalarda sosyal

mühendislik teknikleri yaygın olarak kullanılmaktadır. Bu tür e-postalar, toplumsal yönden tepki yaratması amaçlanan aldatıcı, yanlış bilgiler içermekte ve genellikle son bölümlerinde çok sayıda kişiye iletilmesi için telkinler yer almaktadır. Bir ülke ya da kuruma yönelik gerçek dışı bilgiler, sağlık ile ilgili tehditler, kan aranması, zor durumdaki şahıslara yardım talebi gibi çeşitleri bulunan e-posta aldatmacaları uzun senelerdir kullanılmakta olan etkin bir metottur (İlbaş 2009, 12).

Denial of Service Attack (DoS): Bu metot bir sunucunun çözümleyemeyeceği kadar çok işlem talepte bulunmak suretiyle yetkilinin servis dışı kalmasına neden olunmasıdır. Kaynak burada tüketilmektedir. Saldırgan sayısının çokluğu ve coğrafi yönden yaygın bir alanda faaliyet göstermesi halinde saldırıyı kontrol etmek son derece güçtür. Fakat DoS saldırısı sadece bundan ibaret değildir. Amaca ve metoda göre fiziki zarar, kusurdan faydalanma, kaynak tüketimi ve birebir, çoktan bire, çoktan çoğa saldırılar olarak gruplandırılmaktadır. Elektrik kaynağı ve ağ kabloları gibi mühimmatlarda hedef alınarak fiziki zarar verilmek suretiyle servise ulaşım engellenebilmekte ama bu saldırı kolayca onarılabilmektedir. Bir diğer yöntem ise ağ sisteminin çalışmasını önleyen bir hatadan, ateş duvarı veya yönlendiricideki bir kurulum hatasından faydalanarak erişilebilirlik engellenebilmektedir. Bunun onarımı da kolaydır ve yazılımın doğru biçimde kurulması problemi çözmektedir(Yi Gao 2005, 156).

Tüm bunlardan çıkan sonuç; Bilgi Güvenliği' nin bir teknoloji sorunu olmadığı, bunun bir iş yönetimi (sistem) sorunu olduğudur. Bu nedenle günümüzün rekabet ortamında küresel ekonominin içinde varolmak için bilgi varlıklarımızı koruma ve güvence altına alma, bunu bir yönetim sistemi yaklaşımı içinde kurumsal düzeyde yaygınlaştırma mecburiyeti kurumları Bilgi Güvenliği Yönetim Sistemi kurmaya ve kullanmaya zorlayacaktır

2.5.İşletme Güvenliği

Güvenlik politikası organizasyonlarda olması gereken güvenlik seviyesinin oluşmasına ve tanımlanmasına yardım eden ve tüm çalışanların, ortak çalışma içerisinde bulunulan diğer organizasyon çalışanları dahil, herkesi kapsayan uyulması gereken kurallar bütünüdür (Vural & Sağıroğlu, 2008, 40). Hazırlan politika hem genel bilgi güvenliği politikalarından hem de alt alanları ilgilendiren spesifik

politikalardan oluşur. Bu belirli alanların içinde erişim kontrol politikası, uzaktan erişim politikası, kullanıcı politikası, e-posta kullanım politikası gibi maddeler bulunur. Çalışanlara bunlarla ilgili talimat ve yönergeler verilir. İşletme güvenliği, güvenliğin işleyiş şekli ile ilgilidir. İşletme seviyesi politikaların nasıl uygulanacağı burada belirlenir. Buradaki ilk nokta yönetimin güvenliğe bakışı olacaktır. Burada iki kavram öne çıkmaktadır; itinalı güvenlik ve güvenlikte sebat. İtinalı güvenlik bütün alt başlıkların tek tek incelenerek gerekli olabilecek güvenlik önlemini almaktır, sebat ise politika ve olayların içinden geri dönerek güvenliği tekrar ele almaktır. Bazı organizasyonlar bu politikayı oluştururken her alandaki politikayı tek başlık altında incelerken genel olarak tavsiye edilen bir ana Bilgi Güvenliği Politikası oluşturup diğer alt alanların içeriğiyle bunun ilişkilendirilmesi tavsiye edilir.

2.6.İş Sürekliliği Planı

İş Sürekliliği Planları: Kurumsal işlerin olumsuz ve işi engelleyici faktörlere karşı sürdürülebilirliğinin sağlanması için yapılan planlamalardır. Bu planların, iş kesintilerine neden olan (acil) durumlarda kullanılabilmesi için, planın her bir bileşenini yönetecek ve uygulayacak ekiplerin de tanımlanmış olması gerekir. Bu planlar risk analizi sırasında veya hemen sonrasında yapılabilir. Belirlenen riskleri iyileştirecek olan Risk Tedavi Planlamasına geçmeden önce elimizde olması gerekir, çünkü bu aşamada iş sürekliliğini tehdit eden bulgular varsa, risklerin iyileştirilmesi aşamasında bu bilgilere gereksinimimiz olacaktır(Ersoy 2012, 56). "Böylelikle iş sürekliliği planı ile iş süreçleri muhtemel bir kesintiye uğrasa dahi işin kesintiye uğramayacağı garanti edilir. Fakat yine de iş süreklilik planı ne kadar iyi olursa olsun, kurumlar iş süreklilik planının öngörmediği ölçüde geniş çaplı iş kesintilerine uğrayabilirler. Bu çok beklenmedik bir olaydır ve" felaket kurtarma olayı" olarak adlandırılır. Bu plan organizasyonu yaşanan problem öncesine taşımaya çalışır ve bu doğrultuda süreçler hazırlanıp uygulanır. Burada en önemli nokta organizasyon için kritik olan bilgileri kurtarmaktır" (Birengel 2006, 32). Bu planlar hazırlandıktan ve uygulamaya başladıktan sonra etkili olabilmeleri için zaman zaman test edilmeli ve amaca yaklaşıp yaklaşılmadığına bakılmalıdır.

2.7.Mevzuat

Günümüzde bilişim teknolojileri eğitimden ticarete, ulaşımdan iletişime, kamudan özel sektöre kadar hayatımızın hemen hemen her alanında çok faydalı hale gelmiştir. Fakat bu durum bunu kötüye kullanan kişileri de beraberinde getirmiştir(Akbulut 2003, 547; Ersoy 1994, 152; Değirmenci 2003, 2750). "Bilişim teknolojileri kanunu ihlal edip bu alanla ilgili yeni suç fiilleri oluşturan bu kişiler için yaptırımlar hazırlanmıştır. Bilişim suçlarının da en az bilişim teknolojileri kadar hızlı artması özellikle bunu geliştiren ve sıkça kullanılan devletler tarafından çeşitli kanun ve yaptırımlar hazırlanmış ve mevzuatlar bu çerçevede hazırlanmıştır" (Akıncı vd. 2004, 158). Çok ciddi hazırlanması gereken mevzuat güvenlik kriterlerine, standartlara ve uluslararası mevzuata uygun olmalı, güvenliği sağlamanın yanında kişisel mahremiyete de özen göstermelidir. Ülkemizde, Yeni Türk Ceza Kanunu'nda ise, bu alandaki suçlar hem "Bilişim Alanında Suçlar" adı altında bir bölümde düzenlenmiş, hem de hırsızlık, dolandırıcılık gibi suçlar içerisinde yer almışlardır. Birçok dünya ülkelerinde de bu konuyla ilgili milli ve uluslararası mevzuat düzenlenmiştir(Yılmaz, 2011, 64).

İKİNCİ BÖLÜM
ITIL KÜTÜPHANESİ

ITIL (Information Technology Infrastructure Library = Bilgi Teknolojileri Altyapı Kütüphanesi)Birleşmiş Krallık Ticaret Ofisi tarafından 1980'li yılların sonlarına doğru geliştirilmiş olan standartlardır. Hazırlanma amacı, Birleşik Krallık hükümetinde BT hizmet yönetimini iyileştirmektir. ITIL, BT hizmetlerini en başarılı yöneten örnek uygulamaları esas alarak oluşturulan, süreçleri entegre olarak anlatan bir dizi yazılı rehberdir (ITGI 2006, 4). "Bilişim teknolojileri servisini iş tanımı doğrultusundaki ihtiyaçlara göre düzenler ve bilişim sistemlerini tanımlama, planlama ve desteleme rolü oynar. ITIL bilişim sistemleri oluşturmada kullanılan bir çok konsept ve çerçeve olarak da tanımlanabilir" (Marquis 2006, ss.49-52). ITIL uygulaması sırasında konseptler ve sistemler arasındaki farklı anlamak çok kritiktir (Latif vd. 2010, 112). ITIL tarafından tanımlanan süreçler, prosedürler, işler ve denetim listeleri organizasyon tarafından stratejilerini, değer teslim ve yetkinlik seviyeleri entegrasyonunu korumak amacıyla kullanılır. ITIL organizasyonlara planlanabilir, uygulanabilir ve ölçülebilir kriterler sağlamada önemli bir rol oynar. ITIL bilişim teknolojilerine birçok yönden hizmet eder. Bunlardan bazıları fiyatları düşürmek, müşteri memnuniyetini arttırmak ve verimliliği arttırmaktır. Bunlara ek olarak, metrikleri belirleme ve sonuçları ölçmede bilişim sistemlerine yardımda bulunur (Saleh ve Almsafir 2013, 480).

ITIL üç adet versiyona sahiptir. İlki 1980'lerin sonlarında yayınlanmış, ikincisi 2000 yılında yayınlanmış ve ITIL V3 yani üçüncü versiyon ise 2007' de sunulmuştur. ITIL 'ın üçüncü versiyonu günümüzde 5 ana yayından oluşmaktadır. Bu versiyonda ITIL, ISO/IEC 20000 standardıyla birlikte entegre bir yaklaşıma sahiptir ve hizmet stratejisi, hizmet tasarımı, hizmet operasyonu ve hizmet gerçekleştirimi gibi amaçlara hizmet eder (Sahibudin et al. 2008, 744). Bu yolla bilişim sistemleri servisine sistematik ve profesyonel bir yaklaşım sağlayarak organizasyonların uygun bilişim sistemlerine sahip olmasını ve devamlı olarak belirledikleri iş hedeflerine ulaşarak kar elde etmelerini sağlar.

1.BT Hizmet Süreçleri

ITIL, BT hizmet yönetimi süreçlerini iki bölümde ele almaktadır.

1.1.Hizmet Destek

Hizmet Destek, işlerini desteklemek için müşterilerin uygun BT hizmetlerine nasıl erişebileceklerini tanımlar. Hizmet Destek, müşteri ihtiyaçlarını karşılamak için kullanılan günlük operasyonel hizmet temelini birçok biçimde tanımlar. Hizmet Yönetiminin nasıl uygulanacağını, süreçleri tanımlayarak hizmet döngüsünü oluşturur, bilişim teknolojileri stratejilerine uyumlu tasarım ortaya çıkarılır ve hizmet çizelgesi hazırlanır (http://www.itil-officialsite.com/, Erişim: 26.06.2014). Hizmet destek yönetiminin görevi bilgi hizmetlerinin durağanlığından ve esnekliğinden emin olmaktır. 5 işlemden oluşmaktadır: konfigürasyon yönetimi, değişiklik yönetimi, problem yönetimi, sürüm yönetimi. (Pengwen vd. 2008, ss.450-470)
Hizmet Destek süreçleri şunlardır (www.itgi.org, Erişim: 18/08/2014):

1.1.1.Konfigürasyon Yönetimi

BT teknik altyapısını kontrol etmek, sadece onaylanmış yazılım ve donanımların kullanımını sağlamak. Konfigürasyon Yönetimi sistem konfigürasyon maddelerini tanımlamak ve raporlamaya yarar. Böylelikle maddelerin, altyapının doğruluğunu ve yeterliliğini test eder. Bunu yapmaktaki amaç bilgilerin altyapısına mantıksal bir model sağlamak ve diğer hizmet yönetim süreçlerini desteklemektir (Pengwen vd. 2008, ss.450- 470).

1.1.2.Değişiklik Yönetimi

Her türlü değişikliği etkin şekilde yönetmektir. Değişiklik yönetimi, alt dallardaki bütün hizmet yönetimindeki değişimlerini kontrol etme sürecidir. Bu amaçla değişikliklerle kolayca ve etkili bir biçimde standart metotlar ve prosedürler kullanarak başa çıkılır böylece hizmetin bundan etkilenme payı vardır(Pengwen vd. 2008, 450- 470).

1.1.3.Olay yönetimi

İşlevi belirlenen hizmet düzeylerinin sürekliliğini sağlamak, hizmet kesintilerini etkin ve hızlı bir şekilde gidermektir. Olay yönetimi kullanıcıların olağan operasyonlarında karşılaşacakları kesintilere önceden önlem alır ve problemleri etkili bir şekilde giderir. Bunu normal hizmet düzeyine dönene ve en iyi kalitede hizmet verene kadar yapar (Pengwen vd. 2008, 450- 470).

1.1.4.Problem Yönetimi

İşlevi Hizmet kesintilerini en aza indirmektir. Problem yönetimi bilgi hizmetleri süreçlerinde karşılaşabilecek bütün problemlerle başa çıkmak için vardır. Bunu yaparken önceden tanımlanmış öncelikleri göze alır ve ilişkili problemlerin tekrar meydana gelmesini önleyip problem çözme kapasitesini arttırır (Pengwen vd. 2008, 450- 470).

1.1.5.Sürüm Yönetimi

İşlevi; Değişim sürümlerini yönetmek, sürüm dağıtımını otomatikleştirmek ve onaylı yazılımların kullanımını sağlamak. İçerdiği yazılımların sürüm takibini yapar ve önceden test edilmiş konfigürasyonların doğrulamasını kapsar. Bunun yanında sürümlerin olumlu sonuç vermesi için detaylı bilgi oluşturulmasını sağlar ve finansal etkisini ölçmek adına veri yaratır (ABH Aylık e- bülteni, 2011, 5).

1.2.Hizmet Sunumu

Hizmet Sunumu, BT organizasyonlarının zaruri iş hizmetleri sunmalarına yardım eden beş süreci tanımlar. Doğasında dönüşümsel olan süreçler, kaliteli BT hizmetlerinin planlanması ve sunulmasıyla ilgilidir. Hizmet Sunum süreçleri şunlardır:

1.2.1.Hizmet (Seviyesi) Yönetimi

İşlevi; iş hedefleri ve müşteri istekleri doğrultusunda hizmet ve hizmet

düzeylerini belirlemek, takip ve kontrol etmektir. Hizmet seviyesi yönetimi, bilişim teknolojileri sağlayıcıları ve kullanıcılarını koordine ederek spesifik, sürekli ve ölçülebilir hizmetleri ortaya çıkarmaya yarar. Hizmet seviyesi protokolü bilişim sistemleri sağlayıcıları ve kullanıcıları için sorumluluk, hak ve yaptırımları belirler (Pengwen vd. 2008). Ayrıca hizmet seviyesi yönetimi hangi servisin hangi müşteri tarafından kullanılmakta olduğunun tanımlanmasını da sağlar (ABH Aylık e- bülteni, 2011, 5).

1.2.2.Kapasite Yönetimi

İşlevi; BT kaynaklarını verimli ve etkin kullanmaktır. Kapasite yönetimi, fiyat ve iş gerekliliklerinde gerekli hizmet yapılandırmasını yaparak bilişim teknolojileri altyapısının bugünkü ve gelecekteki iş gereksinimlerini karşıladığından emin olmak içindir belirler (Pengwen vd. 2008, ss.450-470). Bu amaçla kapasite modelleme için veri üretilmesini sağlar ve oluşturduğu plan çerçevesinde ilgili konfigürasyon ögelerinin tanımlanmasını sağlar. Kapasite ile ilgili olay veya problemlerin çözümlemesini sağlar ve risk analizi verisi ortaya çıkarır (ABH Aylık e- bülteni, 2011, 5).

1.2.3.Finansal Yönetim

BT hizmet maliyetlerini hesaplamak, kontrol etmek ve en alt seviyede tutmaktır. Finansal yönetim hangi servisler için hangi konfigürasyon ögeleri kullanıyor onu raporlar ve finansal kapasite kullanımı ile ilgili bilgi sağlar. Bunun yanında gerektiğinde bütçeleme ve finansal hesaplamalar için veriler üretir (ABH, 2011, 5). Bilişim teknolojilerini bütçe hesaplaması ve düzenlemesi yaparak destek olur (Pengwen vd, 2008, 450- 470).

1.2.4.Erişilebilirlik Yönetimi

İşlevi; BT hizmetlerinin kullanılabilirlik düzeylerini en üst seviyede tutmaktır. Erişilebilirliğin tüm konfigürasyon ögelerine ulaşmasını sağlar ve konuyla ilgili bileşenlerin de erişilebilirlik seviyesini gösterir. Ayrıca meydana gelen

hatalardan sorumlu olan konfigürasyon ögesinin erişilebilirlik hatasını kontrol eder (ABH, 2011, 5). Erişilebilirlik yönetimi artan erişilebilirlik ihtiyaçlarını rasyonel bedellerle karşılamaya yarar. Bunu yaparken işe uygun ihtiyaçları ve bilişim teknolojileri altyapı kapasitesini göz önünde bulundurur.

1.2.5.BT Hizmet Sürekliliği Yönetimi

İşlevi; bir felaket sonrasında hizmetlerin aksamamasını sağlamaktır. 10 süreçten oluşan bu yapıya tüm şirket ve BT organizasyonunu etkileyen Altyapı Yönetimi, Güvenlik Yönetimi süreçleri ile Yardım Masası fonksiyonu eklendiğinde ITIL tamamlanmış olur. ITIL süreçleri birbirleriyle entegredir ve aralarındaki ilişkiler nettir. Sık yaşanan bir senaryo üzerinde süreçler arasındaki ilişki rahatlıkla görülebilir. Örneğin; Bir şirket elemanı Yardım Masasını arasın ve bir hizmet konusunda yaşadığı sorunları aktarsın (www.itgi.org, Erişim:18/01/2014):

- Olay Yönetimi süreci devreye girer, olayı kayıt altına alır.
- Problem Yönetimi süreci sorunu inceler ve nedenini araştırır. Kapasite Yönetimi süreci bu çalışmaya destek verir. Hizmet Düzey Yönetimi sorunun daha önceden belirlenen sürede giderilip giderilmediğini takip eder. Gerektiği takdirde, Değişiklik Yönetimi süreci devreye girer ve bir değişim talep edilir.
- Değişiklik Yönetimi süreci değişim talebini takip ve koordine eder.
- Servis Sürekliliği süreci Değişiklik süreci ile birlikte güncel yedekleme konfigürasyonu ile geri almanın mümkün olup olmadığını kontrol eder.
- Finansal Yönetim süreci bir üst sürüm maliyetinin çıkarılmasına yardımcı olur.
- Sürüm Yönetimi süreci, değişim bünyesindeki donanım veya yazılım değişikliklerinin uygulanmasını kontrol eder.
- Sürüm Yönetimi, Konfigürasyon Yönetimini yeni sürümün detayları ile günceller.
- Kullanılabilirlik Yönetimi süreci sürüm değişikliğinin istenen kullanılabilirlik ve güvenirlilik düzeyini sağlayacağından emin olur.
- Konfigürasyon Yönetimi süreci bütün bu akış sırasında Konfigürasyon Yönetim Veritabanının (CMDB) güncellenmesini sağlar.

ITIL, temel süreçlerin planlanması, rol ve aktivitelerin ilişkilendirilmesi ve roller arasındaki bilgi akışının nasıl olacağı konularında denenmiş yöntemler sunar. Roller arasındaki bilgi akışı veya işbirliği eksikliğinden çıkabilecek sorunları en baştan tümüyle engeller veya en aza indirir.

2.ITIL Kitapları

2.1.ITIL Service Strategy (ITIL Hizmet Stratejisi)

Hizmet stratejisi modülü, BT Hizmet yönetiminin stratejik bir varlık olarak tasarlanmasını, geliştirilmesini ve uygulanmasını sağlar. Odak konusu Neden sorusuna cevap bulmaktır, Nasıl yapılacağı konusu bu aşamada öncelikli değildir. Bu modülün hedefi politikaların ve hedeflerinin tanımlanmasıdır (Wagner 2006, 4).

Hizmet stratejisi aşamasında iş ile ilgili stratejiler, planlar ve uzun vadeli hedefler belirlenir ve bilişim teknolojileri servisine şu anki ve muhtemel hedeflerde yol gösterilir. Hizmet stratejisi hizmet yönetiminin nasıl dizaynına karar verir, geliştirir ve uygulamasına dair rehberlik eder. Bunları yaparken organizasyonun bakış açısı, yeteneği ve stratejik varlıkları göz önünde bulundurulur (Wagner 2006, 4). Hizmet Stratejisi iç ve dış piyasaların geliştirilmesi, varlıkları, hizmet kataloğu konularını inceler ve bunu alt başlıklara ayırarak ele alır. Hizmet stratejisi genel olarak finansal yönetim, hizmet portföy yönetimi ve talep yönetimi konularını ele alır. Bu modülde organizasyonların "Hangi hizmetler kime ve nasıl sunulmalıdır?", "Müşterilerim için gerçek değeri nasıl oluştururum?", "Paydaşlarım için değeri nasıl yakalarım?", "Stratejik yatırımları gerçekleştirecek nasıl bir durum oluşturabilirim?", "Finansal Yönetim, değer yaratma üzerinde nasıl görünürlük ve kontrol sağlayabilir?", "Hizmet kalitesini nasıl tanımlamak gerekir?" gibi sorularının cevapları için rehber olabilir (Nabiollahi and Sahibuddin 2008, 2).

2.2.ITIL Service Design (ITIL Hizmet Tasarımı)

Hizmet Tasarım modülü, belirlenen servislerin ve Servis süreçlerinin tasarlanmasını ve geliştirilmesini sağlar. Mevcut hizmetlerin yaşam döngülerini ve hizmet seviyelerini müşteriler için daha değerli ve uygun hale getirmeyi amaçlar. Bu

modül hizmet ve hizmet varlıkları portföyünde hizmet yönetim süreçlerinin geliştirilme yöntemlerini ve dizaynlarını tanımlar. Bu tasarımlar, yeni bir şey ortaya koymak anlamına gelmez çünkü bu modül mevcut hizmetlerin işleyiş ve kalite seviyelerini arttırarak müşteri memnuniyetini arttırmayı amaçlar (Wagner 2006, 4) .Tüm bunlar yapılırken ilgili standartlar ve yasal zorunluluklara uygunluğu da gözden kaçırılmaz. (Nabiollahi and Sahibuddin 2008, 3) .Hizmet Tasarımı Servis Katalog Yönetimi, Hizmet Seviyesi Yönetimi, Kapasite Yönetimi, Stok Yönetimi, BT Hizmet Sürekliliği Yönetimi, Bilgi Güvenliği Yönetimi, Tedarikçi Yönetimi, Uygulama Yönetimi, Veri ve Bilgi Yönetimi gibi alanları içerir (Sahibudin et al. 2008, 750).

2.3.ITIL Service Transition (ITIL Hizmet Geçiş)

Bu modül, yeni/değişen servislerin uygulamaya alınış aşamasının verimli olmasını sağlar. Bu servislerin organizasyona uyumluluğu sağlanır ve kapasitesi arttırılmaya çalışılır. Değişen servislerin değiştirilen kısmında ileriki süreçleri yönetmede rehberlik eder (Wagner H.-T., 2006, 5). Kullanıcılar Hizmet Yönetimiyle ilgili pratik içeriğe ait Yayın Yönetimi, Program Yönetimi ve Risk Yönetimi gibi konuları pratik etmekte kullanırlar (Nabiollahi and Sahibuddin 2008, 3). Hizmet Geçiş süreçleri süreçleri, hizmet varlık ve yapılandırma yönetimi, yayın ve dağıtım yönetimi, bilgi yönetimi, paydaş yönetimi ve geçiş planlama gibi alt dallarda incelenir(Sahibudin et al. 2008, 750).

2.4.ITIL Service Operation (ITIL Hizmet İşletimi)

Servislerin, taahhüt edilen seviyede işletilmesi ve yönetilmesi için süreç ve aktivitelerin yerine getirilmesi ve koordine edilmesini sağlar. Hizmet aşamasında yürütülen operasyonların yönetimi ve organizasyonları hakkında bilgi verir, rehberlik eder. Organizasyon ile müşteri veya servis sağlayıcı için teslimat ve destek aşamalarında etkin rol oynar ve burada hizmet kalitesini yükseltmek ve efektifliği artırmaya yönelik çalışmalara rehberlik eder (Nabiollahi and Sahibuddin, 2008, 3). Hizmet aşamasında yürütülen bu çalışmalar Olay Yönetimi, Vaka Yönetimi, Talep Yönetimi, Problem Yönetimi, Erişim yönetimi konuları altında gerçekleştirilir.

2.5.ITIL Continual Service Improvement (ITIL Sürekli İyileştirme)

Sürekli Servis İyileştirme modülü, servis kalitesinin ve ilgili süreçlerin kalitesinin değerlendirilmesi ve iyileştirmesine yönelik öneriler sunar. Bu modül aslında gelişimin devamlılığını sağlar ve müşteri memnuniyetini arttırmaya yönelik hizmetlerin tasarımı, içeriği ve yürütülmesi konularının daha iyi hale nasıl getirilebileceği hakkında rehberlik eder. Kalite yönetimi, Değişiklik Yönetimi ve Kapasite artırımı konularında metot sağlayıp bunlarla ilgili pratik geliştirip ortaya bir prensip çıkarmada yardımcı olur (Nabiollahi and Sahibuddin, 2008, 3) Bu modül iş gereklilikleri, teknolojik gerekliliklerle ilgili zayıflıkları ortadan kaldırmada önemli bir rol oynar. Böylelikle müşteri memnuniyetini arttırmayı hedefler (Haleh vd. 2010, 158).

Şekil 3. ITIL Hizmet Yaşam Döngüsü

Kaynak: ITGI (Information Technologies Governance Institude - Bilgi Teknolojileri Yönetim Enstitüsü), Price Waterhouse Coopers-ITGI. 2006, www.itgi.org, Erişim: 18/01/2014

Tablo 1. ITIL Versiyon 3 Prosesleri

Temel Süreçler		Servis Strateji	Servis Tasarım	Servis Geçiş	Servis İşletim	Sürekli Servis İyileştirme
Servis Strateji	SS					
Finansal Yönetim	SS					
Servis Portfolyo Yönetimi	SS					
Talep Yönetimi	SS					
Servis Seviyesi Yönetimi	ST					
Servis Katalog Yönetimi	ST					
Erişilebilirlik Yönetimi	ST					
Kapasite Yönetimi	ST					
Bilgi Güvenliği Yönetimi	ST					
Servis Süreklilik Yönetimi	ST					
Tedarikçi Yönetimi	ST					
Değişiklik Yönetimi	SG					
Servis Varlık ve Konfigürasyon Yönetimi	SG					
Sürüm ve Yaygınlaştırma	SG					
Durum Yönetimi	SI					
Olay Yönetimi	SI					
Taleplerin Yerine Getirilmesi	SI					
Problem Yönetimi	SI					
Erişim Yönetimi	SI					
7 Aşamalı Servis İyileştirme Planı	SIY					

Kaynak : ITGI (Information Technologies Governance Institude - Bilgi Teknolojileri Yönetim Enstitüsü), Price Waterhouse Coopers-ITGI. 2006, 250

ÜÇÜNCÜ BÖLÜM
COBIT STANDARTI VE MİMARİSİ

1.COBIT (Bilgi Ve İlgili Teknolojiler İçin Kontrol Hedefleri)

COBIT, Türkçe karşılığı Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri olan "Control OBjectives for Information and related Technology" kelimelerinden üretilmiş bir kısaltmadır. ISACA ve ITGI tarafından 1992 yılında geliştirilmiş, BT Yönetimi için en iyi uygulamalar kümesidir (Guldentops and Haes 2002, ss.25-31). CobiT; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA, GAO tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir (www.itgi.org, Erişim: 18/01/2014). Bir organizasyon içinde yöneticilere, denetçilere ve bilişim teknolojileri kullanıcılarına verimliliği arttırmak için kabul görmüş ölçü, gösterge, süreç ve en iyi uygulamaları sağlar.

COBIT 'in kullanım amacı bilişimsel ve ilgili teknolojilerle alakalı bilgileri kontrol edip yönetmektir (IT Governance Institute, "COBIT Executive Summary", 3rd Edition, Released by COBIT Steering Committee, pp. 3, July 2000.). COBIT bilişim sistemleri teknolojisinin iş alanlarının ihtiyaçları ve amaçları doğrultusunda nasıl bilgi sağladığını kapsar. "COBIT' in vizyonu, bilişim teknolojileri yönetişim (IT governance) modeli olmaktır. CobiT bir denetim aracı olarak kalmayıp yönetişim alanında da hizmet sağlamaktadır. Böylelikle birçok alanda buna bilişim teknolojileri personeli dahil kurum için risk üstlenen taraflara da yarar sağlamayı hedeflemektedir (Uzunay 2007, 185).

COBIT; Bilgi Teknolojilerinin kullanıldığı süreçlerin kontrol ve ölçümlemelerinin nasıl yapılması gerektiğini anlatan metodolojidir. COBIT, 4 grup altında ve 34 adet ana kontrol hedefi içermektedir. Bu guruplar aşağıdaki gibidir (Fasanghari et al. 2008, 516):

- Planla ve Organize Et

- Tedarik ve Uygulama

- Teslimat ve Destek

- Gizle ve Değerlendir

COBIT, aslında süreç değil, kontrol odaklıdır. COBIT çalıştığı organizasyonların işleri ne şekilde yürüttükleriyle değil, neler yapmaları gerektiğiyle ilgili tavsiyelerde bulunur. Ayrıca kullanım popülasyonu açısından sadece kullanıcı ve denetçileri değil iş sürecine dahil olan herkese hitap eder. COBIT çerçevesi, bilgi sistemleri teknolojisine sağladığı kaynaklar açısından önemli bir rehber olmaktadır ve bu alanla ilgili ihtiyaç duyulan bilgiyi sağlayan gruplanmış süreçler olarak da bilinir (Fasanghari et al. 2008, 516).

1.2.COBIT Versiyonları ve Tarihçesi

COBIT dört ana yayımdan oluşmuştur:

- 1996, COBIT birinci baskı yayımlandı.
- 1998, İkinci baskıda yönetim yönergelerine eklendi.
- 2000, Üçüncü baskı yayımlandı.
- 2003, COBIT online sürümü kullanıma sunuldu.
- 2005 Aralık, Dördüncü baskı yayımlandı.
- 2007 Mayıs, Güncel versiyonu 4.1 yayımlandı.

CobiT ’in ilk sürümü 1996 yılında yayımlandı. Amacı; iş yöneticileri ve denetçilerinin günlük kullanımı için geçerli, güncel, uluslararası kabul görmüş BT amaçlarını araştırmak, geliştirmek ve teşvik etmektir. “Yönetim Rehberi”, 1998’de

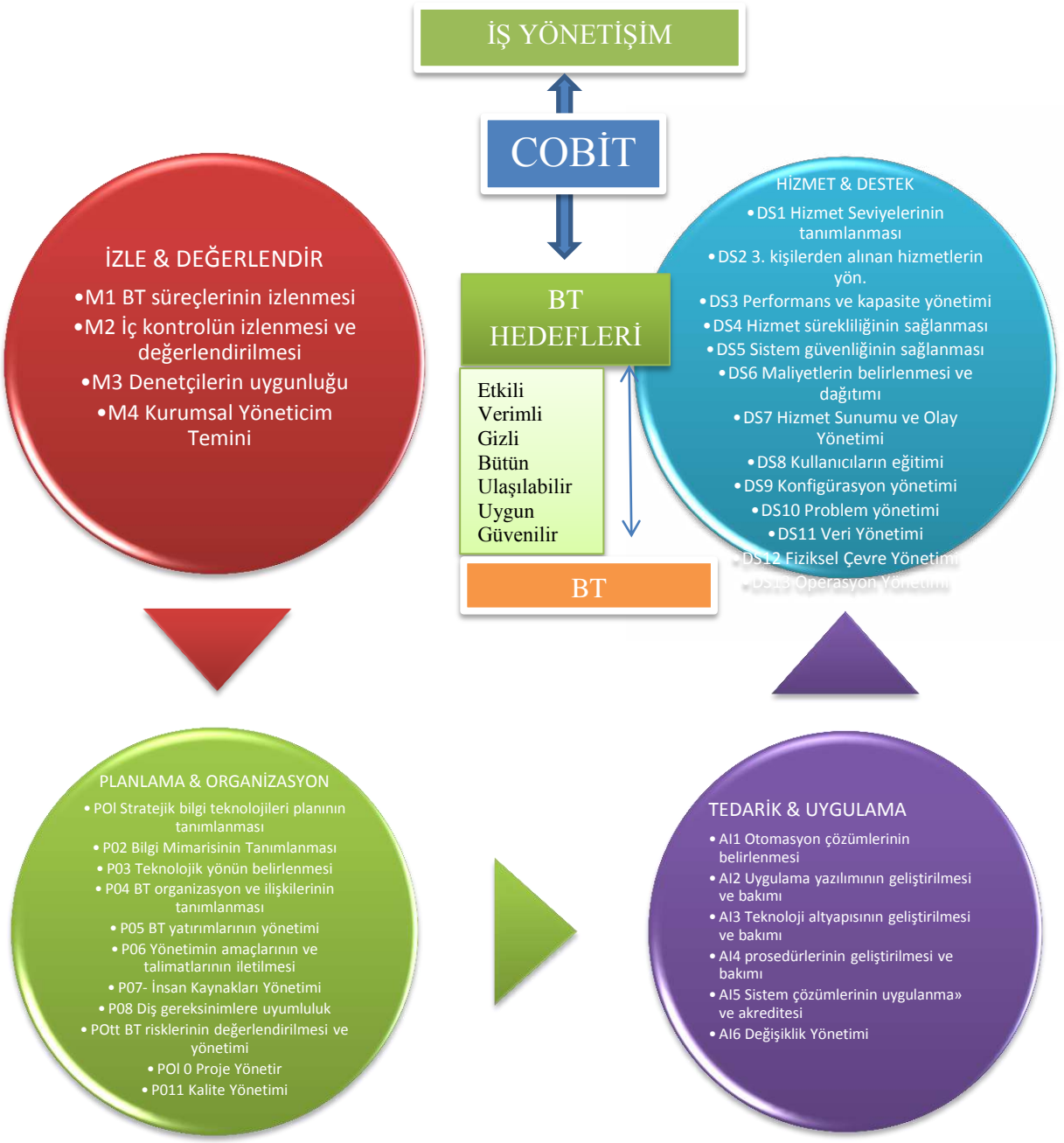
yayınlanan 2. sürüme eklendi. 2000 yılında 3. sürüm yayınlandı. 2003 yılında bilgisayar bağlantılı versiyonu kullanılır duruma geldi. 2005 yılının aralık ayında 4. basım ilk olarak yayınlandı. 2007 yılının mayıs ayında, şu anda kullanılan 4.1 sürümü yayınlandı. Yayında olan bu versiyona ISACA' nın web sitesinden erişilebilmektedir.

CobiT' in jenerik bir model olarak herhangi bir kurumda yer alabilecek tüm teknoloji süreçlerini kapsayan yapısı içerisinde, gruplanmış 4 süreç alanı ve 34 tane temel BT süreci yer almaktadır (www.itgi.org, Erişim: 18/01/2014).

Her COBIT süreci ilk olarak süreç tanımı yapılarak başlanır ve bu süreç tanımında yapılacak çalışmanın genel hatlarından bahsedilir. COBIT çerçevesi bilgi için gerekli olan işletme ihtiyaçları, bilgi teknolojisi kaynakları ve bilgi teknolojisi süreçleri olmak üzere 3 unsurdan oluşur. COBIT çerçeve hazırlarken bir takım bilgi kriteleri kullanır. Bunlar etkililik, verimlilik, gizlilik, bütünlük, kullanırlık, uyum ve güvenirlik başlıkları altındadır. Organizasyonun iş hedeflerine ulaşması için bilginin COBIT tarafından kullanılan kriterlere uygun olması gerekir. (Güneş vd. 2002, 12).

Bilgi teknolojisi süreçleri COBIT yaklaşımı içinde 4 alandan oluşur: süreçleri planlama ve organizasyon, kazanım ve uygulama, teslim ve destekleme, izleme. CobiT' de yer alan "Yönetim Rehberi-Management Guidelines" içerisinde tüm teknoloji süreçleri için Olgunluk Modeli (Maturity Model), Kritik Başarı Faktörleri (Critical Success Factors), Ana Hedef Göstergeleri (Key Goal Indicators) ve Ana Performans Göstergelerinin (Key Performance Indicators) tanımlanmış olması sayesinde, 34 süreç dahilinde, organizasyonun hedeflere ulaşma derecesi ölçümlenebilmektedir.

Hedefler, kaynaklar ve süreç grupları ve süreçler bir araya getirildiğinde oluşturulan CobiT Mimarisi ana hatları ile aşağıda yer almaktadır:



Şekil 4. COBIT İş Hedefleri

Kaynak: Artinyan, E.N., **COBIT Çerçevesi**, Deloitte Kurumsal Risk Hizmetleri, 2008, 132

1.3.COBIT Versiyon 4

COBIT Versiyon 4, COBIT 3 'teki ayrı kitapların tek bir ses halinde ve kullanım kolaylığına sahip olarak geliştirilmiş halidir. COBIT 4.0 ne yapılması

gerektiğinden çok nasıl yapılacağı konusu üzerine odaklanmıştır. Fakat kontrol yapılarını idare edilebilir ve mantıklı yapılara düzenlemekte üstündür. Böylelikle kontrol için yapılması gerekilen aktiviteler ortaya çıkar (Singh-Latulipe R., IT Governance Institute 2006, 20). COBIT 4.0 anlatımı açık ve sade organizasyona sahiptir. Çalışılan her alanın 4 alt kategorisi daha yalın açıklamalar ve bilgi sistemleri yönetim süreçleri ile ilgili birçok ek ile ilgili birçok ek ile birlikte sunulmuştur. Esas olarak bu versiyon diğer versiyonların ele aldığı konuları aynı içerik ile daha yalın hale getirilmiştir. Bu yolla yayım sayısı azaltılmış ve bilgilerin daha kolay hatırlanabilmesini sağlamıştır.

COBIT Versiyon 4.1

COBIT sürümü 4.1 diğer sürümler gibi ISACA web sitesinde mevcuttur. Bu versiyonda bilişim teknolojilerinin yürüttüğü hedef açıklamaları daha basit hale getirilmiş ve yürütülen süreçler ile "İşletme", "BT hedefleri" ve "BT süreçleri" arasındaki karşılıklı ilişki başaklandırılmıştır.

Bu versiyon aşağıdaki 4 yayından oluşmaktadır;

- Yönetimsel Özet,
- Çatı
- Esas İçerik (Kontrol Hedefleri, Yönetim Kılavuzu ve Olgunluk Modelleri)
- Ekler
- Yönetimsel Özet

Bu özet ana hatlarıyla COBIT' in çalıştığı konuları anahtar bilgileriyle ele almış ve kıdemli yöneticilere COBIT' in temel kavram ve kurallarını daha kısa zamanda anlaşılır hale getirmiştir. Böylelikle zaman sıkışıklığı olan organizasyon yöneticileri için COBIT' i daha kullanışlı hale getirmiştir (www.itgi.org, Erişim: 18/01/2014).

Organizasyonun bilişim sistemleri süreçlerini sağlam bir çatı üzerine kurması iş hedeflerine yaklaşma yolunda ilk temel adımdır. Bu çatı, kullanıcılara esas

bileşenler, süreçler, kontroller, hedefler ve metrikler arasındaki ilişkiyi betimler. Bilgi sistemleri kaynaklarının işe tam anlamıyla destek vermesi için yedi bilgi kriterini (etkinlik, verimlilik, gizlilik, bütünlük, uygunluk, uyum ve güvenilirlik) de açıklar. Organizasyonun gereksinimlerini tespit eder ve ana bilgi teknolojisi kaynaklarını belirler. Tüm bunları bilgi teknolojisi faaliyetlerini yaygın ve kabul almış bir süreçmişçesine ele alır. COBIT çatısı bilgi teknolojilerinin organizasyonun hedeflerine daha yakın olabilmesi için gerekli olan ölçüm, indikatör ve süreçleri sağlar (www.itgi.org, Erişim:18/01/2014)

Esas İçerik

Organizasyonun iş hedefleri doğrultusunda ilerlemesi açısından iş süreçleri ve bilgi sistemleri arasındaki birliği iyi yönetebilmesi gerekir. Kontrol aşamaları ve beklenen kontrol seviyelerini normlarla karşılaştırmak için Olgunluk Maddeleri kullanılır. Kritik Başarı Faktörleri, BT işlemleri kontrolü için en önemli faaliyetleri içerir. Anahtar Hedef Göstergeleri, performans hedef seviyelerini tanımlamak içindir. Anahtar Performans Göstergeleri de BT kontrol sürecinin amaca ulaşmasına uygun olup olmadığını ölçmek içindir. Bu yönetim yönergeleri kurumsallaşmış organizasyonların sorunlarına çözüm sunmaktadır(www.itgi.org, Erişim: 18/01/2014).

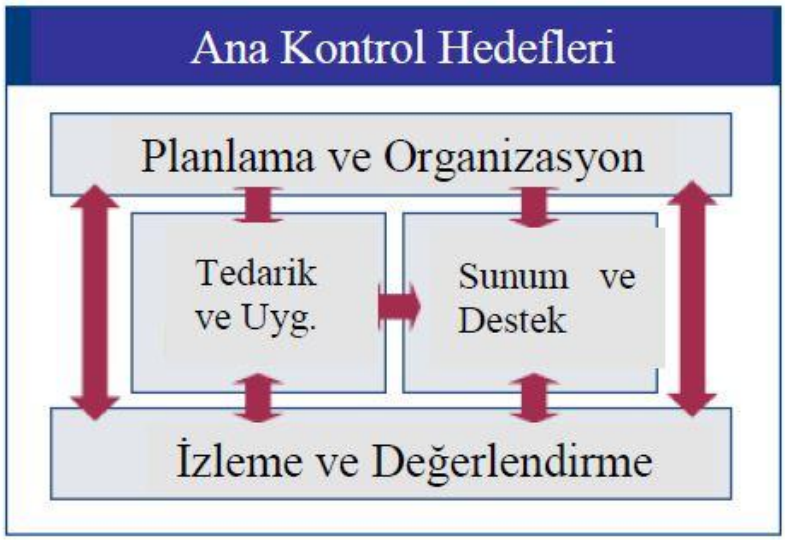
Ekler

Eşleştirmeler ve çapraz başvurular, ilave olgunluk modeli bilgileri, referans materyalleri, proje tanımı ve sözlük yer alır.

2.COBIT'in Ana Kontrol Hedefleri

COBIT ana kontrol hedefleri Şekil 5'de de gösterildiği gibi dört etki alanını kapsar:

- Planlama ve Organizasyon
- Tedarik ve Uygulama
- Hizmet Sunumu ve Destek
- İzleme ve Değerlendirme



Şekil 5. COBIT Ana Kontrol Hedefleri

Kaynak: Artinyan, E.N., **COBIT Çerçevesi,** Deloitte Kurumsal Risk Hizmetleri, 2008, 169.

2.1.Planlama ve Organizasyon

Planlama ve organizasyon bölümü işletme tarafından belirlenen amaçları gerçekleştirme yolunda bilgi teknolojilerine rehberlik eder. Burada bu amaç doğrultusunda yapılacak işlerle ilgili stratejiler ve taktikler yer alır. Hedefleri gerçekleştirirken ortaya sunulan bu stratejik planların gerçekçi olması açısından işletmenin teknolojik altyapısının uygun olup olmadığı incelenir.

.

Planlama ve Organizasyon alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır: (Şahinaslan, vd., 2009, 325)

- PO1 Stratejik bir BT Planı Tanımlama
- PO2 Bilgi Mimarisini Tanımlama
- PO3 Teknolojik Yönü Belirleme
- PO4 BT Prosesleri, Organizasyon ve İlişkilerini Tanımlama
- PO5 BT Yatırımını Yönetme

- PO6 Yönetim Hedefleri ve Yönünü Bildirme
- PO7 BT İnsan Kaynaklarını Yönetme
- PO8 Kaliteyi Yönetme
- PO9 BT Risklerini Değerlendirerek Yönetme
- PO10 Projeleri Yönetme

PO1 Stratejik bir BT Planı Tanımlama

- PO1.1 IT Değer Yönetimi
- PO1.2 İş ve BT Arasındaki Uyumun Sağlanması
- PO1.3 Mevcut Performansın Değerlendirilmesi
- PO1.4 BT Stratejik Planı
- PO1.5 BT Taktik Planları
- PO1.6 BT Portföy Yönetimi

PO1.1 IT Değer Yönetimi

BT süreçler gerçekleştirilirken ortaya çıkabilecek plan dışı 'tüm sapmaları önceden uyarısını sağlamalıdır. BT hizmetleri, kullanıcı ve sağlayıcı açısından adil ve uygulanabilir hizmet seviyesi sözleşmeleri ile koruma altına alınmalıdır. Böylelikle karşılıklı menfaat elde etme ve çeşitli mali kontrollerin sorumluluğu netleştirilir ve takip edilebilir. İş durumlarının, mali değer, kapasiteye ulaşamama riski ve beklenen menfaatleri elde edememe riski dahil, adil, şeffaf, tekrarlanabilir ve kıyaslanabilir bir şekilde değerlendirilmesi sağlanmalıdır. (Osborne 2006, 113)

PO1.2 İş Birimleri ve BT Uyumu

BT' nin kullanım alanının anlaşılabilir olması için organizasyon yöneticilerinin günümüzdeki teknoloji imkanları ve muhtemel gelişmelerde BT 'nin organizasyona sağlayabileceği imkanlarla ilgili eğitilmiş olmalıdır. BT' nin uygulanacağı iş yönünün ayrıntılı bir şekilde ele alınması gereklidir. Bunu yaparken BT' nin sunduğu stratejilerden organizasyonun iş hedeflerinin nasıl yararlanabileceği ve bunun kapsamı net bir şekilde açıklanmalı ve duyurulmalıdır. İş hedeflerine

ulaşma yolunda belirlenen kritik noktalar belirlenmeli ve BT öncelikler tespit etmelidir. Böylelikle iş ile teknolojinin şartları arasında ara yol çizilmelidir (www.itgi.org, Erişim:18/08/2014).

PO1.3 Mevcut Yetenek ve Performans Değerlendirmesi

Mevcut plan ve bilgi sistemlerinin performansını, iş hedeflerine katkı, işlevsellik, istikrar, karmaşıklık, maliyetler, güçlü ve zayıf noktalar açısından değerlendirilmelidir.

PO1.4 BT Stratejik Planı

BT stratejik planı ilgili ortaklarla birlikte BT' nin organizasyonun iş hedeflerine ve stratejik amaçlarına maliyet ile ilgili ne şekilde yarar sağlayacağını kapsar. Planın içinde hedeflere ulaşma yolu ve bunların nasıl ölçüleceği belirlenip resmi onaydan geçer. BT stratejik planı yatırım/işlemler bütçesi, finansman kaynakları, kaynak stratejisi, tedarik stratejisi ile yasa ve yönetmenliklerin şartlarını kapsamalıdır. Stratejik plan, BT taktik planlarının belirlenmesine izin verecek şekilde yeterince ayrıntılı olmalıdır. (Osborne 2006, 114).

PO1.5 BT Taktik Planları

"Taktik planları, proje planlarının belirlenmesine izin verecek şekilde yeterince ayrıntılı olmalıdır Belirlenen taktik BT planları ve inisiyatiflerini proje ve hizmet portföylerinin analizi yoluyla aktif bir şekilde yönetilmelidir. Bu, düzenli olarak ihtiyaç ve kaynakların dengelenmesi, bunların stratejik ve taktik hedeflere ve beklenen menfaatlere ulaşılmasıyla kıyaslanması ve sapmalar halinde gerekenin yapılmasını kapsamalıdır." (Şahinaslan, vd., 2009, 329)

Etkili bir BT taktik planı geliştirmek için öncelikle organizasyonun stratejik planları gözden geçirilmelidir. Stratejik planlar ve taktik planları listelendikten sonra bu planların içinde teknolojinin yararı olabilecek noktalar ortaya çıkar. BT planlarına ulaşabilmiş bir çok organizasyon reaktif yapıdan ziyade proaktif yapıya sahiptir ve taktik planları o alanla ilgili yatırım yapılıp yapılmaması yönünde turnusol kağıdı

gibi işlev görür. Bütçe sürecinde proje gözden geçirilirken organizasyonun stratejik hedeflerini gerçekleştirmede bu projenin katkısı olur mu ona bakılmalıdır (Herr 2006, 410)

PO1.6 BT Portföy Yönetimi

Bireyler ve kurumların değişik yatırımlarını bir portföy olarak değerlendirip yönetmesi gibi organizasyonlar da benzer nedenle çeşitli projelerini portföy olarak yürütmelidir. Böylece riski aza indirerek yatırımdan olabilecek en yüksek getiri sağlamak hedeflenir. BT portföy yönetimi bir dizi projenin birlikte ele alınarak önceliklere karar verilmesi, yürütülmesi ve katkılarının izlenmesi kapsamında gerçekleşir. Proje portföyü kurumun tüm projelerini kapsayabileceği gibi, kurum içindeki değişik departmanların kendi proje portföyleri de olabilir. Özellikle projelerin toplam karlılığa katkısı ayrı ayrı ölçülecekse her yönetimin kendi portföyünü oluşturması İstenilen iş sonuçlarının netleştirilmesi, program hedeflerinin sonuçlara ulaşılmasını desteklemesinin sağlanması, sonuçlara ulaşmak için gerekli çabaların tam kapsamının anlaşılması, destekleyici önlemlerin net bir sorumluluğunun tahsis edilmesi, program içindeki projelerin tanımlanması, kaynak ve finansmanın bulunması, yetkilerin verilmesi ve ilgili projelerin program başlangıcında uygulamaya konulması bu kapsama dahil olmalıdır (Osborne 2006, 129).

PO2 Bilgi Mimarisini Tanımlama

- PO2.1 İşletme Bilgisi Mimarisi Modeli
- PO2.2 İşletme Veri Sözlüğü ve Veri Sentaks Kuralları
- PO2.3 Veri Sınıflandırma Şeması
- PO2.4 Bütünlük Yönetimi

PO2.1 İşletme Bilgisi Mimarisi Modeli

Stratejik BT Planı oluşturmadaki amaç gibi, BT hedefleriyle uyumlu uygulama geliştirmek ve karar mekanizmasını destekleyen faaliyetler oluşturmak

için organizasyon bilişim modeli oluşturmalıdır. Bu model işletme tarafından bilginin optimum olarak oluşturulması ve paylaşılmasını sağlar. Modelin ana yapısı bütünlüğü sağlayıcı olmalıdır. Bir çok alandaki çalışmaların ortak noktası üzerinden hareket etmelidir ve bunları entegre etmelidir. Aynı zamanda çeşitli beklenmedik durumlara karşı esnek ve her hedef için bir işlevsel olmalıdır. Organizasyon açısından bu modelin uygun maliyetli olması da önemli bir nitelik taşır. Ortaya çıkan mimarinin amaçlar doğrultusunda güvenilir ve başarısızlığa karşı dayanıklı olması da gerekir (Önel vd. 2007, 138).

PO2.2 İşletme Veri Sözlüğü ve Veri Sentaks Kuralları

Müessesenin veri sentaks kuralarını içeren işletme veri sözlüğü tutulmalıdır. Bu sözlük, veri unsurlarının uygulama ve sistemler arasında paylaşılmasını sağlamalıdır, BT ve iş kullanıcıları arasında verilerin ortak olarak anlaşılmasını kolaylaştırmalıdır ve uyumsuz veri unsurlarının oluşturulmasını önlemelidir.

PO2.3 Veri Sınıflandırma Şeması

"İşletme verilerinin kritiklik ve hassasiyet derecesine (örn. kamuya açık, gizli, çok gizli) dayalı, işletmenin tamamında geçerli olarak bir sınıflandırma şeması oluşturulmalıdır. Bu şema, verinin mülkiyeti hakkındaki bilgiler, ilgili güvenlik dereceleri ve koruma kontrollerinin tanımı ve verinin tutulması ve imha edilmesi şartları, kritikliği ve hassasiyetinin kısa tanımını içermelidir. Şema, erişim kontrolleri, arşivleme yada şifreleme gibi kontrollerin uygulanması için temel teşkil etmelidir." (Uzunay 2007, 245).

PO2.4 Bütünlük Yönetimi

Veri tabanları, veri depoları ve veri arşivleri gibi, elektronik biçimde muhafaza edilen tüm verilerin bütünlük ve tutarlılığını sağlamak için gerekli prosedürler tanımlanmalıdır ve uygulanmalıdır.

PO3 Teknolojik Yönü Belirleme

- PO3.1 Teknolojik Yönün Planlanması

- PO3.2 Teknolojik Altyapı Planı
- PO3.3 Gelecekteki Eğilimler ve Yönetmenliklerin Takibi
- PO3.4 Teknoloji Standartları
- PO3.5 BT Mimarisi Kurulu

Kaynak: Osborne, 2006, 114

PO3.1 Teknolojik Yönün Planlanması

Mevcut ve yeni ortaya çıkan teknolojileri analiz ederek BT stratejisi ile iş sistemleri mimarisini gerçekleştirmek için hangi teknolojik yönün uygun olduğu planlanmalıdır. Ayrıca plan içinde hangi teknolojilerin iş fırsatlarını yaratma potansiyeli olduğu belirtilmelidir. Plan sistemlerin mimarisi, teknolojik yön, göç stratejileri ve altyapı bileşenlerinin ihtimal dahilindeki unsurlarını içermelidir.

PO3.2 Teknolojik Altyapı Planı

BT stratejik ve taktik planlarıyla uyumlu olan bir teknolojik altyapı planı oluşturarak tatbik edilmelidir. Plan teknolojik yöne dayalı olup risk düzenlemeleri ve teknoloji kaynaklarının dağıtımı için talimatı içermelidir. Planda rekabet ortamındaki değişiklikler, bilişim sistemlerine personel alınması ve yatırım yapılması boyutunu taşıyan ekonomiler ve platformlar ile uygulamaların arasında geliştirilmiş ara-çalışabilirlik ele alınmalıdır (Yıldız 2007, 39).

PO3.3 Gelecekteki Eğilimler ve Yönetmenliklerin Takibi

İş sektörü, teknoloji, altyapı, mevzuat ve düzenleme çevre eğilimlerini takip etmek amacıyla bir süreç oluşturulmalıdır. Bu eğilimlerin sonuçlarını, BT teknoloji altyapı planının geliştirilmesine dahil edilmelidir.

PO3.4 Teknoloji Standartları

İşletme çapında tutarlı, etkili ve güvenli teknoloji çözümlerini sunmak için teknoloji ilkeleri, altyapı ürünlerin üzerine danışmanlık ve teknoloji seçimi konusunda rehberlik sağlamak için bir teknoloji forumunu kurunuz ve bu standart ile

ilkelere uyumu ölçülmelidir. Bu forum, iş ilgisi, risk ve dış şartlara uyumları bazında teknoloji standartlarını yönetmelidir (Önel ve Dinçkan, 2007, 338).

PO3.5 BT Mimarisi Kurulu

Mimari ilkelerini sağlamak, bunların uygulaması konusunda danışmanlık vermek ve uyumluluğu kontrol etmek üzere bir BT Mimarisi Kurulu oluşturulmalıdır. Bu organ BT mimarisi tasarımını yöneterek bu tasarımın iş stratejisini etkinleşmesini sağlamalıdır ve yönetmenliklere uyum ile süreklilik şartlarını değerlendirmelidir. Bu, bilişim mimarisine ilişkilendirilmelidir / bilişim mimarisi ile ilgili olmalıdır.

PO4 BT Prosesleri, Organizasyon ve İlişkilerini Tanımlama

- PO4.1 BT Proses Çerçevesi
- PO4.2 BT Stratejisi Komitesi
- PO4.3 BT Yönetim Komitesi
- PO4.4 BT İşlevinin Organizasyon içinde Yerleştirilmesi
- PO4.5 BT Organizasyon Yapısı
- PO4.6 Rol ve Sorumluluklar
- PO4.7 BT Kalite Güvencesi Sorumluluğu
- PO4.8 Risk, Güvenlik ve Uyum Sorumluluğu
- PO4.9 Veri ve Sistem Mülkiyeti
- PO4.10 Denetleme
- PO4.11 Sorumlulukların Ayrıştırılması
- PO4.12 BT Personel Alımı
- PO4.13 Ana BT Personeli
- PO4.14 Sözleşmeli Personel Politika ve Prosedürleri

PO4.1 BT Süreç Çerçevesi

BT stratejik planını tatbik etmek için BT süreç çerçevesi tanımlanmalıdır. Bu çerçeve bir BT süreç yapısı ve ilişkilerini (örn. süreç boşlukları ve bindirmelerini

yönetmek için), mülkiyet, vade, performans ölçümü, iyileştirme, uyum, kalite hedefleri ve bunlara ulaşmanın planlarını içermelidir. Çerçeve, BT' ye özgü olan süreçler, işletme portföy yönetimi, iş süreçleri ve iş değişim süreçleri arasındaki entegrasyonu sağlamalıdır. BT süreç çerçevesi kalite yönetim sistemi ile iç kontrol çerçevesine entegre edilmelidir (Önel ve Dinçkan 2007, 327).

PO4.2 BT Stratejisi Komitesi

Kurul düzeyinde bir BT stratejisi komitesi kurulmalıdır. Bu komite, kurumsal yönetimin bir parçası olarak BT yönetiminin gerektiği şekilde ele alınması, stratejik yön konusunda danışmanlık sunması ve ana yatırımları gözden geçirmesini sağlamalıdır (www.itgi.org, Erişim:18/01/2014).

PO4.3 BT Yürütme Komitesi

Yönetici ile iş ve BT yönetiminden oluşan bir BT yürütme komitesi proje statülerini ve kaynak uyumsuzluklarını çözme amaçlarıyla oluşturulmalıdır.

PO4.4 BT İşlevinin Organizasyon içinde Yerleştirilmesi

Başta BT' nin iş stratejisi için kritiklik derecesi ve BT' ye işlevsel bağımlılık derecesi olmak üzere BT' nin işletme içerisindeki önemine bağlı olarak BT işlevini bir iş modeli genel organizasyon yapısı içerisinde konumlandırılmalıdır. CIO 'nun raporlama satırı, BT' nin işletme içindeki önemiyle bağlantılı olmalıdır.

PO4.5 BT Organizasyon Yapısı

İş ihtiyaçlarını yansıtan bir iç ve dış BT organizasyon yapısı kurulmalıdır. Buna ilave olarak personel alım ihtiyaçları ve kaynak stratejilerini, beklenen iş hedeflerine ve değişen şartlara uyacak şekilde değiştirmek amacıyla BT organizasyon yapısını periyodik olarak gözden geçirmek için bir süreç uygulanmalıdır.

PO4.6 Rol ve Sorumluluklar

Bilişim sistemlerine ilişkin olarak müessesedeki tüm personel için, personele verilen rol ve sorumlulukları yerine getirmeleri için yeterli yetkinin verilmesi amacıyla, rol ve sorumluluklar tanımlanmalıdır. Rol tanımları oluşturularak bunlar düzenli olarak güncellenmelidir. Bu tanımlar hem yetki hem de sorumluluğu sınırlar, ilgili pozisyonda gerekli yetenek ve tecrübenin tarifini içerir ve performansın değerlendirilmesinde kullanıma uygun olmalıdır. Rol tanımları iç kontrol sorumluluğunu içermelidir (Önel ve Dinçkan 2007, 339).

PO4.7 BT Kalite Güvencesi Sorumluluğu

Kalite güvence işlevinin yerine getirilmesinden kaynaklanan sorumluluğu yükleyerek kalite güvence grubuna uygun kalite güvence sistemleri, kontrol ve iletişim yetenek ve deneyim sağlanmalıdır. Organizasyon içinde konumlandırma, sorumluluklar ve kalite güvence grubunun büyüklüğü müessesenin ihtiyaçlarına uygun olmalıdır (Hansche 2003, 19).

PO4.8 Risk, Güvenlik ve Uyum Sorumluluğu

İşletme içinde BT ile ilgili risklerin aidiyet ve sorumluluğunu ilgili üst düzey seviyeye entegre edilmelidir. Bilgi güvenliği, fiziksel güvenlik ve uyumdan kaynaklanan sorumluluk dahil olmak üzere BT risklerinin yönetimi açısından kritik olan roller tanımlanarak tahsis edilmelidir. Müessese çapındaki sorunları ele alabilmek için müessese çağındaki düzeyde risk ve güvenlik yönetimi sorumluluğu oluşturulmalıdır. İlgili güvenlik sorunlarının ele alınabilmesi için ilave güvenlik yönetim sorumlulukları sisteme özgü düzeyde tahsis edilmelidir. BT risklerinin alınabilirliği ve arta kalan tüm BT risklerinin onaylanması konusunda üst düzey yönetimden talimat alınmalıdır (Önel ve Dinçkan 2007, 334).

PO4.9 Veri ve Sistem Mülkiyeti

İşletmeye veri ve bilişim sistemlerinin mülkiyetinden kaynaklanan sorumlulukların ele alınabileceği şekilde prosedür ve araç sağlanmalıdır. Bilgi ve

sistemlerin sınırlandırılması ve bu sınıflandırmaya göre korunması konusundaki kararlar sahipler tarafından verilmelidir (www.itgi.org, Erişim:18/01/2014).

PO4.10 Denetleme

Rol ve sorumlulukların gerektiği şekilde yerine getirilmesinden emin olmak, rol ve sorumluluklarını yerine getirmek için personelin tamamının yeterli yetki ve kaynaklara sahip olup olmadığını değerlendirmek ve genel olarak ana performans göstergelerini gözden geçirmek için BT işlevi içerisinde gerekli denetleme uygulamaları yürütülmelidir (www.itgi.org, Erişim:18/01/2014).

PO4.11 Sorumlulukların Ayrıştırılması

Tek bir bireyin kritik bir süreci bozması ihtimalini azaltacak şekilde rol ve sorumluluklar ayrıştırılmalıdır. Yönetim ayrıca personelin yalnızca, ilgili iş ve pozisyonlarına uygun, yetki aldıkları görevleri yerine getirmesi sağlanmalıdır.

PO4.12 BT Personel Alımı

BT işlevi için yeterli sayıda yetkin BT personelinin bulunduğundan emin olabilmek için personel alım ihtiyaçlarını işletme, işlevsel çevre yada BT çevresinde yapılan büyük değişiklikler üzerine değerlendirilmelidir. Personel alımında işletme/BT personelinin karşılıklı konumu, işlevler arası iş rotasyonu ve dış kaynak kullanımı dikkate alınmalıdır (Önel ve Dinçkan, 2007, 337).

PO4.13 Ana BT Personeli

Ana BT personeli tanımlanmalıdır ve tespit edilmelidir ve bunlara olan aşırı bağlılık en aza indirgenmelidir. Acil durum halinde ana personele ulaşma planı bulunmalıdır.

PO4.14 Sözleşmeli Personel Politika ve Prosedürleri

Müessesenin bilgi varlıklarının korunmasının sağlamak ve kararlaştırılan sözleşeme şartlarının yerine getirmek amacıyla danışman ve diğer sözleşmeli

personelin faaliyetlerinin BT işleviyle ile kontrolü için politika ve prosedür tanımlanmalıdır ve uygulanmalıdır (www.itgi.org, Erişim:18/01/2014).

PO5 BT Yatırımını Yönetme

- PO5.1 Mali Yönetim Çerçevesi
- PO5.2 BT Bütçesi içinde Önceliklerin Tanınması
- PO5.3 BT Bütçe Oluşturma Prosesi
- PO5.4 Maliyet Yönetimi
- PO5.5 Fayda Yönetimi

PO5.1 Mali Yönetim Çerçevesi

Yatırım, hizmet ve varlık portföyleri bazında bütçe oluşturma ve maliyet/fayda analizini belirleyen BT için mali bir çerçeve oluşturulmalıdır. Mevcut BT bütçesinin temelini teşkil eden BT-etkili yatırım programları, BT hizmetleri ve BT varlıklarının portföyleri tutulmalıdır. Mevcut BT varlık ve hizmet portföylerini dikkate alarak yeni yatırımlar için iş olur incelemelerine girdi sağlanmalıdır. Hizmet ve varlık portföylerine yeni yatırımlar ve bakım BT bütçesinin geleceğini etkileyecektir. Bu portföylerin maliyet ve fayda bilgilerini bütçe içinde önceliklerin tanınması, maliyet yönetimi ve fayda yönetimi süreçleri kullanılmalıdır (Önel ve Dinçkan, 2007, 340).

PO5.2 BT Bütçesi İçinde Önceliklerin Tanınması

İşletmenin portföyünde BT-etkili yatırım programları ve diğer BT hizmet ve varlıklarının getirisini optimum hale getirmeye yönelik BT' nin katkısını en yüksek seviyeye çıkarmak için işlemler, projeler ve bakım için BT kaynaklarının tahsisine öncelik tanımak amacıyla bir karar alma süreci uygulanmalıdır.

PO5.3 BT Bütçe Oluşturma Süreci

İşletmenin BT-etkili yatırım programları portföyü tarafından belirlenen öncelikleri yansıtan ve mevcut altyapıyı çalıştırma ve devam ettirmenin sürekli

maliyetlerini dahil eden bir bütçeyi hazırlama ve sürdürmenin süreci oluşturulmalıdır (Önel ve Dinçkan, 2007, 337). Bu süreç genel bir BT bütçesinin gelişmesini desteklerken aynı zamanda, programların BT bileşenlerine özel vurgu ile birlikte ayrı programlar için geliştirme bütçelerini desteklemelidir. Süreç, genel bütçe ile ayrı programlara ait bütçelerin sürekli olarak gözden geçirilmesi, ayarlanması ve onaylanmasına izin vermelidir (Birengel 2006, 149).

PO5.4 Maliyet Yönetimi

Gerçek maliyetleri bütçelerle karşılaştıran bir maliyet yönetimi süreci uygulanmalıdır. Maliyetler takip edilerek rapor edilmelidir. Sapmalar söz konusu olduğunda bunlar zamanında tespit edilerek bunların programlar üzerindeki etkisi değerlendirilmelidir ve bu programların iş sponsoruyla birlikte uygun çözüm önlemleri alınmalıdır ve gerekirse programın iş olur incelemesi güncellenmelidir.

PO5.5 Fayda Yönetimi

Fayda takip süreci uygulanmalıdır. BT-etkili yatırım programlarının bileşeni yada düzenli işlevsel desteğin bir parçası olarak BT' nin iş sonuçlarına beklenen katkısı tespit edilmelidir, kararlaştırılmalıdır, takip edilmelidir ve raporlanmalıdır. Raporlar gözden geçirilmelidir ve BT' nin katkısını iyileştirme fırsatları söz konusu olduğunda gereken önlemler tespit edilerek alınmalıdır (Önel ve Dinçkan, 2007, 337). BT' nin katkısında gerçekleşen değişiklikler programı etkilediğinde ya da ilgili diğer projelerdeki değişiklikler programı etkilediğinde programın iş olur incelemesi güncellenmelidir.

PO6 Yönetim Hedefleri ve Yönünü Bildirme

- PO6.1 BT Politikası ve Kontrol Ortamı
- PO6.2 İşletme BT Riski ve İç Kontrol Çerçevesi
- PO6.3 BT Politikalarının Yönetimi
- PO6.4 Politikanın Yaygınlaştırılması
- PO6.5 BT Amaçlarının Bildirilmesi ve Yönlendirme

PO6.1 BT Politikası ve Kontrol Ortamı

"BT için, işletmenin felsefe ve çalışma tarzına göre düzenlenmiş bir kontrol ortamının unsurları tanımlanmalıdır. Bu unsurlar, BT yatırımlarından değer elde edilmesiyle ilgili beklentiler/ihtiyaçlar, risk alınabilirliği, bütünlük, etik değerler, personel yetkinliği, hesap verebilirlik ve sorumluluğu kapsamalıdır. Kontrol ortamı, ciddi riskleri yönetirken değerlerin elde edilmesini destekleyen, bölümler arası işbirliği ve takım çalışmasını teşvik eden, uyumluluk ve sürekli süreç iyileştirmeyi ilerleten ve süreç sapmalarıyla (başarısızlık dahil) iyi başa çıkan bir kültüre dayanmalıdır(Osborne 2006, 113).

PO6.2 İşletme BT Riski ve İç Kontrol Çerçevesi

BT kaynak ve sistemlerini korurken değer sunabilmek için işletmenin risk ve iç kontrole genel yaklaşımını tespit eden bir çerçeve geliştirerek sürdürülmelidir. Çerçeve BT süreç çerçevesi ve kalite yönetim sistemiyle entegre edilerek genel iş maçlarına uymalıdır. Çerçeve, önleyici faaliyetler, düzensizliklerin zamanında tespiti, kayıpların sınırlanması ve iş varlıklarının zamanında kurtarılması yoluyla bilgi varlıklarına yönelik riskleri en aza indirgerken değer elde etme başarısını maksimum seviyeye çıkarmaya yönelik olmalıdır (Osborne 2006, 113).

PO6.3 BT Politikalarının Yönetimi

BT stratejisini desteklemek için bir takım politikalar geliştirerek sürdürülmelidir. Bu politikalar politika niyeti, rol ve sorumluluklar, istisna süreci, uyumluluk yaklaşımı ve prosedür, standart ve kılavuzlara referansı içermelidir. Politikalar, kalite, güvenlik, gizlilik, iç kontroller ve fikri mülkiyet gibi ana konuları ele almalıdır. Bunların güncelliği düzenli olarak teyit edilerek onaylanmalıdır (www.itgi.org, Erişim:18/01/2014).

PO6.4 Politikanın Yaygınlaştırılması

İşletme işlemleri üzerine kurulu ve bu işlemlerin ayrılmaz bir parçası haline getirilmesini sağlamak için BT politikalarının ilgili personelin tamamı arasında yaygınlaştırıldığından ve yürütülerek uygulandığından emin olunmalıdır.

PO6.5 BT Amaçlarının Bildirilmesi ve Yönlendirme

İş ve BT amaçları ile yönlendirmenin bilinci ve anlaşılmasının işletme çapında bildirilerek yaygınlaşması sağlanmalıdır. Bildirilen bilgi, net bir şekilde belirtilmiş misyon, hizmet amaçları, güvenlik, iç kontroller, kalite, etik/davranış kuralları, politika ve prosedürler, vs. içermeli ve üst düzey yönetim tarafından hem konuşma hem de fiiliyat olarak desteklenen sürekli bir iletişim programına dahil edilmelidir. Yönetim, BT güvenlik bilincini ve BT güvenliğinin herkesin sorumluluğunda olduğu mesajını yaygınlaştırma özellikle dikkat etmelidir (www.itgi.org, Erişim:18/01/2014).

PO7 BT İnsan Kaynaklarını Yönetme

- PO7.1 Personel Alımı ve İstihdam
- PO7.2 Personel Yetkinlikleri
- PO7.3 Roller için Personel Alımı
- PO7.4 Personel Eğitimi
- PO7.5 Bireylere Bağlılık
- PO7.6 Personel Onay Prosedürleri
- PO7.7 Çalışanın İş Performansı Bakımından Değerlendirilmesi
- PO7.8 İş Değişikliği ve İşe Son Verilmesi

PO7.1 Personel Alımı ve İstihdam

BT personel alım süreçlerinin kuruluşun genel personel politikaları ve prosedürlerine (örn. İşe alım, pozitif çalışma ortamı ve oryantasyon) uygun olması sağlanmalıdır. Yönetim, organizasyon hedeflerine ulaşabilmek için gerekli yeteneklere sahip, gerekli şekilde istifade edilen Bilgi Teknolojileri işgücünün müessesede bulunmasını sağlamak için süreçler uygulanmalıdır. (Uzunay 2007, 199)

PO7.2 Personel Yetkinlikleri

Personelin, eğitim, öğretim ve/veya tecrübeleri bazında rollerini yerine getirme yetkinliklerinin bulunup bulunmadığını düzenli olarak kontrol edilmelidir.

Ana BT yetkinlik şartlarını tanımlayarak gerektiğinde kalifikasyon ve belgeleme programlarını kullanarak bunlara uyulduğunu doğrulanmalıdır.

PO7.3 Roller için Personel Alımı

Yönetim politika ve prosedürleri, etik ve mesleki uygulamalarına bağlı kalma şartı dahil olmak üzere personel için rol, sorumluluk ve telafi çerçeveleri tanımlanmalıdır, takip edilmelidir ve denetlenmelidir. İstihdam şartları çalışanın bilgi güvenliği, iç kontrol ve tüzüklere uyum konusundaki sorumluluğunu vurgulamalıdır. Denetim düzeyi, pozisyonun hassasiyetine ve tahsis edilen sorumluluk derecesine uygun olmalıdır. BT çalışanlarına işe alındığında uygun oryantasyon ve bilgi, yetenek, imkan, iç kontrol ve güvenlik bilinçlerini, organizasyon hedeflerine ulaşabilmek için gerekli seviyede tutmak için sürekli eğitim sağlanmalıdır (Birengel 2006, 152).

PO7.5 Bireylere Bağlılık

Bilginin belgelenmesi, bilgi paylaşımı, birbirine vekalet edebilecek pozisyonların planlanması ve personelin yedeklenmesi yoluyla ana bireylere kritik bağlılık ihtimali en aza indirgenmelidir.

PO7.6 Personel Onay Prosedürleri

Bilgi Teknolojileri için personel alım sürecine geçmiş kontrolünü dahil edilmelidir. Bu kontrollerin periyodunun derece ve sıklığı işlevin hassasiyeti ve/veya kritikliğine bağlı olup çalışan, yüklenici ve satıcılara uygulanmalıdır.

PO7.7 Çalışanın İş Performansı Bakımından Değerlendirilmesi

Müessesenin hedeflerinden türetilen bireysel hedefler, belirlenen standartlar ve işe özgü sorumluluklar bazında düzenli olarak zamanında değerlendirme yapılması talep edilmelidir. Gerektiğinde çalışanlar performans ve davranış konusunda eğitim alabilmelidir (Uzunay 2007, 185).

PO7.8 İş Değişikliği ve İşe Son Verilmesi

Bilgi Teknolojilerinde iş değişiklikleri, özellikle de işten çıkarmalar konusunda uygun önlemler alınmalıdır. Riskler en aza indirgeneceği ve işlev sürekliliğinin garantileneceği şekilde bilgi transferi düzenlemeleri yapılmalıdır, sorumluluklar yeniden tahsis ve erişim hakları iptal edilmelidir.

PO8 Kaliteyi Yönetme

- PO8.1 Kalite Yönetim Sistemi
- PO8.2 BT Standartları ve Kalite Uygulamaları
- PO8.3 Geliştirme ve İktisap Standartları
- PO8.4 Müşteri Odağı
- PO8.5 Sürekli İyileştirme
- PO8.6 Kalite Ölçümü, Takip ve Gözden Geçirme

PO8.1 Kalite Yönetim Sistemi

İş şartlarına uygun kalite yönetimine ilişkin standart, resmi ve sürekli bir yaklaşım sağlayan bir KYS 'ni oluşturulmalıdır ve sürdürülmelidir. KYS, kalite şart ve kriterleri, ana BT süreçleri ve bunların sıra ve aralarındaki etkileşimi ile uygunsuzlukların tanımlanması, tespit edilmesi, düzeltilmesi ve önlenmesi amaçlı politika, kriter ve yöntemleri tanımlar. KYS, rol, görev ve sorumlulukları kapsayacak şekilde kalite yönetimi için organizasyon yapısını tanımlamalıdır. Tüm ana alanlar kalite planlarını, kriter ve politikalara uygun olarak geliştirir ve kalite verilerinin kaydı tutulmalıdır. KYS 'nin etkililiği ve kabul edilebilirliğini takip edilerek ölçülmelidir ve gerektiğinde iyileştirilmelidir (Kovacich 2003, 69).

PO8.2 BT Standartları ve Kalite Uygulamaları

Kalite Yönetim Sistemi niyetine ulaşma konusunda müesseseye kılavuzluk etmek üzere ana BT süreçleri için standart, prosedür ve uygulamaları tanımlanmalıdır ve sürdürülmelidir. Müessesenin kalite uygulamaları iyileştirilmelidir ve planlarken sektörün en iyi uygulamaları kullanılmalıdır.

PO8.3 Geliştirme ve Tedarik Standartları

Nihai elde edilebilenin hayat döngüsünü takip eden tüm geliştirme ve tedarikler için standartlar oluşturulmalıdır ve sürdürülmelidir. Kararlaştırılan onay kriterleri bazında ana kilometre taşlarında onay kullanılmalıdır. Dikkate alınacak konular arasında yazılım kodlama standartları; isimlendirme kararları; dosya biçimleri; şema ve veri sözlüğü tasarım standartları; kullanıcı arabirimi standartları; karşılıklı çalışabilirlik; sistem performans verimliliği; ölçeklenebilirlik; geliştirme ve test standartları; şartlara göre doğrulama; test planları ve birim, regresyon ile entegrasyon testleri bulunmalıdır (Hansche 2003, 39).

PO8.4 Müşteri Odağı

Müşterilerin şartlarını tespit ederek ve bu şartları Bilgi Teknolojileri standart ve uygulamalarına entegre ederek kalite yönetiminin müşterilere odaklanması sağlanmalıdır. Kullanıcı/müşteri ile BT müessesesi arasındaki anlaşmazlıkların çözümü ile ilgili rol ve sorumluluklar tanımlanmalıdır.

PO8.5 Sürekli İyileştirme

Sürekli iyileştirmeyi kolaylaştıran genel kalite planı sürdürülmeli ve düzenli açıklanmalıdır.

PO8.6 Kalite Ölçümü, Takip ve Gözden Geçirme

KYS ve KYS 'nin sunmuş olduğu değere sürekli uyumu takip etmek için gerekli ölçümler tanımlanmalı ve uygulanmalıdır. Bilgilerin ölçüm, takip ve kaydedilmesi süreç sahibi tarafından ilgili düzeltme ve önleme faaliyetlerinde bulunmak için kullanılmalıdır (Yıldız, 2007, 73).

PO9 BT Risklerini Değerlendirerek Yönetme

- PO9.1 BT ve İş Riski Yönetiminin Uyumlaştırılması
- PO9.2 Risk Bağlamının Tespiti
- PO9.3 Olay Tanımlama
- PO9.4 Risk Değerlendirme

- PO9.5 Risk Yanıtı
- PO9.6 Risk Faaliyet Planının Sürdürülmesi ve Takibi

PO9.1 BT ve İş Riski Yönetiminin Uyumlaştırılması

BT yönetimi, risk yönetimi ve kontrol çerçevesini müessesenin (işletmenin) risk yönetimi çerçevesiyle entegre edilmelidir. Bu, müessesenin risk alınabilirlik ve riske tahammül seviyesiyle uyumlaştırmayı da kapsamaktadır.

PO9.2 Risk İçeriğinin Tespiti

Uygun sonuçları sağlamak için risk değerlendirme çerçevesinin uygulandığı içerik tespit edilmelidir. Her risk değerlendirmesinin iç ve dış bağlamının tespiti, değerlendirmenin amacı ve riskler değerlendirilirken kullanılacak kriterler bu kapsam dahil edilmelidir (Uzunay 2007, 185).

PO9.3 Olay Tanımlama

İş, yönetmenlik, yasa, teknoloji, ticari ortak, insan kaynakları ve işlevsel unsurlar dahil olmak üzere, işletmenin hedeflerine potansiyel bir etkiye sahip olan tüm olaylar tanımlanmalıdır. Olumlu ya da olumsuz olmak üzere etkinin özelliği de tespit edilerek bu bilgiler sürdürülmelidir (Uzunay 2007, 185).

PO9.4 Risk Değerlendirme

Tekrarlanabilirlik bazında nicel ve nitel yöntemler kullanarak tanımlanmış tüm risklerin ihtimal ve etkisi değerlendirilmelidir. İçsel ve arta kalan riskle ilgili ihtimal ve etki ayrı-ayrı olarak, kategoriye göre portföy bazında tespit edilmelidir.

PO9.5 Risk Yanıtı

"Risk sahibi ile etkilenen süreç sahipleri tespit edilmelidir, uygun maliyetli kontrol ve güvenlik önlemlerinin sürekli olarak risklere karşı savunmasızlığı hafifletmesini sağlamak için risk yanıtı geliştirilerek sürdürülmelidir. Risk yanıtı, önleme, azaltma, paylaştırma ya da kabul şeklinde risk stratejilerini tanımlamalıdır. Yanıtı geliştirirken maliyet ve faydaları dikkate alınız ve arta kalan riskleri belirli risk tahammül sınırları içerisinde tutan yanıtlar tercih edilmelidir." (Birengel 2006, 178).

PO9.6 Risk Faaliyet Planının Sürdürülmesi ve Takibi

Maliyet, fayda ve uygulama sorumluluğunun tespit edilmesi dahil olmak üzere gerekli olarak tanımlanan risk yanıtlarının uygulanması amaçlı kontrol faaliyetler tüm seviyelerde öncelik sırasına göre planlanmalıdır. Önerilen faaliyetler için onay ve arta kalan tüm riskler için kabul istenmelidir, yapılan faaliyetlerin, etkilenen süreç sahibi (sahipleri) tarafından sahiplenmesi sağlanmalıdır. Planların yerine getirilmesi takip edilerek tüm sapmalar üst düzey yönetime raporlanmalıdır(Uzunay 2007, 185).

PO10 Projeleri Yönetme

- PO10.1 Program Yönetim Çerçevesi
- PO10.2 Proje Yönetim Çerçevesi
- PO10.3 Proje Yönetim Yaklaşımı
- PO10.4 Paydaş Bağlılığı
- PO10.5 Proje Kapsam Beyanı
- PO10.6 Proje Aşamasının Başlatılması
- PO10.7 Entegre Proje Planı
- PO10.8 Proje Kaynakları
- PO10.9 Proje Risk Yönetimi
- PO10.10 Proje Kalite Planı
- PO10.11 Proje Değişiklik Kontrolü
- PO10.12 Güvence Yöntemlerinin Proje Planlaması
- PO10.13 Proje Performansının Ölçülmesi, Raporlanması ve Takibi
- PO10.14 Proje Kapanışı

PO10.1 Program Yönetim Çerçevesi

Projeler tespit edilmelidir, tanımlanmalıdır, değerlendirmelidir, önceliklendirilmelidir, seçilmelidir, başlatılmalıdır, yönetilmelidir ve kontrol edilmelidir. BT etkili yatırım programlarının portföyüyle ilgili projelerin programını tutulmalıdır. Projelerin, program hedeflerini desteklemesi sağlanmalıdır. Çoklu projelerin faaliyet ve birbirine bağlılığını koordine edilmelidir, program içindeki tüm

projelerin beklenen sonuçlara katkısını yönetilmelidir ve kaynak ihtiyaçları ile anlaşmazlıkları çözülmelidir.

PO10.2 Proje Yönetim Çerçevesi

Projeleri yönetmenin kapsamı ve sınırlarını, ayrıca da üstlenilen her projede benimsenen ve uygulanan yöntem sistemlerini tanımlayan bir proje yönetim çerçevesi kurularak sürdürülmelidir. Yöntem sistemleri minimum olarak projelerin başlangıç, planlama, yürütme, kontrol ve kapanış aşamaları, ayrıca da kontrol noktaları ve onayları kapsamalıdır. Çerçeve ve destek niteliğindeki yöntem sistemleri, işletme portföy yönetimi ve program yönetim süreçleriyle entegre edilmelidir (Johnson 2007, 258).

PO10.3 Proje Yönetim Yaklaşımı

"Her projenin boyut, karmaşıklık ve yönetmenlik gereksinimleriyle orantılı birer proje yönetim yaklaşımı oluşturulmalıdır. Proje yönetim yapısı program sponsorunun rol, sorumluluk ve hesap verebilirlikleri, proje sponsorları, yürütme komitesi, proje bürosu ile proje müdürü ve bunların söz konusu sorumlulukları (raporlama ve aşamaların gözden geçirilmesi gibi) yerine getirebilecekleri mekanizmaları içermelidir. Tüm BT projelerinin, stratejik programın tamamı boyunca projenin yürütülmesini sahiplenmek için yeterli yetkiye sahip sponsorların bulunmasına dikkat edilmelidir." (Hansche 2003, 64).

PO10.4 Paydaş Bağlılığı

Projenin, BT-etkili yatırım programının tamamı bağlamı dahilinde tanımlanmalıdır ve yürütülmesinden etkilenen paydaşların bağlılık ve katılımı sağlanmalıdır.

PO10.5 Proje Kapsam Beyanı

Paydaşlar arasında projenin ve BT-etkili yatırım programının tamamı içerisindeki diğer projelerle nasıl bağlantılı olduğunun genel olarak anlaşılmasını sağlamak ve bu anlayışı geliştirmek amacıyla projenin özellik ve kapsamı

tanımlanarak belgelenmelidir. Proje başlatılmadan önce söz konusu proje sponsorlar tarafından resmi olarak onaylanmalıdır (Uzunay 2007, 185).

PO10.6 Proje Aşamasının Başlatılması

Ana proje aşamalarının başlatılmasının resmi olarak onaylanarak tüm paydaşlara bildirilmesi sağlanmalıdır. Başlangıç aşamasının onaylanması, program yönetimi kararlarına bağlı olmalıdır. Sonraki aşamaların onayı bir önceki aşamada elde edilenlerin gözden geçirilerek kabul edilmesi ve programın bir sonraki büyük gözden geçirilişinde güncellenmiş iş olur incelemesinin onaylanmasına bağlı olmalıdır. Proje aşamalarının üst üste binmesi (örtüşmesi) durumunda onay noktası, projenin ilerlemesinin onaylanması için program ve proje sponsorları tarafından tespit edilmelidir (Kovacich 2003, 65).

PO10.7 Entegre Proje Planı

Proje ömrü boyunca projenin yürütülmesi ve proje kontrolüne kılavuzluk etmek üzere (iş ve bilişim sistemleri kaynaklarını kapsayan) resmi, onaylı ve entegre bir proje planı oluşturulmalıdır (Hansche 2003, 64). Çoklu projelerin program içindeki faaliyet ve birbirine bağlılıkları anlaşılmalı ve belgelenmelidir. Proje planı, projenin ömrü boyunca sürdürülmelidir. Proje planı ve ona yapılan değişiklikler, program ve proje yönetim çerçevesine uygun olarak onaylanmalıdır.

PO10.8 Proje Kaynakları

Proje takım üyelerinin sorumluluk, ilişki, yetkiler ve performans kriterleri tanımlanmalıdır ve projede yetkin personelin ve/veya sözleşmeli elemanların alınarak görevlendirilmesi için temel tanımlanmalıdır. Her proje için gerekli ürün ve hizmetlerin istihsali, müessesenin istihsal uygulamalarını kullanarak proje hedeflerine ulaşmak için planlanmalıdır ve yönetilmelidir (Pekel 2008, 35).

PO10.9 Proje Risk Yönetimi

İstenmeyen değişikliklere neden olma potansiyeli bulunan alan yada olaylar için sistematik bir planlama, tanımlama, analiz, yanıt, takip ve kontrol süreciyle ayrı projelerle ilgili spesifik riskler ortadan kaldırılmalıdır yada en aza indirgenmelidir. Proje yönetim süreci ve projeden elde edilenlerin maruz kaldığı riskler tespit edilmeli ve kesinlikle kayda geçirilmelidir.

PO10.10 Proje Kalite Planı

Proje kalite sistemi ve bu sistemin nasıl uygulanacağını tanımlayan bir kalite yönetim planı hazırlanmalıdır. Plan, ilgili tüm taraflarca resmi olarak gözden geçirilerek kararlaştırılmalı ve daha sonra entegre proje planına alınmalıdır.

PO10.11 Proje Değişiklik Kontrolü

Projenin ana kısmına (örn. maliyet, program, kapsam ve kalite) yapılan tüm değişiklikler gerektiği şekilde gözden geçirilmelidir, onaylanmalıdır ve entegre proje planına program ve proje yönetim çerçevesine uygun olarak konulması için her proje için değişiklik kontrol sistemi oluşturulmalıdır (Pekel 2008, 35).

PO10.12 Güvence Yöntemlerinin Proje Planlaması

Proje planlama sırasında yeni yada değiştirilen sistemlerin akreditasyonu (tanınmasını) desteklemek için gerekli güvence görevlerini tespit ederek bunları entegre proje planı kapsamına alınmalıdır. Görevler, iç kontrol ve güvenlik özelliklerinin tanımlanan şartlara uygun olduğunun güvencesini sağlamalıdır.

PO10.13 Proje Performansının Ölçülmesi, Raporlanması ve Takibi

Proje performansı ana proje kriterlerine (örn. kapsam, program, kalite, maliyet ve risk) göre ölçülmelidir; gerçekleşen tüm plandan saplamaları tespit edilmelidir; bunların proje ve program geneline olan etkisini değerlendirilmelidir; sonuçları ana paydaşlara bildirilmelidir ve gerektiğinde program ve proje yönetim çerçevesine uygun olarak sorun giderme faaliyetleri önerilmelidir, uygulanmalıdır ve takibini yapılmalıdır (Hansche 2003, 64).

PO10.14 Proje Kapanışı

Her projenin sonunda proje paydaşlarının, projenin planlanan sonuç ve faydaları sağlayıp sağlamadığını tespit etmeleri talep edilmelidir. Projenin planlanan sonuçları ve programın faydalarını elde etmek için gerekli, eksik kalmış tüm faaliyetler tespit edilerek bildirilmelidir ve gelecekteki proje ve programlarda kullanılmak üzere alınan tüm ders ve çıkarımlar tespit edilerek belgelenmelidir (Pekel 2008, 35).

2.2.Tedarik ve Uygulama

Tedarik ve Uygulama alanı BT gereksinimlerini belirleme, teknolojiyi satın alma ve kurumun mevcut iş süreçlerine uyarlama için kurumun stratejilerini adreslemektedir. Bu alan aynı zamanda bilgi teknolojileri sisteminin ve parçalarının hayatını sürdürebilmesi için kurumun kabulleneceği bir bakım planı geliştirilmesini içermektedir.

Tedarik ve Uygulama alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır: (Vural ve Sağıroğlu 2008, ss.630-652)

- AI1 Otomatize Edilmiş Çözümleri Tanımlama
- AI2 Uygulama Yazılımını Temin Ederek Bulundurma
- AI3 Teknoloji Altyapısını Temin Ederek Sürdürme
- AI4 Çalışma ve Kullanımı Etkinleştirme
- AI5 BT Kaynaklarını Elde Etme
- AI6 Değişiklikleri Yönetme
- AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu

AI1 Otomatize Edilmiş Çözümleri Tanımlama

- AI1.1 İşletmenin İşlevsel ve Teknik Şartlarının Tanımlanarak Sürdürülmesi
- AI1.2 Risk Analiz Raporu
- AI1.3 Fizibilite Araştırması ve Alternatif Faaliyet Yollarının Oluşturulması
- AI1.4 Şartlar ve Fizibilite Kararı ile Onayı

AI1.1 İşletmenin İşlevsel ve Teknik Şartlarının Tanımlanarak Sürdürülmesi

BT-etkili yatırım programının beklenen sonuçlarını elde etmek için gerekli tüm inisiyatiflerin tam kapsamını dahil eden, işletmenin işlevsel ve teknik şartları tanımlanmalıdır, önceliklendirilmelidir, belirtilmelidir ve kararlaştırılmalıdır. Şartların kabulü için kriterler tanımlanmalıdır. İşletmenin iş, iş süreçleri, insan yetenek ve yetkinlikleri, organizasyon yapısı ve işi kolaylaştıran teknolojisi için gerekli tüm değişiklikler bu inisiyatiflerin kapsamında olmalıdır (Pekel 2008, 35). İşin işlevsel ihtiyaçları, işletmenin teknolojik yönü, performans, maliyet, güvenilirlik, uyumluluk, denetlenebilirlik, güvenlik, kullanılabilirlik ve süreklilik, ergonomi, kullanım kolaylığı, emniyet ve yasalar ihtiyaçlarda dikkate alınmalıdır. Süregelen sistem tedarik ve geliştirmesinin kontrolü için temel olarak iş ihtiyaçlarının bütünlük, doğruluk ve cariliğini sağlama ve yönetme amaçlı süreçleri oluşturmalıdır. Bu ihtiyaçlar iş sponsoru tarafından sahiplenmelidir (Vural ve Sağıroğlu 2008, 630-652).

AI1.2 Risk Analiz Raporu

Müessesenin ihtiyaç geliştirme sürecinin bir parçası olarak iş süreçleriyle ilgili riskler tespit edilmelidir, belgelenmelidir ve analiz edilmelidir. Veri bütünlüğü, güvenliği, kullanılabilirliği, gizliliğine ve yasa ile yönetmenliklere uyuma karşı tehditler riskler arasındadır. Gerekli iç kontrol önlemleri ve denetim izleri bu ihtiyaçların bir parçası olarak tespit edilmelidir(Uzunay 2007, 185).

AI1.3 Fizibilite Araştırması ve Alternatif Faaliyet Yollarının Oluşturulması

İhtiyaçların uygulanabilirliğini inceleyen bir fizibilite araştırması geliştirilmelidir. Araştırma, yazılım, donanım, hizmet ve yetenekler için, işletmenin tespit edilen işlevsel ve teknik ihtiyaçlarını karşılayan alternatif faaliyet yolları tanımlamalıdır ve tanımlanan her faaliyet yolunun, BT-etkili yatırım programı bağlamında teknolojik ve ekonomik fizibilitesini (potansiyel maliyet ve fayda analizi) değerlendirmelidir. İş süreçlerine yapılan değişiklikler, teknoloji ve yetenekler gibi faktörlerin etkileri değerlendirildikçe

fizibilite araştırmasının geliştirilmesinde çok sayıda yineleme gerçekleşebilir. BT işleviyle desteklenen iş yönetimi fizibilite ve alternatif faaliyet yollarını değerlendirmeli ve iş sponsoruna öneride bulunmalıdır (Pekel 2008, 35).

AI1.4 Şartlar ve Fizibilite Kararı ile Onayı

Önceden tespit edilen önemli aşamalarda iş sponsoru işletmenin işlevsel ve teknik ihtiyaçları onaylanmalıdır teyit edilmelidir. Her teyit, kalite incelemelerinin başarılı bir şekilde geçmesi sonrası gerçekleşir. Çözüm ve tedarik yaklaşımı kararıyla ilgili nihai karar hakkı iş sponsoruna aittir.

AI2 Uygulama Yazılımını Temin Ederek Bulundurma

- AI2.1 Üst Düzey Tasarım
- AI2.2 Ayrıntılı Tasarım
- AI2.3 Uygulama Kontrolü ve Denetlenebilirliği
- AI2.4 Uygulama Güvenliği ve Kullanılabilirliği
- AI2.5 Tedarik Edilen Uygulama Yazılımının Konfigürasyon (Yapılandırma) ve Uygulanması
- AI2.6 Mevcut Sistemler için Ana Upgrade'ler (Yükseltimler)
- AI2.7 Uygulama Yazılımının Geliştirilmesi
- AI2.8 Yazılım Kalite Güvencesi
- AI2.9 Uygulama İhtiyaçlarının Yönetimi
- AI2.10 Uygulama Yazılımının Sürdürülmesi

AI2.1 Üst Düzey Tasarım

Müessesenin teknolojik yönü ve bilgi mimarisini dikkate alarak iş ihtiyaçları yazılım geliştirme için üst düzey tasarım spesifikasyonuna çevrilmelidir ve üst düzey tasarımının ihtiyaçlara cevap vermesini sağlamak için tasarım spesifikasyonları onaylanmalıdır. (IT Governance Institute, "CobiT 4.1", 2007)

AI2.2 Ayrıntılı Tasarım

Ayrıntılı yasarım ve teknik yazılım uygulama ihtiyaçları hazırlanmalıdır. İhtiyaçların kabulü için kriterler belirlenmelidir. Üst düzey tasarıma uygun olmalarını sağlamak için ihtiyaçlar onaylanmalıdır. Sınırlama konulmaksızın kapsama alınacaklar arasında giriş şartı tanımlaması ve belgeleri, arabirim tanımı, kullanıcı arabirimi, kaynak verilerini toplama tasarımı, program spesifikasyonu, dosya ihtiyaçlarının tanımı ve belgeleri, süreç ihtiyaçları, çıkış şartının tanımı, kontrol ve denetlenebilirlik, güvenlik ve kullanılabilirlik ve testler bulunmaktadır. Geliştirme ya da sürdürme sırasında önemli teknik yada mantıksal tutarsızlıkların ortaya çıkması halinde değerlendirme yeniden yapılmalıdır(Vural ve Sağıroğlu 2008, 630-652).

AI2.3 Uygulama Kontrolü ve Denetlenebilirliği

İş kontrollerinin, sürecin doğru, tam, zamanlı, yetkili ve denetlenebilir olacağı şekilde, gerektiği gibi uygulama kontrollerine çevrilmesi sağlanmalıdır. Özellikle ele alınacak konular yetkilendirme mekanizmaları, bilgi bütünlüğü, erişim kontrolü, yedekleme ve denetim izlerinin tasarımı konuları olmalıdır.

AI2.4 Uygulama Güvenliği ve Kullanılabilirliği

Tespit edilen risklere cevap ve veri sınıflandırılması, müessesenin bilgi güvenliği mimarisi ve risk profiline uygun olarak uygulama güvenliği ve kullanılabilirliği ele alınmalıdır. Ele alınacak konular arasında erişim hakları ve imtiyazların yönetimi, tüm aşamalarda hassas bilginin korunması, doğrulama ve işlem bütünlüğü ve otomatik kurtarma bulunmalıdır.

AI2.5 Tedarik Edilen Uygulama Yazılımının Konfigürasyon (Yapılandırma) ve Uygulanması

Yapılandırma, kabul ve test prosedürlerini kullanarak iktisat edilen otomatize işlevselliği uyarlanarak uygulanmalıdır. Ele alınarak konular arasında sözleşme

şartlarına göre doğrulama, müessesenin bilgi mimarisi, mevcut uygulamalar, mevcut uygulama ve veri tabanı sistemleriyle karşılıklı çalışabilirlik, sistem performans verimi, belgeler ve kullanım kılavuzları, entegrasyon ve sistem test planları bulunmalıdır (Uzunay 2007, 185).

AI2.6 Mevcut Sistemler için Ana Upgrade' ler (Yükseltimler)

Mevcut tasarımlar ve/veya işlevsellikte ciddi değişikliklere sebebiyet veren, mevcut sistemler ve büyük değişiklikler durumunda, yeni sistemlerin geliştirilmesine benzer geliştirme süreci izlenmelidir. Ele alınacak konular arasında etki analizi, maliyet/fayda doğrulaması ve ihtiyaçların yönetilmesi bulunmalıdır.

AI2.7 Uygulama Yazılımının Geliştirilmesi

Otomatize işlevselliğin tasarım spesifikasyonlarının, geliştirme ve belge standartları ve kalite şartlarına göre geliştirilmesi sağlanmalıdır. İşlevsellik, performans ve kalite incelemelerinin başarılı bir şekilde yapılmasından sonra uygulama yazılımını geliştirme sürecinin her ana aşamasına onay verilerek teyit edilmelidir. Ele alınacak konular arasında tasarım spesifikasyonlarının iş, işlevsellik ve teknik ihtiyaçlarına uygun olduğuna dair onay; değişiklik taleplerinin onaylanması ve uygulama yazılımının üretime uygun olup göç için hazır olduğu teyidi bulunmalıdır. Bunun yanı sıra, tüm yasal ve sözleşme ile ilgili unsurların tanımlanarak üçüncü taraflarca geliştirilen uygulama yazılımlarıyla ilgili olarak ele alınması sağlanmalıdır (Uzunay 2007, 185).

AI2.8 Yazılım Kalite Güvencesi

İhtiyaçlar tanımı ve müessesenin kalite politika ve prosedürlerinde belirtilen kaliteyi elde etmek için bir kalite güvence planı geliştirilmelidir ve plan için kaynak tahsis ederek plan uygulanmalıdır. Kalite güvencesi planında ele alınacak konular arasında kalite kriterleri belirtilmelidir ve, inceleme, deneme ve testler dahil, doğrulama ve kontrol süreçleri bulunmalıdır (Vural ve Sağıroğlu 2008, ss.630-652).

AI2.9 Uygulama İhtiyaçlarının Yönetimi

Tasarım, geliştirme ve uygulama sırasında ayrı ihtiyaçların (reddedilen tüm ihtiyaçlar dahil olmak üzere) durumu takip edilmelidir ve ihtiyaçlara yapılan değişikliklerin kurulu bir değişiklik yönetim süreci ile onaylanması sağlanmalıdır.

AI2.10 Uygulama Yazılımının Sürdürülmesi

Yazılım uygulamalarının sürdürülmesi ve onaylanması için strateji ve plan geliştirilmelidir. Ele alınacak konular arasında onay planlama ve kontrolü, kaynak planlama, küçük hata giderimi ve hataların düzeltilmesi, küçük iyileştirmeler, belgelerin bulundurulması, acil durum değişiklikleri, diğer uygulama ve altyapı ile karşılıklı bağlılık, yükseltme stratejileri, destek konuları ve yükseltmeler gibi sözleşme şartları, iş ihtiyaçlarına göre periyodik gözden geçirme, riskler ve güvenlik şartları bulunmalıdır (Uzunay 2007, 185).

AI3 Teknoloji Altyapısını Temin Ederek Sürdürme

- AI3.1 Teknoloji Altyapısı Tedarik Planı
- AI3.2 Altyapı Kaynaklarının Korunması ve Kullanılabilirliği
- AI3.3 Altyapının Bakımı (Sürdürülmesi)
- AI3.4 Fizibilite Testi Ortamı

AI3.1 Teknoloji Altyapısı Tedarik Planı

İşletmenin kurulu işlevsel ve teknik ihtiyaçlarını karşılayan ve müessesenin teknoloji yönüne uygun olan teknoloji altyapısının tedarik, uygulama ve sürdürülmesi için bir plan geliştirilmelidir. Planda, gelecekteki kapasite eklentileri için esneklik, geçiş masrafları, teknik riskler ve teknoloji yükseltmeleri (upgrades) için yatırımın ömrü dikkate alınmalıdır. Yeni teknik kapasite eklenirken karmaşıklık maliyetleri ve satıcı ile ürünün ticari olarak ayakta kalma şansı (finansal kapasitesini) değerlendirilmelidir.

AI3.2 Altyapı Kaynaklarının Korunması ve Kullanılabilirliği

Kaynakları korumak ve kullanılabilirlik ile bütünlüğü sağlamak için donanım ve altyapısal yazılımın yapılandırma, entegrasyon ve bakımı (sürdürülmesi) sırasında iç kontrol, güvenlik ve denetlenebilirlik önlemleri uygulanmalıdır. Hassas altyapı

bileşenlerinin kullanımıyla ilgili sorumluluklar net bir şekilde tanımlanmalıdır ve altyapı bileşenlerini geliştiren ve entegre edenler tarafından anlaşılmalıdır. Bunların kullanımı takip edilmelidir ve değerlendirilmelidir.

AI3.3 Altyapının Bakımı (Sürdürülmesi)

Altyapının sürdürülmesi için bir strateji ve plan geliştirilmelidir ve değişikliklerin, müessesenin değişiklik yönetim prosedürüne göre kontrol edilmesi sağlanmalıdır. İş ihtiyaçlarına göre periyodik gözden geçirme, yama yönetimi ve yükseltme(upgrade) stratejileri, riskler ve güvenlik ihtiyaçları kapsam dahiline alınmalıdır (Vural ve Sağıroğlu 2008, 630-652).

AI3.4 Fizibilite Testi Ortamı

Tedarik ve geliştirme sürecinin erken aşamalarında uygulama ve altyapının etkili ve verimli fizibilite ve entegrasyon testini desteklemek amacıyla geliştirme ve test ortamları oluşturulmalıdır. İşlevsellik, donanım ve yazılım konfigürasyonu, entegrasyon ve performans testi, ortamlar arasında göç, versiyon kontrolü, test araçları ve güvenliği ele alınmalıdır.

AI4 Çalışma ve Kullanımı Etkinleştirme

- AI4.1 İşlemsel Çözümleri İçin Planlama
- AI4.2 İşletme Yönetimine Bilgi Transferi
- AI4.3 Son Kullanıcılara Bilgi Transferi
- AI4.4 İşlemler ve Destek Personeline Bilgi Transferi

AI4.1 İşletimsel Çözümler için Planlama

Otomatize sistemler yada altyapının kullanıma alınması yada yükseltilmesi (upgrade) sonucunda tüm paydaşların yönetim, kullanıcı ve işlem prosedürlerinin üretilmesinde zamanında sorumluluk alabileceği şekilde tüm teknik unsurlar,

işlemsel kapasite ve gerekli hizmet seviyelerini tanımlamak ve belgelemek amacıyla bir plan geliştirilmelidir(www.itgi.org, Erişim: 18/01/2014).

AI4.2 İşletme Yönetimine Bilgi Transferi

Sistem ve verileri sahiplenmeleri ve hizmetlerin sunulması ile kalite, iç kontrol ve yönetim süreçlerinin uygulanmasından kaynaklanan sorumluluğu icra etmelerine izin vermek için işletme yönetimine bilgi transfer edilmelidir. Bilgi transferi erişim onayı, imtiyaz yönetimi, görevlerin ayrıştırılması, otomatik iş kontrolleri, yedekleme/kurtarma, fiziksel güvenlik ve kaynak belgelerin arşivlenmesini kapsamalıdır.

AI4.3 Son Kullanıcılara Bilgi Transferi

Son kullanıcılara, iş süreçlerini desteklemek amacıyla, uygulama sistemini etkili ve verimli bir şekilde kullanmalarına izin vermek için bilgi ve yetenek transferi gerçekleştirilmelidir. Bilgi transferi, başlangıçtaki ve devam eden eğitim ve yetenek gelişimi, eğitim materyalleri, kullanım kılavuzları, prosedür kılavuzları, çevrimiçi yardım, hizmet masası desteği, ana kullanıcının tanımlanması ve değerlendirilmesi konularını ele almak için bir Eğitim Prosedürünün geliştirilmesini kapsamalıdır.

AI4.4 İşlemler ve Destek Personeline Bilgi Transferi

İşlemler ve destek personelinin uygulama sistemi ve ilgili altyapıyı gerekli hizmet seviyelerine göre etkili ve verimli sağlama, destekleme ve sürdürmesine izin vermek için bilgi ve yetenek transferi gerçekleştirilmelidir. Bilgi transferi başlangıçtaki ve devam eden eğitim ve yeteneklerin gelişimi, eğitim materyalleri, çalışma kılavuzları, prosedür kılavuzları ve hizmet masası senaryolarını içermelidir.

AI5 BT Kaynaklarını Elde Etme

- AI5.1 Tedarik Kontrolü
- AI5.2 Tedarikçi Sözleşmesinin Yönetimi
- AI5.3 Tedarikçi Seçimi

- AI5.4 Yazılım Tedariki
- AI5.5 Geliştirme Kaynaklarının Tedariki
- AI5.6 Altyapı, Tesis ve İlgili Hizmetlerin Tedariki

AI5.1 Tedarik Kontrolü

BT ile ilgili altyapı, tesis, donanım, yazılım ve hizmetlerin iş ihtiyaçlarını karşılamasını sağlanmak için iş müessesinin genel istihsal süreci ve tedarik stratejisine uygun bir takım prosedür ve standartlar geliştirilerek bunlar izlenmelidir.

AI5.2 Tedarikçi Sözleşmesinin Yönetimi

Tüm tedarikçilerle sözleşmelerin akdedilmesi, değiştirilmesi ve feshi için bir prosedür oluşturulmalıdır. Prosedür minimum olarak, yasal konular, mali konular, organizasyon konuları, belge konuları, performans, güvenlik, güvenlik, fikri mülkiyet ve fesih sorumluluklar ve yükümlülüklerini (ceza hükümleri dahil) kapsamalıdır. Tüm sözleşme ve sözleşme değişiklikleri hukuk danışmanları tarafından incelenmelidir. (ITGI, 2007).

AI5.3 Tedarikçi Seçimi

Potansiyel tedarikçilerden alınan bilgi ile geliştirilmiş ve müşteri ile tedarikçi(ler) arasında kararlaştırılmış şartlar bazında sürdürülebilir en uygun alternatifi sağlamak için tedarikçiler adil ve resmi bir uygulamaya göre seçilmelidir.

AI5.4 Yazılım Tedariki

Tedarik ile ilgili tüm taahhüt sözleşmelerinde müessesenin çıkarlarının korunması sağlanmalıdır. Tedarik konusu yazılımın devam eden kullanımı için sözleşme şartlarına tüm tarafların hak ve sorumlulukları dahil edilerek icra edilmelidir. Bu hak ve sorumluluklar arasında fikri mülkiyetin mülkiyet hakları ve lisanslanması, bakım, garantiler, mahkeme prosedürleri, yükseltme (upgrade) şartları ve güvenlik, emanet ve erişim hakları dahil olmak üzere amacına uygunluk bulunmalıdır.

AI5.5 Geliştirme Kaynaklarının Tedariki

Tedarik ile ilgili tüm taahhüt sözleşmelerinde müessesenin çıkarlarının korunması sağlanmalıdır. Tedarik konusu geliştirme kaynaklarının dağıtımı için sözleşme şartlarına tüm tarafların hak ve sorumlulukları dahil edilerek icra edilmelidir. Bu hak ve sorumluluklar arasında fikri mülkiyetin mülkiyet hakları ve lisanslanması, geliştirme yöntem sistemleri, diller, test, istenilen performans kriterleri, performansın incelenmesi, ödeme temeli, garantiler, mahkeme prosedürleri, insan kaynakları yönetimi ve müessesenin politikalarına uyum dahil kalite yönetim süreçleri bulunmalıdır.

AI5.6 Altyapı, Tesis ve İlgili Hizmetlerin Tedariki

Altyapı, tesis ve ilgili hizmetlerin tedariki için kabul kriterleri dahil olmak üzere sözleşme şartlarına tüm tarafların hak ve sorumlulukları dahil edilerek icra edilmelidir. Bu hak ve sorumluluklar arasında hizmet seviyeleri, bakım prosedürleri, erişim kontrolleri, güvenlik, performans incelemesi, ödeme temeli ve mahkeme prosedürleri bulunmalıdır.

AI6 Değişiklikleri Yönetme

- AI6.1 Standart ve Prosedürleri Değiştiriniz
- AI6.2 Etki Değerlendirmesi, Önceliklendirme ve Yetkilendirme
- AI6.3 Acil Durum Değişiklikleri
- AI6.4 Değişiklik Durumunun İzlenmesi ve Raporlanması
- AI6.5 Değişikliğin Kapanışı ve Belgelenmesi (www.itgi.org, Erişim: 18/01/2014)

AI6.1 Standart ve Prosedürleri Değiştiriniz

Uygulama, prosedür, süreç, sistem ve hizmet parametreleri ile temelinde bulunan platformlara yapılan değişikliklerle ilgili tüm talepleri (bakım ve yamalar dahil) standartlaştırılmış bir şekilde işlemden geçirmek için resmi değişiklik yönetimin prosedürleri oluşturulmalıdır.

AI6.2 Etki Değerlendirmesi, Önceliklendirme ve Yetkilendirme

Tüm değişiklik taleplerinin, işletim sistemi ve onun işlevselliği üzerindeki etkiler bakımından yapılandırılmış bir şekilde değerlendirilmesi sağlanmalıdır. Bu değerlendirme değişikliklerin kategorilere ayrılması ve önceliklendirilmesini içermelidir. Üretime geçişten önce değişiklikler için ilgili paydaş tarafından onay verilmelidir.

AI6.3 Acil Durum Değişiklikleri

Kurulu değişiklik sürecini izlemeyen acil durum değişikliklerin tanımlanması, geliştirilmesi, değerlendirilmesi ve onaylanması için bir süreç oluşturulmalıdır. Belgeleme ve testler muhtemelen, acil durum değişikliği yapıldıktan sonra yapılır.

AI6.4 Değişiklik Durumunun İzlenmesi ve Raporları

Raporlama sistemi oluşturulmalıdır.

AI6.5 Değişikliğin Kapanışı ve Belgelenmesi

Sistem değişiklikleri her uygulandığında ilgili sistem ve kullanıcı belgeleri ile prosedürleri ona göre güncellenmelidir. Değişikliklerin eksiksiz olarak uygulanmasını sağlamak için gözden geçirme süreci oluşturulmalıdır.

AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu

- AI7.1 Eğitim
- AI7.2 Test Planı
- AI7.3 Uygulama Planı
- AI7.4 Test Ortamı
- AI7.5 Sistem ve Veri Dönüşümü
- AI7.6 Değişikliklerin Test Edilmesi
- AI7.7 Son Kabul Testi
- AI7.8 Üretim Promosyonu

- AI7.9 Yazılım Sürümü
- AI7.10 Sistem Dağıtımı
- AI7.11 Değişikliklerin Kaydı ve İzlenmesi (www.itgi.org, 18/01/2014)

AI7.1 Eğitim

Her enformasyon sistemi gelişiminin, uygulama veya modifikasyon projesinin bir parçası olarak, tanımlanan eğitim ve uygulama planı ve yardımcı materyaller ile birlikte BT fonksiyonu operasyon ve etkilenen kullanıcı bölümleri kadrosunun eğitimi sağlanmalıdır.

AI7.2 Test Planı

Bir test planı hazırlanması ve ilgili taraflardan onay alınmasıdır. Test planı kurum genelindeki standartlara dayanmalıdır ve rolleri, sorumlulukları ve başarı kriterleri tanımlanmalıdır. Plan hazırlanırken test hazırlığı (site hazırlığı dahil), eğitim gereklilikleri, tanımlanan test ortamının kurulması veya güncellenmesi, test vakalarının planlanması/ gerçekleştirilmesi/ belgelenmesi/ elde tutulması, hata işlemleri ve düzeltmeler, ve resmi onay dikkate alınmalıdır. Sistem başarısızlığı risk değerlendirmesi ve uygulama hatalarına dayanarak, plan performans, stres, kullanışlılık, pilot ve güvenlik testi için gereklikleri içermelidir.

AI7.3 Uygulama Planı

Bir uygulama planı oluşturulmalıdır ve ilgili taraflardan onay alınmalıdır. Plan, sürüm tasarımını, sürüm paketlerinin oluşturulmasını, ürünün yeni pazarlara girişi prosedürlerini/kurulumunu, olay işlemlerini, dağıtım kontrollerini (araçlar dahil), yazılım saklanmasını, sürüm revizyonunu ve değişikliklerin belgelenmesini tanımlar.

AI7.4 Test Ortamı

Test için ayrı bir test ortamı hazırlanmalıdır. Bu ortam sağlam testler için gelecek operasyonlar ortamını (örn. Benzer güvenlik, iç kontroller ve iş yükleri)

yansıtmalıdır. Test ortamında kullanılan prosedürlerin üretim ortamında kullanılacak verilerin (gerekirse temizlenmiş) temsilcisi olmasını sağlamak için prosedürler yerinde olmalıdır. Hassas test verilerinin açıklanmasını önlemek için yeterli önlemler alınmalıdır. Belgelendirilmiş test sonuçları elde tutulmalıdır

AI7.5 Sistem ve Veri Dönüşümü

Kurumun gelişme metotlarının tüm gelişme, uygulama veya modifikasyon projelerinin, donanım, yazılım, işlem verileri, veri dosyaları, yedekleme ve arşivler, diğer sistemlerle ara yüzler, prosedürler, sistem dokümantasyonu gibi tüm gerekli unsurların eski sistemden yenisine önceden belirlenmiş bir plana göre dönüştürmesi sağlanmalıdır. Dönüşüm öncesi ve sonrası sonuçlarının bir denetim raporu hazırlanmalıdır ve korunmalıdır. Yeni sistemin ilk sürecinin detaylı bir doğrulaması başarılı geçişi konfirme etmek için sistem sahipleri tarafından yapılmalıdır.

AI7.6 Değişikliklerin Test Edilmesi

Düzenli operasyonel ortamda kullanılmaya başlamadan değişikliklerin bağımsız (kuruculardan oluşan) bir test grubu tarafından ayrı bir test ortamında performans boyutunu içeren etki ve kaynak değerlendirmesine dayanan ve tanımlanan kabul planı ile uygun olarak test edilmesi sağlanmalıdır. Planın parçası olarak paralel veya pilot testi düşünülmelidir. Güvenlik kontrolleri, açılımdan önce test edilmeli ve değerlendirilmelidir, bu şekilde güvenlik etkinliği belgelenebilir. Geri çekme planları da üretim değişikliği promosyonundan önce geliştirilmelidir ve test edilmelidir.

AI7.7 Son Kabul Testi

Yeni veya modifiye edilmiş enformasyon sistemlerinin kalite güvence testi veya nihai kabulünün bir parçası olarak, prosedürler, etkilenen kullanıcı bölümleri ve BT fonksiyon yönetimi tarafından test sonuçlarının resmi değerlendirmesini ve onayını sağlamalıdır. Testler enformasyon sisteminin tüm unsurlarını (örn. Uygulama yazılımı, tesisler, teknoloji ve kullanıcı prosedürleri) kapsamalı ve tüm

unsurların enformasyon güvenlik gerekliliklerini karşılaması sağlanmalıdır. Test verileri denetim ve gelecekteki testler için saklanmalıdır.

AI7.8 Üretime Promosyon

Uygulama planı ile paralel olarak gelişmeden operasyonların test aşamasına kadar sistemin devir teslimini kontrol etmek için resmi prosedürler uygulanmalıdır. Yönetim gereğince sistem sahibi yetkisinin yeni bir sistemin üretime geçmesinden ve eski sistemin iptalinden önce alınmalıdır. Yeni sistemin günlük, aylık, üç aylık ve yıl-sonu üretim devrelerinde çalışması kontrol edilmelidir.

AI7.9 Yazılım Sürümü

Yazılım sürümünde oturumu kapatma, paketleme, regresyon testi, dağıtım, devir teslim, statü izleme, yedekleme prosedürleri ve kullanıcı bildirisi resmi prosedürleri izlenmelidir.

AI7.10 Sistem Dağıtımı

Zamanında ve doğru dağıtımın sağlanması ve onaylanan konfigürasyon ürünlerinin güncellenmesi için kontrol prosedürleri belirlenmelidir. Bunlar arasında entegre kontrolleri, yapan, test eden ve işletenler arasındaki görev ayrımı; ve tüm eylemlerin uygun denetim raporları olmalıdır.

AI7.11 Değişikliklerin Kaydı ve İzlenmesi

Uygulamalar, prosedürler, süreçler, sistem ve hizmet parametreleri ve altta yatan platformlar için yapılan değişikliklerin kaydı ve izlenmesini desteklemek ve uygulama sistem değişikliklerini izlemek için otomatik sistem kullanılmalıdır.

2.3.Hizmet Sunumu ve Destek

Hizmet Sunumu ve Destek alanı bilgi teknolojilerinin teslim yönüne odaklanmaktadır. Bu alan bilgi teknolojileri sistemindeki uygulamaların hayata

geçirilmesi ve sonuçları ile bu BT sistemlerinin etkin ve elverişli uyarlanmasını sağlayan destek süreçlerini de kapsamaktadır. Bu destek süreçleri güvenlik konuları ve eğitimini içermektedir.

Hizmet Sunumu ve Destek alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır: (Üvey 2009, 32)

- DS1 Hizmet Düzeyi Yönetimi
- DS2 Üçüncü Parti Hizmetlerin Yönetilmesi
- DS3 Performans ve Kapasite Yönetimi
- DS4 Sürekli Hizmetin Sağlanması
- DS5 Sistem Güvenliğinin Sağlanması
- DS6 Maliyetlerin Tanımlanması ve Dağıtımı
- DS7 Kullanıcıların Eğitimi ve Öğretimi
- DS8 Hizmet Masası ve Olaylar Yönetimi
- DS9 Konfigürasyon Yönetimi
- DS10 Sorun Yönetimi
- DS11 Veri Yönetimi
- DS12 Fiziksel Ortamların Yönetimi
- DS13 Operasyonların Yönetim

DS1 Servis Düzeyi Yönetimi

- DS1.1 Hizmet Düzeyi Yönetimi Çerçevesi
- DS1.2 Hizmetlerin Tanımı
- DS1.3 Hizmet Düzeyi Anlaşmaları
- DS1.4 İşletim Düzeyi Anlaşmaları
- DS1.5 Hizmet Düzeyi Başarılarının İzlenmesi ve Raporlanması
- DS1.6 Hizmet Düzeyi Anlaşmaları ve Sözleşmelerinin Revizyonu

DS1.1 Hizmet (Düzeyi) Yönetimi Çerçevesi

"Müşteri ve hizmet sağlayıcı arasında resmi hizmet düzey yönetim süreci sağlayan bir çerçeve tanımlanmalıdır. Bu çerçeve iş gereklilikleri ve öncelikleri için sürekli bir sıralama sağlamalı ve müşteri ve tedarikçi(ler) arasında ortak anlayışı kolaylaştırmalıdır. Çerçeve hizmet gerekliliklerinin oluşturulması, hizmet tanımları,

hizmet düzeyi anlaşmaları (SLA' ler), işletim düzeyi anlaşmaları (OLA 'ler) ve fon kaynakları için süreçleri içermelidir. Bu yaklaşımlar hizmet kataloğunda organize edilmelidir. Çerçeve iç ve dış hizmet sağlayıcılarının ve müşterilerin rollerini, görev ve sorumluluklarını kapsayan, hizmet düzeyi yönetimi için kurumsal yapıyı tanımlamalıdır." (Üvey 2009, 39).

DS1.2 Hizmetlerin Tanımı

Hizmet kataloğu yaklaşımı uygulaması üzerinden merkezi olarak organize edilen ve saklanan, hizmet özellikleri ve işletme gereklilikleri hakkında BT hizmetlerinin temel tanımlanmalıdır (Tyler 2000, 30–32) .

DS1.3 Hizmet (Düzeyi) Sözleşmeleri

"Müşteri gereklilikleri ve BT kapasitelerine dayanan tüm kritik BT hizmetleri için hizmet düzeyi anlaşmaları tanımlanmalı ve kabul prosedürleri belirlenmelidir. Bu, müşteri taahhütlerini, hizmet destek gerekliliklerini, hissedarlar tarafından sonlandırılan hizmet ölçümü için nicel ve nitel metrikleri, varsa fon ve ticari anlaşmaları, ve SLA gözetimi dahil rol ve sorumlulukları kapsamalıdır. Dikkate alınacak konular, bulunabilirlik, güvenilirlik, performans, büyüme kapasitesi, destek düzeyleri, süreklilik planlaması, güvenlik ve talep sınırları olmalıdır." (Üvey 2009, 45).

DS1.4 Operasyonel Hizmet (Düzeyi) Sözleşmeleri

İşletim düzeyi anlaşmaları optimal tarzda SLA' leri desteklemek için teknik olarak hizmetlerin nasıl dağıtılacağını açıklamalıdır. OLA' lar hizmet sağlayıcıya anlamlı olarak teknik süreçleri belirtmeli ve çeşitli SLA' ları desteklemelidir.

DS1.5 Hizmet (Düzeyi) Başarılarının İzlenmesi ve Raporlanması

Belirtilen hizmet düzeyi performans kriterleri sürekli olarak izlenmelidir. Hizmet düzeyi başarıları hakkında müşteriye anlamlı bir formatta raporlar sunulmalıdır. İzleme istatistikleri analiz edilmeli ve toplam hizmetler için olduğu gibi

bireysel hizmetler için de negatif ve pozitif trendlerin tanımlanması için bunlar kullanılmalıdır.

DS1.6 Hizmet (Düzeyi) Anlaşmaları ve Sözleşmelerinin Revizyonu

Hizmet anlaşmaları ve bağlı sözleşmelerin etkin, güncel olmasını ve gerekli değişikliklerin yapılmasını sağlamak için bunlar iç ve dış hizmet sağlayıcıları ile düzenli revize edilmelidir (Tyler 2000, 30–32) .

DS2 Üçüncü Parti Hizmetlerin Yönetilmesi

- DS2.1 Tüm Tedarikçi İlişkilerinin Tanımlanması
- DS2.2 Tedarikçi İlişkisi Yönetimi
- DS2.3 Tedarikçi Risk Yönetimi
- DS2.4 Tedarikçi Performans Gözlemi

DS2.1 Tüm Tedarikçi İlişkilerinin Tanımlanması

Tüm tedarikçi hizmetler tanımlanmalı ve bunlar tedarikçi türü, önem ve kritikliğe göre kategorize edilmelidir. Bu tedarikçilerin temsilcilerinin rollerini ve sorumluluklarını, amaçlarını, beklenen teslimlerini ve onaylarını kapsayan teknik ve kurumsal ilişkilerin resmi dokümantasyonu sağlanmalıdır.

DS2.2 Tedarikçi İlişkisi Yönetimi

Her tedarikçi için tedarikçi ilişkisi yönetim süreci formalize edilmelidir. İlişki sahipleri müşteri ve tedarikçi konuları hakkında irtibat kurmalı ve güven ve şeffaflığa dayanarak (örn. Hizmet düzeyi anlaşmaları) ilişki kalitesi sağlanmalıdır.

DS2.3 Tedarikçi Risk Yönetimi

Sürekli temelde güvenli ve etkin bir tarzda hizmet teslimine devam etmek için tedarikçilerin yeteneği ile ilgili riskler tanımlanmalı ve hafifletilmelidir. Yasal ve mevzuat gerekliliklerine uygun olarak sözleşmelerin evrensel işletme standartlarına uygunluğu sağlanmalıdır. Risk yönetimi aynı zamanda gizli anlaşmalar, emanet sözleşmeler, sürekli tedarikçi finansal kapasitesi, güvenlik gerekleri ile uygunluk, para cezaları ve ödülleri de dikkate alınmalıdır (Tyler 2000, 30–32).

DS2.4 Tedarikçi Performans Gözlemi

Tedarikçinin mevcut iş gerekliliklerini karşılamasını sağlamak ve sözleşme anlaşmalarına ve hizmet düzeyi anlaşmalarına bağlı kalmasını sağlamak ve performansın alternatif tedarikçiler ve Pazar koşulları ile rekabet etmesi için hizmet dağılımını gözleme süreci geliştirilmelidir.

DS3 Performans ve Kapasite Yönetimi

- DS3.1 Performans ve Kapasite Planlama
- DS3.2 Mevcut Kapasite ve Performans
- DS3.3 Gelecekteki Kapasite ve Performans
- DS3.4 IT Kaynakların Mevcudiyeti
- DS3.5 Gözlem Ve Raporlama

DS3.1 Performans ve Kapasite Planlama

Hizmet anlaşmaları tarafından belirlenen şekilde anlaşılan iş yüklerini işleme koymak için düşük maliyetli kapasite ve performansın mevcut olmasını sağlamak amacıyla BT kaynaklarının performans ve kapasite revizyonu için bir planlama süreci oluşturulmalıdır. Kapasite ve performans planları, mevcut ve tahmin edilen performans modeli, kapasitesi üretmek ve BT kaynakları üretimi için uygun model tekniklerini içermelidir.

DS3.2 Mevcut Kapasite ve Performans

Hizmet düzeyindeki anlaşmaların yerine getirilmesi için yeterli kapasite ve performansın var olup olmadığını belirlemek için BT kaynaklarının performans ve kapasitesi revize edilmelidir.

DS3.3 Gelecekteki Kapasite ve Performans

Yetersiz kapasite veya performans degradasyonuna bağlı olarak hizmet bozukluklarının riskini minimuma indirmek için düzenli aralıklarda BT kaynaklarının performans ve kapasite tahminleri yapılmalıdır. Performans ve

kapasite planlarına girdi sağlamak için tahminler belirlenmeli ve iş yükü trendleri tanımlanmalıdır.

DS3.4 BT Kaynakların Mevcudiyeti

Normal iş yükleri, beklenmeyen olaylar, saklama gereklilikleri ve BT kaynağı yaşam devreleri gibi özellikler dikkate alınarak gereken kapasite ve performans sağlanmalıdır. Görev öncelikleri, hata tolerans mekanizmaları ve kaynak tahsis uygulamaları gibi performans ve kapasitenin istenen düzeye ulaşmadığı durumlarda genel hükümler yapılmalıdır. Yönetim beklenmeyen olay planlarının BT kaynaklarının mevcudiyeti, kapasitesi ve performansını uygun şekilde belirtmesini sağlamalıdır.

DS3.5 Gözlem ve Raporlama

BT kaynaklarının performans ve kapasitesinin sürekli gözlenmelidir. Elde edilen veriler iki amaca hizmet etmelidir, s.

- BT içindeki mevcut performansın korunması ve düzenlenmesi ve esneklik, beklenmeyen olaylar, mevcut ve projelendirilmiş iş yükleri, saklama planları ve kaynak edinimi gibi konuların belirtilmesi.
- SLA' lar tarafından gereken şekilde işletmeye sağlanan hizmet mevcudiyetinin rapor edilmesi. Düzeltme eylemleri için önerilerle birlikte tüm istisna raporlarının eklenmesi.

DS4 Sürekli Hizmetin Sağlanması

- DS4.1 IT Süreklilik Çerçevesi
- DS4.2 IT Süreklilik Planları
- DS4.3 Kritik IT Kaynakları
- DS4.4 IT Süreklilik Planının Korunması
- DS4.5 IT Süreklilik Planı Testi
- DS4.6 IT Süreklilik Planı Eğitimi
- DS4.7 IT Süreklilik Planı Dağıtımı

- DS4.8 IT Hizmetlerinin Kurtarılması ve Yeniden Başlatılması
- DS4.9 Alan Dışı Yedekleme Belleği
- DS4.10 Yeniden Başlatma Sonrasında Revizyon

DS4.1 IT Süreklilik Çerçevesi

Sürekli bir süreç ile kurum içinde iş sürekliliği yönetimini desteklemek için, BT sürekliliği, için bir çerçevenin geliştirilmelidir. Çerçevenin amacı, içyapının istenen esnekliğinin belirlenmesine yardımcı olmak ve afet iyileştirme gelişimini ve BT beklenmeyen olay planlarını yönetmek olmalıdır. Çerçeve, süreklilik yönetimi için kurumsal yapıyı belirtmelidir, bu da iç ve dış hizmet sağlayıcılarının rollerini, görevlerini ve sorumluluklarını, bunların yönetimini ve müşterilerini, kuralları ve belge yapılarını, afet iyileştirme test ve yönetimini ve BT beklenmeyen olay planlarını kapsamalıdır. Plan aynı zamanda, kritik kaynakların tanımlanması, kritik kaynakların mevcudiyet gözlemi ve raporları, alternatif süreçler, alternatif işlemler ve yedekleme ve iyileştirme ilkeleri gibi konuları da belirtmelidir (British Standards Institute 2005, ss.750- 780).

DS4.2 BT Süreklilik Planları

Anahtar iş fonksiyonları ve süreçlerdeki temel bozukluğun etkisini azaltmak için tasarlanan çerçeveye dayanan BT süreklilik planları geliştirilmelidir. Planlar esneklik gerekleri, alternatif süreçler ve tüm kritik BT hizmetlerinin iyileştirme kapasitesini belirtmelidir. Bunlar aynı zamanda kullanım kılavuzları, prosedürler, süreçler ve test yaklaşımlarını da kapsamalıdır.

DS4.3 Kritik BT Kaynakları

Esneklik oluşturmak için BT süreklilik planında en önemli olarak belirtilen konular üzerinde odaklanma ve iyileşme durumlarında öncelikler belirlenmelidir. Daha az önemli konuların iyileştirilmesinde dikkatin dağılması önlenmeli ve öncelikli iş ihtiyaçları ile paralel olarak yanıt ve iyileşme sağlanmalı ve maliyetlerin makul bir düzeyde tutulması ve mevzuat ve sözleşme gereklerine uyulması sağlanmalıdır. Farklı bağlayıcılar için esneklik, yanıt ve iyileşme gerekleri dikkate

alınmalıdır, s. Örnek; bir - dört saat, dört - 24 saat, 24 saatten fazla ve kritik iş operasyon periyotları.

DS4.4 BT Süreklilik Planının Korunması

BT yönetimi değişiklik kontrol prosedürlerini tanımlama ve yürütme konusu teşvik edilmelidir ve BT süreklilik planının güncel tutulması ve sürekli olarak fiili iş gerekliliklerinin yansıması sağlanmalıdır. Sorumluluklardaki değişiklikler zamanında bildirilmelidir.

DS4.5 BT Süreklilik Planı Testi

BT süreklilik planı düzenli temelde test edilerek, BT sistemlerinin etkin olarak iyileştirilmesi, kısa yolların belirtilmesi ve planın ilgili kalması sağlanmalıdır. Bu dikkatli hazırlık, dokümantasyon, test sonuçlarının raporlanmasını ve sonuçlara göre, bir eylem planının uygulanmasını gerektirir. Tek uygulama iyileştirmeleri testi entegre test senaryoları ile ve bunlar da sonuç testleri ve entegre satıcı testleri ile karşılaştırılmalıdır.

DS4.6 BT Süreklilik Planı Eğitimi

Bir olay veya afet durumunda prosedürler ve rolleri ve sorumlulukları bakımından tüm ilgili tarafların düzenli eğitim programları alması sağlanmalıdır.

DS4.7 BT Süreklilik Planı Dağıtımı

Gerektiği zaman ve yerde uygun yetkili ilgili taraflara planların uygun ve güvenli dağıtımının ve hazır bulundurulmasının sağlanması için tanımlanan ve yönetilen bir dağıtım stratejisi bulundurulmalıdır. Tüm felaket senaryolarında planlar erişilebilir olmalıdır (British Standards Institute 2005, 750- 780).

DS4.8 BT Hizmetlerinin Kurtarılması ve Yeniden Başlatılması

BT hizmetlerinin geri alınması ve yeniden başlatılması sürecinde uygulanacak eylemler planlanmalıdır. Bunlar arasında yedekleme sitelerinin aktivasyonu, alternatif işlemlerin başlatılması, müşteri ve hissedar iletişimi, yeniden

başlatma prosedürleri olmalıdır. İşin geri alınması ve yeniden başlatılması gereksinimlerini desteklemek için işletmenin BT yeniden başlatma sürelerini ve gereken teknoloji yatırımlarını anlaması sağlanmalıdır.

DS4.9 Alan Dışı Yedekleme Belleği

BT kurtarma ve iş sürekliliği planları için alan dışında tüm kritik yedek medya, dokümantasyon ve diğer BT kaynaklarının saklanması gereklidir. Yedekleme belleğinin içeriği, iş süreci sahipleri ve BT personeli arasında işbirliği ile belirlenmelidir. Alan dışı saklama tesisinin yönetimi veri sınıflandırma politikasına ve kurumun medya depolama uygulamalarına yanıt vermelidir. BT yönetimi, alan dışı düzenlemelerin periyodik olarak, en azından yıllık olarak, içerik, çevresel korunma ve güvenlik bakımından değerlendirilmesini sağlamalıdır. Arşivlenen verilerin restore edilmesi için donanım ve yazılım uyumu sağlanmalı ve arşivlenen veriler periyodik olarak test edilmeli ve yenilenmelidir.

DS4.10 Yeniden Başlatma Sonrasında Revizyon

Bir felaketten sonra BT fonksiyonunun başarılı yeniden başlatılması için, BT yönetiminin plan uygunluğunu değerlendirmek için belirli prosedürleri olup olmadığı belirlenmeli ve buna göre plan güncellenmelidir.

DS5 Sistem Güvenliğinin Sağlanması

- DS5.1 IT Güvenliği Yönetimi
- DS5.2 IT Güvenlik Planı
- DS5.3 Kimlik Yönetimi
- DS5.4 Kullanıcı Hesabı Yönetimi
- DS5.5 Güvenlik Testi, Gözetim ve Gözlem
- DS5.6 Güvenlik Olay Tanımı
- DS5.7 Güvenlik Teknolojisinin Korunması
- DS5.8 Kriptografik Anahtar Yönetimi
- DS5.9 Zararlı Yazılım Korunması, Tespiti ve Düzeltilmesi
- DS5.10 Ağ Güvenliği

- DS5.11 Hassas Verilerin Değişimi

DS5.1 BT Güvenliği Yönetimi

BT güvenliği uygun olan en yüksek kurumsal düzeyde yönetilmelidir ve güvenlik eylemleri yönetiminin iş gereklilikleri ile paralel olması sağlanmalıdır.

DS5.2 BT Güvenlik Planı

İş enformasyon gerekleri, BT konfigürasyonu, enformasyon riski eylem planları ve enformasyon güvenlik kültürü toplam BT güvenlik planına çevrilmelidir. Plan, hizmetler, personel, yazılım ve donanımda uygun yatırımlar ile birlikte güvenlik politikaları ve prosedürlerinde uygulanmalıdır. Güvenlik politikaları ve prosedürleri hissedarlara ve kullanıcılara bildirilmelidir (British Standards Institute, 2005, 750- 780).

DS5.3 Kimlik Yönetimi

Tüm kullanıcılar (iç, dış ve geçici) ve onların BT sistemlerindeki etkinlikleri (iş uygulaması, sistem operasyonu, geliştirme ve bakım) ayrı ayrı tanımlanabilir olmalıdır. Sistem ve verilere kullanıcı erişim hakları belli ve belgeli işletme gereksinimleri ve iş gereklilikleri ile paralel olmalıdır. Kullanıcı erişim hakları kullanıcı yönetimi tarafından talep edilmelidir, sistem sahibi tarafından onaylanmalıdır ve güvenlik sorumlusu tarafından uygulanmalıdır. Kullanıcı kimlikleri ve erişim hakları merkez havuzda saklanmalıdır. Maliyet-etkili teknik ve prosedür önlemleri açıklanmalıdır ve kullanıcı tanımı belirlenmelidir, onay uygulaması ve erişim haklarının güçlendirilmesi için yürürlükte tutulmalıdır (Tyler, 2000, 30–32) .

DS5.4 Kullanıcı Hesabı Yönetimi

Kullanıcı hesaplarının talep edilmesi, oluşturulması, çıkarılması, askıya alınması, modifiye edilmesi ve kapatılmasının kullanıcı hesabı yönetimi tarafından belirlenmesi sağlanmalıdır. Erişim ayrıcalıkları sağlayan veri veya sistem sahibini belirten onay prosedürü de dahil edilmelidir. Bu prosedürler, yöneticiler (ayrıcalıklı

kullanıcılar), iç ve dış kullanıcılar, dahil olmak üzere tüm kullanıcılar için ve normal ve acil durumlar için uygulanmalıdır. Girişim sistemleri ve bilgiye erişim için ilgili haklar ve zorunluluklar tüm kullanıcı tipleri için sözleşmelerle düzenlenmelidir. Tüm hesaplar ve ilgili ayrıcalıkların düzenli yönetim revizyonu gerçekleştirilmelidir (The IT Governance Institute 2007, 156).

DS5.5 Güvenlik Testi, Gözetim ve Gözlem

BT güvenlik uygulamasının proaktif olarak test edilmesi ve gözlenmesi sağlanmalıdır. Onaylanan güvenlik düzeyinin sağlanması için BT güvenliği periyodik olarak yeniden akredite edilmelidir. Bir kayıt ve gözlem fonksiyonu belirlenmesi gereken olağan dışı veya anormal etkinliklerin erken tespiti sağlanmalıdır. Kayıt bilgilerine erişim, erişim hakları ve elde tutma gereklilikleri bakımından işletme gereklilikleri ile paralel olmalıdır (J. Lainhart, 2001, 191–193).

DS5.6 Güvenlik Olay Tanımı

Potansiyel güvenlik olayları özelliklerinin açık olarak tanımlanması ve bildirilmesi sağlanmalıdır. Bu şekilde güvenlik olayları olay veya sorun yönetimi süreci tarafından uygun şekilde yönetilmelidir. Özellikler arasına güvenlik olayı ve etki derecesi olarak düşünülen şeylerin tanımı konmalıdır (British Standards Institute, 2005, 750- 780). . Etki düzeylerinin sınırlı sayısı belirlenmelidir ve gereken her özel eylem için ve belirtilmesi gereken kişiler için tanımlanmalıdır.

DS5.7 Güvenlik Teknolojisinin Korunması

Önemli güvenlik teknolojisinin tehditlere karşı dirençli olması sağlanmalıdır ve güvenlik belgeleri gereksiz şekilde açıklanmamalıdır, örn. Düşük bir profile sahiptir. Ancak, sistemlerin güvenliğinin güvenlik spesifikasyonlarının gizliliğine bağlı olmaması sağlanmalıdır.

DS5.8 Kriptografik Anahtar Yönetimi

Modifikasyon ve yetkisiz açılmalara karşı anahtarların korunmasını sağlamak için kriptografik anahtarların yaratılmasının, değiştirilmesinin, iptalinin, bozulmasının, dağıtımının, sertifikasyonunun, saklanmasının, girişinin, kullanımının ve arşivlenmesinin düzenlenmesi için politika ve prosedürler yerinde olmalıdır (The IT Governance Institute, 2007, 156)..

DS5.9 Zararlı Yazılım Korunması, Tespiti ve Düzeltilmesi

Bilgi sistemlerinin ve teknolojisinin zararlı yazılımlardan korunması için (virüsler, solucanlar, casus yazılımlar, spam, içsel olarak geliştirilen tahrip edici yazılımlar, vb) koruyucu, tespit edici ve düzeltici önlemlerin yerinde olması sağlanmalıdır (özellikle güncel güvenlik yolları ve virüs kontrolü).

DS5.10 Ağ Güvenliği

Güvenlik teknikleri ve ilgili yönetim prosedürlerinin (örn. Ateş duvarları, güvenlik uygulamaları, ağ segmentasyonu ve işgal tespiti) ağdan ağa bilgi akışını kontrol etmek ve erişimi yetkilendirmek için kullanılması sağlanmalıdır.

DS5.11 Hassas Verilerin Değişimi

Hassas işlem verilerinin içerik uyumu, sunum kanıtı, belge kanıtı ve kökenin reddedilmemesini sağlamak için sadece güvenli bir yoldan veya kontrollü olarak değişimi sağlanmalıdır.

DS6 Maliyetlerin Tanımlanması ve Dağıtımı

DS6.1 Hizmetlerin Tanımı

DS6.2 IT Muhasebesi

DS6.3 Maliyet Modelleri ve tarifeler

DS6.4 Maliyet Modeli Bakımı

DS6.1 Hizmetlerin Tanımı

Şeffaf bir maliyet modelini desteklemek için tüm BT maliyetler tanımlanmalıdır ve bunlar BT hizmetlerine bildirilmelidir. BT hizmetleri işletme

süreçlerine bağlanmalıdır ve işletme ilgili hizmet fiyatlandırma düzeyleri tanımlanmalıdır.

DS6.2 BT Muhasebesi

Tanımlanan maliyet modeline göre fiili maliyetler tanımlanmalıdır ve dağıtılmalıdır. Tahminler ve fiili maliyetler arasındaki farklılıklar işletmenin finansal ölçme sistemlerine uygun olarak analiz edilmelidir ve raporlanmalıdır (The IT Governance Institute, 2007, 156).

DS6.3 Maliyet Modelleri ve Tarifeler

Hizmet tanımına dayanarak, hizmetlerin direkt, endirekt ve toplam maliyetlerini içeren bir maliyet modeli tanımlanmalıdır ve her hizmet için geri tarife oranlarının hesaplanması desteklenmelidir. Maliyet modeli işletmenin maliyet muhasebesi prosedürleri ile paralel olmalıdır. BT maliyet modeli hizmet tarifelerinin tanımlanabilir, ölçülebilir ve kaynakların uygun kullanımını teşvik etmek için kullanıcılar tarafından öngörülebilir olmasını sağlamalıdır. Kullanıcı yönetimi hizmetlerin fiili kullanımını ve hizmetlerin tarifesini doğrulamalıdır (British Standards Institute, 2005, 750- 780).

DS6.4 Maliyet Modeli Bakımı

Maliyet/tarife modelinin uygunluğu düzenli olarak revize edilmelidir, işaretlenmelidir ve gelişen işletme ve BT etkinliklerine uygunluğu ve ilgisi korunmalıdır.

DS7 Kullanıcıların Eğitimi ve Öğretimi

DS7.1 Eğitim ve Öğretim Gereksinimlerinin Tanımlanması
DS7.2 Eğitim ve Öğretimin Verilmesi
DS7.3 Alınan Eğitimin Değerlendirilmesi

DS7.1 Eğitim ve Öğretim Gereksinimlerinin Tanımlanması

Her çalışan hedef grubu için bir öğretim programı oluşturulmalıdır, düzenli olarak güncellenmelidir ve aşağıdaki konular dikkate alınmalıdır (British Standards Institute, 2005, 750- 780).

- Mevcut ve gelecekteki iş gerekleri ve stratejisi
- Kurumsal değerler (etik değerler, kontrol ve güvenlik kültürü, vb.)
- Mevcut beceriler, yetkinlik profilleri ve sertifikasyon ve/veya resmi onay gereksinimleri
- Teslim metotları (örn. Sınıf, web tabanlı), hedef grup boyutu, erişilebilirlik ve zamanlama

DS7.2 Eğitim ve Öğretimin Verilmesi

Tanımlanan eğitim ve öğretim gereksinimlerine dayanarak, hedef gruplar ve üyeleri, etkin teslim mekanizmaları, öğretmenler, belletmenler ve danışmanlar tanımlanmalıdır. Süreli temelde öğretmenler atanmalı ve eğitim programları düzenlenmelidir. Kayıtlar (ön gerekler dahil), devamlılık ve performans değerlendirmeleri kaydedilmelidir(Herr D., 2006, 410).

DS7.3 Alınan Eğitimin Değerlendirilmesi

Eğitim ve öğretim içeriği tamamlanmasından sonra ilgi, kalite, etkinlik, bilginin yakalanması ve tutulması, maliyet ve değer bakımından değerlendirilmelidir. Bu değerlendirme sonuçları gelecekteki müfredat programı tanımı ve eğitim programları için bir girdi olarak alınmalıdır.

DS8 Hizmet Masası ve Olaylar Yönetimi

- DS8.1 Hizmet Masası
- DS8.2 Müşteri Anketlerinin Kaydı
- DS8.3 Olay Yükseltilmesi
- DS8.4 Olay Kapatma
- DS8.5 Trend Analizi

DS8.1 Hizmet Masası

BT ile kullanıcı ara yüzü olarak, tüm çağrıları, kayıtlı olayları, hizmet taleplerini ve bilgi taleplerini kaydetmek, iletmek, dağıtmak ve analiz etmek için bir hizmet masası fonksiyonu oluşturulmalıdır. Bir olay, hizmet talebi veya bilgi talebi

olarak kaydedilen herhangi bir konunun sınıflandırmasını ve önceliğini sağlayan uygun SLA ile ilgili anlaşma sağlanan hizmet düzeylerine dayanan gözlem ve yükselme prosedürleri bulundurulmalıdır. Hizmet masası kalitesi ve BT hizmetleri ile son kullanıcı memnuniyeti ölçülmelidir (Herr 2006, 410).

DS8.2 Müşteri Anketlerinin Kaydı

Çağrıların, olayların, hizmet taleplerinin ve bilgi gereksinimlerinin kaydı ve izlenmesini sağlayan bir fonksiyon ve sistem oluşturulmalıdır. Olay yönetimi, problem yönetimi, değişiklik yönetimi, kapasite yönetimi ve mevcudiyet yönetimi gibi süreçlerle birlikte çalıştırılmalıdır. Olaylar iş ve hizmet önceliklerine göre sınıflandırılmalıdır ve uygun sorun yönetimi ekibine göre yönlendirilmelidir ve müşteriler anket durumu hakkında bilgilendirilmelidir.

DS8.3 Olay Yükseltilmesi

Hizmet masası prosedürleri oluşturulmalıdır, bu şekilde hemen çözülemeyen olaylar SLA' da tanımlanan sınırlara göre uygun şekilde yükseltilmelidir ve varsa, iş çevreleri sağlanmalıdır. Olay sahipliği ve yaşam devri gözleminin BT grubunun çözüm etkinlikleri hakkında çalışmasından bağımsız olarak kullanıcıya dayanan olaylar için hizmet masasında kalması sağlanmalıdır (The IT Governance Institute, 2007, 156).

DS8.4 Olay Kapatma

Müşteri anketlerinin açıklanmasının zamanında gözlenmesi için prosedürleri oluşturulmalıdır. Olay çözüldüğünde, köken nedeni biliniyorsa hizmet masası tarafından kaydedilmelidir ve uygulanan eylem müşteri tarafından onaylanmalıdır.

DS8.5 Trend Analizi

Hizmet performansını ve hizmet yanıt sürelerini ölçmek için ve trendleri ve tekrarlayan sorunları tanımlamak için yönetimi sağlamak üzere hizmet masası raporları üretilmelidir ve hizmet sürekli olarak geliştirilmelidir.

DS9 Konfigürasyon Yönetimi

- DS9.1 Konfigürasyon Havuzu ve Dayanak

- DS9.2 Konfigürasyon Maddelerinin Tanımlanması ve Korunması
- DS9.3 Konfigürasyon Entegrite Revizyonu

DS9.1 Konfigürasyon Havuzu ve Dayanak

Konfigürasyon maddeleri hakkında tüm ilgili bilgiyi içeren merkezi bir havuz oluşturulmalıdır. Bu havuzda donanım, uygulama yazılımı, orta yazılım, parametreler, dokümantasyon, prosedürler ve işletme araçları, sistemlerin ve hizmetlerin erişimi ve kullanımı bulundurulmalıdır. Dikkate alınacak ilgili bilgiler, isimlendirme, versiyon numaraları ve lisans detaylandırılmalıdır (Herr 2006, 410).. Her sistem ve hizmet için değişikliklerden sonra dönülecek bir kontrol noktası olarak konfigürasyon maddelerinin dayanağı korunmalıdır (The IT Governance Institute, 2007, 156)..

DS9.2 Konfigürasyon Birimleri Tanımlanması ve Korunması

Aşağıdakiler için prosedürler uygulanmalıdır (Herr 2006, 410).:

- Konfigürasyon birimleri ve özellikleri tanımlanmalıdır
- Yeni, modifiye edilmiş ve silinmiş konfigürasyon maddeleri kaydedilmelidir.
- Konfigürasyon havuzunda konfigürasyon birimleri arasında ilişkiler tanımlanmalıdır ve korunmalıdır
- Konfigürasyon havuzundaki mevcut konfigürasyon maddeleri güncellenmelidir
- Yetkisiz yazılım kullanılması önlenmelidir
- Bu prosedürler konfigürasyon havuzundaki tüm eylemlerin uygun yetkilendirilmesini ve kayıtlarını sağlamalıdır ve değişiklik yönetimi ve sorun yönetimi prosedürleri ile uygun şekilde entegre edilmelidir.

DS9.3 Konfigürasyon Entegrite Revizyonu

Gerektiğinde, düzenli temelde, mevcut ve geçmişteki konfigürasyon verilerinin bütünlüğünün doğrulanması ve fiili durumlara karşı karşılaştırılması için uygun araçlar kullanılarak konfigürasyon maddelerinin statüsü revize edilmelidir ve doğrulanmalıdır. Mevcut lisans anlaşmalarının dışında herhangi bir yazılım veya lisanssız yazılım kullanılmasına karşı yazılım kullanımı politikaları periyodik olarak

revize edilmelidir. Hatalar ve sapmalar rapor edilmelidir, müdahale edilmelidir ve düzeltilmelidir (The IT Governance Institute, 2007, 156).

DS10 Sorun Yönetimi

DS10.1 Sorunların Tanımlanması ve Sınıflandırılması

DS10.2 Sorun İzleme Ve Çözüm

DS10.3 Sorun Kapatma

DS10.4 Değişiklik, Konfigürasyon ve Sorun Yönetimi Entegrasyonu

DS10.1 Sorunların Tanımlanması ve Sınıflandırılması

Olay yönetiminin parçası olarak tanımlanan sorunlar rapor edilmelidir ve sınıflandırılması için süreçler uygulanmalıdır. Sorun sınıflandırmada yer alan adımlar olay sınıflandırma adımları ile benzerdir; bunlar, kategori, etki, aciliyet ve önceliklerin belirlenmesidir. Sorunlar ilgili gruplar veya bölgelere uygun olarak kategorize edilmelidir (örn. Donanım, yazılım, destek yazılımı). Bu gruplar kurumsal sorumlulukları veya kullanıcı ve müşteri temelini birleştirir ve kadroyu desteklemek için sorunların tahsisinde temeldir (Herr 2006, 410).

DS10.2 Sorun İzleme Ve Çözüm

Sorun yönetimi sistemi, kaydedilen tüm sorunların köken nedenini izlemeyi, analizini ve belirlenmesini sağlayan uygun denetim raporu kolaylıkları sağlamalıdır ve şunları dikkate almalıdır:

- Tüm ilgili konfigürasyon birimleri
- Var olan sorunlar ve olayları
- Bilinen ve kuşku duyulan hataları

Belirlenen değişiklik yönetimi süreci üzerinden değişiklik talebi doğuran kök nedeni bildiren sürdürülebilir çözümler tanımlanmalıdır ve başlatılmalıdır. Çözüm süreci boyunca, sorun yönetimi, sorun ve hataların çözümünde var olan değişiklik yönetiminden düzenli raporlar alınmalıdır. Sorun çözümü sorunların devam eden etkilerini ve kullanıcı hizmetlerindeki bilinen hatalar gözlenmelidir. Bu etkinin şiddetli olması durumunda, sorun yönetimi sorunu yükseltilmelidir ve değişiklik

talebi önceliğini arttırmak için yönetim kuruluna bildirilmelidir ve uygun acil değişiklik uygulanmalıdır. Sorun çözüm gelişimi SLA 'lere karşı gözlenmelidir (The IT Governance Institute, 2007, 156).

DS10.3 Sorun Kapatma

Bilinen hatanın başarılı eliminasyonunun onayından sonra veya alternatif çözüm yollarının işletme ile belirlenmesinden sonra sorun kayıtlarını kapatmak için bir prosedür uygulanır.

DS10.4 Değişiklik, Konfigürasyon ve Sorun Yönetimi Entegrasyonu

Etkin sorun ve olay yönetimini sağlamak için, ilgili değişiklik süreçleri, konfigürasyon ve sorun yönetimi entegrasyonu uygulanmalıdır. İş gelişmesinin sağlanması yerine problemi, sorunu çözmek için ne kadar çaba gösterildiği ve gerekirse sorunları minimuma indirmek için ne yapılması gerektiği gözlenmelidir(The IT Governance Institute 2007, 156) .

DS11 Veri Yönetimi

DS11.1 Veri Yönetimi için İşletme Gereklilikleri
DS11.2 Saklama ve Elde Tutma Düzenlemeleri
DS11.3 Medya Kütüphane Yönetimi Sistemi
DS11.4 Elden Çıkarma
DS11.5 Yedekleme ve Restorasyon
DS11.6 Veri Yönetimi için Güvenlik Gereklilikleri

DS11.1 Veri Yönetimi için İşletme Gereklilikleri

İşletmeden beklenen kaynak belgelerin teslim alınmasını sağlamak için düzenlemeler yapılmalıdır, işletmeden alınan tüm veriler işleme konulmalıdır, işletmenin gerektirdiği tüm çıktı hazırlanmalıdır ve teslim edilmelidir ve yeniden başlatma ve yeniden süreçlendirme gereksinimleri desteklenmelidir.

DS11.2 Saklama ve Elde Tutma Düzenlemeleri

Veri saklama ve arşivleme için prosedürler tanımlanmalıdır ve uygulanmalıdır, bu şekilde veriler erişilebilir ve kullanışlı kalacaktır. Prosedürler yeniden kullanma gerekleri, maliyet etkinliği, sürekli entegre ve güvenlik gereklerini dikkate almalıdır. Kodlama ve onay için kullanılan veriler (anahtarlar, sertifikalar) gibi belgeler, veriler, arşivler, programlar, raporlar ve mesajlar (gelen ve giden) için yasal, mevzuat ve iş gereklerini karşılamak amacıyla saklama ve elde tutma düzenlemeleri yapılmalıdır (The IT Governance Institute, 2007, 156).

DS11.3 Medya Kütüphane Yönetimi Sistemi

On site medya envanterinin sağlanması için prosedürler tanımlanmalıdır ve uygulanmalıdır ve kullanışlılıkları ve entegresi sağlanmalıdır. Prosedürler uyuşmazlıklar hakkında zamanında revizyon ve takip sağlamalıdır.

DS11.4 Elden Çıkarma

Bir başka kullanıma aktarılacağı veya elden çıkarılacağı zaman ekipman ve medyadan hassas verilere ve yazılıma erişimi önlemek için prosedürler tanımlanmalıdır ve uygulanmalıdır. Bu prosedürler silinen veya atılan verilerin tekrar kullanılamayacağını sağlamalıdır.

DS11.5 Yedekleme ve Restorasyon

İş gerekleri ve süreklilik planı ile paralel olarak sistemlerin yedekleme ve restorasyonu, veri ve dokümantasyonu için prosedürler tanımlanmalıdır ve uygulanmalıdır. Yedekleme prosedürleri ile uygunluğu doğrulanmalıdır ve başarılı ve tam yenileme için yetenek ve zaman doğrulanmalıdır. Yedekleme medyası ve restorasyon süreci test edilmelidir.

DS11.6 Veri Yönetimi için Güvenlik Gereklilikleri

Makbuz, süreç, fiziksel depolama ve verilere ve hassas mesajlara uygulanan güvenlik gerekleri tanımlanmalıdır ve uygulanması için düzenlemeler yapılmalıdır.

Bunlar fiziksel kayıtları, veri aktarımlarını ve site dışında saklanan verileri içermelidir.

DS12 Fiziksel Ortamların Yönetimi

DS12.1 Site Seçimi ve Planı

DS12.2 Fiziksel Güvenlik Önlemleri

DS12.3 Fiziksel Erişim

DS12.4 Çevresel Faktörlere Karşı Koruma

DS12.5 Fiziksel Tesis Yönetimi

DS12.1 Site Seçimi ve Planı

İş stratejisine bağlı olan teknoloji stratejisini desteklemek için BT ekipmanı için fiziksel siteler tanımlanmalıdır ve seçilmelidir. Bir site planının seçimi ve tasarımı, meslek sağlığı ve güvenlik mevzuatı gibi ilgili yasalar ve düzenlemeler ile birlikte doğal insan kaynaklı felaketlerle ilgili riski de dikkate almalıdır.

DS12.2 Fiziksel Güvenlik Önlemleri

İş gerekleri ile paralel olarak fiziksel güvenlik önlemleri tanımlanmalıdır ve uygulanmalıdır. Önlemler şunları içermelidir, ancak bunlarla sınırlı kalmamalıdır, s. Güvenlik parametresi planı, güvenlik bölgeleri, kritik ekipmanın lokasyonu, ve sevkiyat ve teslim alanları. Özellikle, kritik ve önem arz eden Bilgi Teknolojileri operasyonlarının varlığı hakkında düşük bir profil tutulmalıdır. Gözlem sorumlulukları ve rapor prosedürleri ve fiziksel güvenlik olaylarının çözümü belirlenmelidir (Heschl 2006, 157 – 168).

DS12.3 Fiziksel Erişim

Acil durumlar da dahil olmak üzere iş gereklerine göre arazilere, bina ve alanlara erişim verilmelidir, sınırlanması ve feshedilmesi için prosedürler tanımlanmalıdır ve uygulanmalıdır. Arazi, bina ve alan erişimleri değerlendirilmelidir, yetkilendirilmelidir, kaydedilmelidir ve gözlenmelidir. Bu, kadro, geçici kadro, müşteriler, satıcılar, ziyaretçiler veya diğer üçüncü taraflar dahil olmak üzere, arazilere giren tüm kişilere uygulanmalıdır.

DS12.4 Çevresel Faktörlere Karşı Koruma

Çevresel faktörlere karşı korunma için önlemler tasarlanmalıdır ve uygulanmalıdır. Çevre gözlemi ve kontrolü için uzmanlaşmış ekipman ve cihazlar kurulmalıdır.

DS12.5 Fiziksel Tesis Yönetimi

Yasa ve mevzuat, teknik ve iş gerekleri, satıcı spesifikasyonları ve sağlık ve güvenlik kılavuzları ile paralel olarak güç ve iletişim ekipmanı dahil, tesisler yönetilmelidir.

DS13 Operasyonların Yönetimi

DS13.1 Operasyonlar Prosedürleri ve Talimatları
DS13.2 İş Cetvelleri
DS13.3 IT İç Yapı Gözlemi
DS13.4 Hassas Belgeler ve Çıktı Cihazları
DS13.5 Donanım için Koruyucu Bakım

DS13.1 Operasyonlar Prosedürleri ve Talimatları

BT operasyonları için standart prosedürler tanımlanmalıdır, uygulanmalıdır ve korunması ve operasyon kadrosunun onlara verilen tüm operasyon görevleri hakkında bilgi sahibi olması sağlanmalıdır. Operasyonel prosedürler sürekli operasyonu sağlamak için vardiya devir teslimini kapsamalıdır (Heschl 2006, 157 – 168).

DS13.2 İş Cetvelleri

İş gereklerini karşılamak için iş cetvelleri, süreçleri ve görevler en etkin sıraya göre düzenlenmelidir, üretim ve kullanışlılık maksimuma çıkarılmalıdır. Bu cetvel değişiklikleri ile birlikte ilk cetveller yetkilendirilmelidir. Standart iş

cetvellerinden hareketleri tanımlamak, araştırmak ve onaylamak için prosedürler uygulanmalıdır.

DS13.3 BT Alt Yapı Gözlemi

BT alt yapısı ve ilgili olayları gözlemlemek için prosedürler tanımlanmalıdır ve uygulanmalıdır. Yeterli kronolojik bilginin operasyonlar kaydında saklanması sağlanmalıdır. Bu şekilde operasyonların zaman dizilerinin rekonstrüksiyonu, revizyonu ve değerlendirmesi ve operasyonları çevreleyen veya destekleyen diğer aktiviteler mümkün kılınır (Heschl 2006, 157 – 168).

DS13.4 Hassas Belgeler ve Çıktı Cihazları

Özel formlar, görüşülen enstrümanlar, özel amaçlı yazıcılar veya güvenlik jetonları gibi hassas BT aktifleri üzerinde envanter yönetimi ve muhasebe uygulamaları ve uygun fiziksel güvenlik sağlanmalıdır.

DS13.5 Donanım için Koruyucu Bakım

Başarısızlık etkisi ve sıklığını veya performans düşüklüğünü azaltmak için içyapının zamanında korunmasını sağlamak amacıyla prosedürler tanımlanmalıdır ve uygulanmalıdır.

2.4.Gözlem ve Değerlendirme

Gözlem ve Değerlendirme alanı kurumun ihtiyaçlarını, mevcut BT sisteminin hedefleri karşılayıp karşılamadığını ve yasal gereksinimlerle uyumluluk için gerekli kontrolü tayin etmek için kurumun stratejilerini irdelemektedir. Gözlem ve Değerlendirme aynı zamanda bilgi teknolojileri sisteminin iş hedeflerini karşılamadaki etkinliği ile iç ve dış denetçilerce yapılan kurumun kontrol süreçlerinin bağımsız değerlendirmesi konularını kapsamaktadır.

Gözlem ve Değerlendirme alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır (Heschl 2006, 157 – 168):

ME1 IT Performansının Gözlemi ve Değerlendirmesi

ME2 İç Kontrol Gözlemi ve Değerlendirmesi

ME3 Yönetmeliklere Uyumluluğun Sağlanması

ME4 BT Yönetimi Sağlanması

ME1 IT Performansının Gözlemi ve Değerlendirmesi

ME1.1 Gözlem Yaklaşımı

ME1.2 Gözlem Verilerinin Tanımı ve Toplanması

ME1.3 Gözlem Metodu

ME1.4 Performans Değerlendirmesi

ME1.5 Yönetim Kadrosu ve Yönetici Raporlama

ME1.6 Çözüm Eylemleri

ME2 İç Kontrol Gözlemi ve Değerlendirmesi

ME2.1 İç Kontrol Çerçevesinin Gözlenmesi

ME2.2 Denetim Revizyonu

ME2.3 Kontrol İstisnaları

ME2.4 Kontrol Öz-değerlendirme

ME2.5 İç Kontrol Güvencesi

ME2.6 Üçüncü Taraflarda İç Kontrol

ME2.7 Çözüm Eylemleri

ME3 Yönetmeliklere Uyumluluğun Sağlanması

ME3.1 BT üzerinde Potansiyel Etkisi Olan Yasa ve Yönetmeliklerin Tanımlanması

ME3.2 Yönetmelik Koşullarının Karşılanmasında Optimizasyonun Sağlanması

ME3.3 Yönetmelik Koşullarıyla Uyumluluğun Değerlendirilmesi

ME3.4 Uyumluluğun Olumlu Biçimde Sağlanması

ME3.5 Tümleşik Raporlama

ME4 BT Yönetimi Sağlanması

ME4.1 BT Yönetimi Çerçevesinin Oluşturulması

ME4.2 Stratejik Uyum

ME4.3 Değer Yaratma

ME4.4 kaynak Yönetimi

ME4.5 Risk Yönetimi

ME4.6 Performans Ölçümü

ME4.7 Bağımsız Denetim/Güvence (ITGI, 2007) Gözlem ve Değerlendirme

Gözlem ve Değerlendirme alanı kurumun ihtiyaçlarını, mevcut BT sisteminin hedefleri karşılayıp karşılamadığını ve yasal gereksinimlerle uyumluluk için gerekli

kontrolü tayin etmek için kurumun stratejilerini irdelemektedir. Gözlem ve Değerlendirme aynı zamanda bilgi teknolojileri sisteminin iş hedeflerini karşılamadaki etkinliği ile iç ve dış denetçilerce yapılan kurumun kontrol süreçlerinin bağımsız değerlendirmesi konularını kapsamaktadır.

Gözlem ve Değerlendirme alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır (Heschl 2006, 157 – 168):

ME1 IT Performansının Gözlemi ve Değerlendirmesi

ME2 İç Kontrol Gözlemi ve Değerlendirmesi

ME3 Yönetmeliklere Uyumluluğun Sağlanması

ME4 BT Yönetimi Sağlanması

ME1 IT Performansının Gözlemi ve Değerlendirmesi

ME1.1 Gözlem Yaklaşımı

ME1.2 Gözlem Verilerinin Tanımı ve Toplanması

ME1.3 Gözlem Metodu

ME1.4 Performans Değerlendirmesi

ME1.5 Yönetim Kadrosu ve Yönetici Raporlama

ME1.6 Çözüm Eylemleri

ME1.1 Gözlem Yaklaşımı

Yönetim, işletmenin portfolio yönetimi sonuçlarına ve program yönetimi süreçlerine ve Bilgi Teknolojileri kapasitesi ve hizmetlerinin teslimine özel süreçlere BT katkısının gözlenmesi için izlenecek kapsamı, metodolojiyi ve süreci tanımlayan genel bir gözlem çerçevesi ve yaklaşımı oluşturmalıdır. Çerçeve kurumsal performans yönetimi sistemi ile entegre edilmelidir.

ME1.2 Gözlem Verilerinin Tanımı ve Toplanması

İşletme ile çalışan Bilgi Teknolojileri yönetimi performans amaçları, önlemleri, hedefleri ve vurgularının dengeli bir setini tanımlamalıdır ve bunların işletme ve ilgili hissedarlar tarafından imzalanarak onaylanmasını sağlamalıdır. Performans göstergeleri şunları içermelidir (Heschl 2006, 159):

İşletme katkısı finansalları içeren ancak bunlarla sınırlı olmayan Stratejik iş ve BT planına karşı performans, Mevzuat ile uyum ve risk, İç ve dış kullanıcı tatmini,

Gelişme ve hizmet teslimini içeren anahtar BT süreçleri, Geleceğe yönelik aktiviteler, örneğin, var olan teknoloji, tekrar kullanılabilen içyapı, iş ve BT personeli beceri setleri. Hedef gelişmeleri hakkında raporlar için zamanında ve doğru verilerin toplanması amacıyla süreçler geliştirilmelidir.

ME1.3 Gözlem Metodu

Gözlem sürecinin kısa ve kapsamlı Bilgi Teknolojileri performansı gözlemi sağlayan bir metot açıklaması sağlanmalıdır (örn. Dengeli puan kartı) ve bu işletme gözlem sistemi ile uygun olmalıdır.

ME1.4 Performans Değerlendirmesi

Periyodik olarak performans hedeflere karşı revize edilmelidir, köken neden analizi yapılmalıdır ve altta yatan nedenlerin belirlenmesi için çözüm eylemi başlatılmalıdır.

ME1.5 Yönetim Kadrosu ve Yönetici Raporlama

Kurum gelişmesi hakkında yüksek yönetim revizyonu için yönetim raporları sağlanmalıdır. Bu raporlarda tanımlanan amaçlar, özellikle BT yatırım programlarının işletme portfolyosu performansı ve bireysel programların hizmet düzeyleri ve BT katkısı belirtilmelidir. Statü raporları planlanan amaçların gerçekleştirilme derecesini, alınan teslimleri, karşılanan performans hedeflerini ve hafifletilen riskleri içermelidir. Revizyon üzerine, beklenen performanstan sapmalar tanımlanmalıdır ve uygun yönetim eylemi başlatılmalıdır ve rapor edilmelidir (www.itgi.org, Erişim:18/08/2014).

ME1.6 Çözüm Eylemleri

Performans gözlemi, değerlendirme ve raporlamaya dayanarak çözüm eylemleri tanımlanmalıdır ve başlatılmalıdır. Bu, tüm gözlem, raporlama ve değerlendirmelerin takibini içermelidir:
Yönetim yanıtlarının revizyonu, müzakereleri ve oluşturulması

Çözüm için sorumluluk atamaları
Taahhüt edilen eylemlerin sonuçlarının izlenmesi

ME2 İç Kontrol Gözlemi ve Değerlendirmesi

ME2.1 İç Kontrol Çerçevesinin Gözlenmesi
ME2.2 Denetim Revizyonu
ME2.3 Kontrol İstisnaları
ME2.4 Kontrol Öz-değerlendirme
ME2.5 İç Kontrol Güvencesi
ME2.6 Üçüncü Taraflarda İç Kontrol
ME2.7 Çözüm Eylemleri

ME2.1 İç Kontrol Çerçevesinin Gözlenmesi

BT kontrol ortamı sürekli olarak gözlenmelidir ve çerçeve kontrol edilmelidir. BT kontrol ortamı ve kontrol çerçevesini geliştirmek için en iyi endüstri uygulamaları ve işaretlerinin kullanılarak değerlendirme yapılmalıdır (Uzunay 2007, 185).

ME2.2 Denetim Revizyonu

Denetim revizyonu ile BT üzerindeki iç kontrollerin etkinliği gözlenmelidir ve rapor edilmelidir: Örnek; politika ve standartlarla uygunluk, enformasyon güvenliği, kontrollerin değiştirilmesi ve hizmet düzeyi anlaşmalarında belirlenen kontroller.

ME2.3 Kontrol İstisnaları

Tüm kontrol istisnaları bakımından bilgiler kaydedilmelidir ve altta yatan neden analiz edilmelidir ve düzeltici eylem uygulanmalıdır. Fonksiyon için bireysel sorumluya iletilecek istisnalara yönetim karar vermelidir. Yönetim etkilenen tarafların bilgilendirilmesinden de sorumlu olmalıdır.

ME2.4 Kontrol Öz-değerlendirme

Sürekli bir kendi kendini değerlendirme programı ile BT süreçleri, politikaları ve sözleşmeleri üzerindeki yönetimin iç kontrollerinin bütünlüğü ve etkinliği değerlendirilmelidir.

ME2.5 İç Kontrol Güvencesi

Gereken şekilde üçüncü taraf revizyonları ile iç kontrollerin tamlık ve etkinliğinin güvencesi alınmalıdır. Bu revizyonlar kurumsal uygunluk fonksiyonu ile yönetilmelidir veya yönetim talebi üzerine yapılmalıdır, iç denetim veya komisyonlu dış denetimciler ve danışmanlar veya sertifikasyon grupları tarafından yapılmalıdır. Denetimi yapan bireylerin kalifikasyonları sağlanmalıdır(www.itgi.org, Erişim:18/08/2014).

ME2.6 Üçüncü Taraflarda İç Kontrol

Her dış hizmet sağlayıcının iç kontrol statüsü değerlendirilmelidir. Dış hizmet sağlayıcıları yasal ve mevzuat gerekleri ve sözleşme zorunlulukları ile uyumlu davranmalıdır. Bu üçüncü taraf denetimi ile veya yönetimin iç denetim fonksiyonu ve denetim sonuçlarından sağlanmalıdır.

ME2.7 Çözüm Eylemleri

Kontrol değerlendirmeleri ve raporlara dayanarak çözüm eylemleri tanımlanmalı ve başlatılmalıdır. Raporlarda şunlar yer almalıdır:
Yönetim yanıtlarının revizyonu, görüşmeleri ve oluşturulması
Çözüm için sorumluluk atanması (risk kabulünü içerebilir)
Taahhüt edilen eylem sonuçlarının izlenmesi.

ME3 Yönetmeliklere Uyumluluğun Sağlanması

ME3.1 BT üzerinde Potansiyel Etkisi Olan Yasa ve Yönetmeliklerin Tanımlanması
ME3.2 Yönetmelik Koşullarının Karşılanmasında Optimizasyonun Sağlanması
ME3.3 Yönetmelik Koşullarıyla Uyumluluğun Değerlendirilmesi

ME3.4 Uyumluluğun Olumlu Biçimde Sağlanması
ME3.5 Tümleşik Raporlama

ME3.1 BT üzerinde Potansiyel Etkisi Olan Yasa ve Yönetmeliklerin Tanımlanması

Bilgi, üçüncü taraf hizmetlerini de kapsayan bilgi hizmetleri teslimatı ve Bilgi Teknolojileri organizasyonu, süreçleri ve altyapısıyla ilgili yerel ve uluslararası yasal koşulların, sözleşme, politika ve yönetmelik koşullarının zamanında tanımlanmasını sağlayacak bir süreç geliştirilmelidir. Elektronik ticaret, veri akışı, gizlilik, iç denetimler, finansal raporlama, sektörel yönetmelikler, fikri haklarla telif haklarının korunması ile sağlık ve güvenlik hakkındaki yasa ve yönetmelikler göz önüne alınmalıdır.

ME3.2 Yönetmelik Koşullarının Karşılanmasında Optimizasyonun Sağlanması

Yasa ve yönetmelikler tarafından belirlenen koşulların etkin biçimde kapsanmasını sağlamak amacıyla, Bilgi Teknolojileri politikalarını, standartlarını ve prosedürleri incelenerek, en iyi hale getirilmelidir.

ME3.3 Yönetmelik Koşullarıyla Uyumluluğun Değerlendirilmesi

Yasa ve yönetmeliklerde belirtilen koşullar da dahil olmak üzere, Bilgi Teknolojileri politikaları, standartlar ve prosedürler ile uyumluluğu, iş ve Bilgi Teknolojileri yönetiminin idaresinde ve iç denetim mekanizması da çalıştırılarak etkin biçimde değerlendirilmelidir.

ME3.4 Uyumluluğun Olumlu Biçimde Sağlanması

Uyumluluğun olumlu biçimde sağlanması ve raporlanması amacıyla, gerektiğinde sorumlu süreç sahibinin zamanında olası uyumluluk eksikliklerleriyle ilgili olarak düzeltici önlemleri almasını/uygulamasını sağlayan prosedürler tanımlanmalıdır ve uygulanmalıdır. Uyumluluk ilerleme ve mevcut durumu

hakkındaki Bilgi Teknolojileri raporlaması, diğer iş fonksiyonlarından gelen benzer çıktılarla bütünleştirilmelidir.

ME3.5 Tümleşik Raporlama

Yasal gereklilikler hakkındaki Bilgi Teknolojileri raporlaması, diğer iş fonksiyonlarından gelen benzer çıktılarla bütünleştirilmelidir.

ME4 BT Yönetimi Sağlanması

ME4.1 BT Yönetimi Çerçevesinin Oluşturulması
ME4.2 Stratejik Uyum
ME4.3 Değer Yaratma
ME4.4 kaynak Yönetimi
ME4.5 Risk Yönetimi
ME4.6 Performans Ölçümü
ME4.7 Bağımsız Denetim/Güvence

ME4.1 BT Yönetimi Çerçevesinin Oluşturulması

Yönetim Kuruluyla birlikte çalışarak, kuruluşun BT' nin etkinleştirildiği yatırım programlarının kendi stratejileriyle uyum içinde olmasını ve hedeflerine ulaşmasını sağlayacak liderlik, süreçler, roller ve sorumluluklar, bilgi gereksinimleri ve organizasyonel yapıları kapsayan BT yönetim çerçevesini tanımlanmalıdır ve oluşturulmalıdır. Söz konusu çerçeve; kuruluşun stratejisi, bu stratejiyi uygulayan BT' nin etkinleştirildiği yatırım programları portföyü, bağımsız yatırım programları ile programları hazırlayan işletme ve BT projeleri arasında açık ve anlaşılır bir bağlantı sağlamalıdır. Çerçeve, iç denetimde ve idarede kopma yaşanmaması için sağlam/anlaşılır sorumluluklar ve uygulamalar sağlamalıdır. Çerçeve, kuruluşun genel denetim ortamıyla ve genel kabul gören denetim ilkeleriyle tutarlı olmalıdır ve BT sürecini ve denetim çerçevesini temel almalıdır (Uzunay 2007, 185).

ME4.2 Stratejik Uyum

BT' nin rolü, teknolojik öngörüsü ve yetenekleri gibi BT konularında yönetim kurulunun ve yöneticilerin bilgi sahibi olması sağlanmalıdır. BT' nin işletme stratejisine yapacağı olası katkı konusunda işletme ve BT arasında ortak bir anlayış geliştirilmelidir. BT' nin etkinleştirildiği yatırımlar, işletmenin stratejilerine ulaşırken BT yeteneklerinden elde ettiği değeri en uygun hale getirmek için yapmak zorunda olduğu değişikliklerin tamamını içeren bir program portföyü olarak yönetildiğinde; değerin yalnızca BT' den sağlandığı konusunun açıkça anlaşılması sağlanmalıdır. BT stratejik komitesi gibi yönetim organlarını tanımlayıp uygulamaya koyarken, BT ile ilgili yönetime strateji yön sağlamak amacıyla yönetim kuruluyla birlikte çalışarak, stratejilerin ve hedeflerin işletme birimlerine ve BT fonksiyonlarına doğru yayılmasını ve işletme ile BT arasında güven oluşturulması sağlanmalıdır. Stratejik ve operasyonel açıdan BT' nin işletmeden ayrılmasını sağlayarak, işletme ve BT' yi stratejik karar alma ve BT' nin etkinleştirildiği yatırımlardan yarar elde etme konusunda sorumluluğun paylaşılması cesaretlendirilmelidir(Heschl 2006, 185).

ME4.3 Değer Yaratma

BT' nin etkinleştirildiği yatırım programları ve BT varlıklarıyla hizmetleri, kuruluşun stratejisini ve hedeflerini desteklemede olası en yüksek değeri sağlayacak biçimde yönetilmelidir. BT' nin etkinleştirildiği yatırımlardan ve bu sonuçları elde etmek için harcanması gereken çaba kapsamının tamamından beklenen iş sonuçlarının anlaşılması, kapsamlı ve tutarlı iş durumlarının oluşturulması ve paydaşlarca onaylanması, varlıkların ve yatırımların ekonomik ömür döngüsü içinde yönetilmesi ve yeni hizmetler, etkin kazançlar ve iyileştirilmiş müşteri talebi karşılama oranı gibi yararların elde edilmesinde aktif bir yönetim bulunması sağlanmalıdır. Portföy, program ve proje yönetiminde disiplinli bir yaklaşım uygulanmalıdır. işletmenin tüm BT' nin etkinleştirildiği yatırımların sahipliğini üstlenmesinde ve BT' nin de kendi olanaklarını ve hizmetlerini sunma maliyetlerini en uygun düzeye getirmesinde kararlı davranılmalıdır. Teknoloji yatırımlarının olası

en yüksek oranda standartlaştırılmasını sağlanmalıdır ve teknik çözüm çeşitliliğinin yol açacağı artan maliyet ve karmaşıklıktan kaçınılmalıdır.

ME4.4 Kaynak Yönetimi

Yatırımı ve BT varlıklarının kullanımını düzenli değerlendirmelerle en iyi duruma getirilmelidir, BT' nin şu anki ve gelecekteki stratejik hedeflere ulaşabilecek ve işletme taleplerini karşılayabilecek yeterli, güncel ve yetenekli kaynaklarının bulunması sağlanmalıdır. Açıkça anlaşılır, tutarlı ve zorlayıcı insan kaynakları ve satın alma politikaları uygulayarak kaynak gereksinimlerinin etkin biçimde karşılanması ve yapısal politikalara ve standartlara uyulması sağlanmalıdır. BT altyapısı, olası her yerde standartlaştırılmasının ve gereken her yerde de birlikte çalışabilirlik özelliği taşımasının sağlanması amacıyla, düzenli olarak değerlendirilmelidir (Uzunay 2007, 185).

ME4.5 Risk Yönetimi

Kuruluştaki BT riskini tanımlamak amacıyla yönetim kuruluyla birlikte çalışılmalıdır. BT risk planını kuruluşa yayarak, bir risk planı üzerinde anlaşma sağlanmalıdır. Organizasyonda risk yönetimi sorumlulukları belirleyerek, işletmenin ve BT' nin düzenli olarak BT ile ilgili riskleri ve iş üzerindeki olası etkilerini düzenli olarak değerlendirilmesi ve raporlanması sağlanmalıdır. BT yönetiminin, iç denetimdeki ve yönetimdeki BT denetimi başarısızlıklarına ve zayıflıklarına ve bunların işletme üzerindeki gerçek ve olası etkilerine özellikle dikkat ederek risk oluşan yerlerin izlemesi sağlanmalıdır. Kuruluşun BT risk pozisyonu tüm paydaşlar tarafından izlenmelidir (Birengel 2006, 149).

ME4.6 Performans Ölçümü

Portföy, program ve BT performansıyla ilgili bilgiler yönetim kuruluna ve yöneticilere zamanında ve eksiksiz biçimde bildirilmelidir. Durum raporları ise, hangi planlanan hedeflere ulaşıldığı, hangi çıktıların elde edildiği, karşılanan

performans hedefleri ve giderilen riskler kapsamında tutulmalıdır. Diğer işletme fonksiyonlarından gelen benzer çıktıya sahip raporlar birleştirilmelidir. Performans ölçümleri büyük paydaşlar tarafından onaylanmalıdır. Yönetim kurulu ve üst yönetim bu raporları sorgulamalıdır ve BT yönetimine de olası sapmaları ve performans sorunlarını açıklama fırsatı verilmelidir (Üvey 2009, 142).

ME4.7 Bağımsız Denetim/Güvence

Kuruluşun yeterli ve uygun sayıda personele sahip, BT' nin politikalar, standartlar ve prosedürlerin yanı sıra genel kabul gören uygulamalar açısından da uyumluluğu hakkında zamanında yönetim kuruluna (büyük bir olasılıkla bir denetim kurulu aracılığıyla) bağımsız denetim bilgileri sunacak dış denetim hizmetlerini sağlayan bir fonksiyon kurması ve çalıştırması sağlanmalıdır. COBIT denetim ilkeleri; anlamayı sağlama, kontrol değerlendirmesi, uyum değerlendirmesi ve teşvik riski olmak üzere dört unsurdan oluşur. COBIT yönetim ilkeleri; kritik başarı faktörleri, kilit hedef göstergeleri, kilit performans göstergeleri, vade modelleri olmak üzere dört unsurdan oluşur. COBIT bu süreçler sonucunda işletme hedeflerinin gerçekleştirilmesini amaçlar. (Uzunay 2007, 224)

3.COBIT Olgunluk Modelleri

Bilgi teknolojilerinin iş hayatındaki önemi arttıkça, oldukça yüklü yatırım ve riskli proje yönetimlerini gerektiren bilgi teknolojileri süreçlerinin olgunluk seviyeleri hakkında güvence sağlayacak denetim metodolojilerine olan ihtiyaç da artmaktadır. Bu amaçla CobiT için düzenlenmiş olan olgunluk seviyeleri kurumun bugün nerede olduğunu, endüstrideki durum ve karşılaştırmalarını ve kurumun ileride nerede olmak istediği sorularına cevap vermektedir. Son zamanlarda CobiT olgunluk seviyeleri hakkında bir sürü spekülasyonun ortaya atılması CobiT 4.1'in ortaya çıkması ile durmuştur. Ana hatları ile 0 ila 5 arasında puan verilerek sınıflandırılan CobiT Olgunluk Modellerinin hesaplaması tabloda gösterildiği gibidir:

Tablo 2. Cobit Olgunluk Modelleri

	Anlayış ve Farkındalık	**Eğitim ve İletişimin**	**Süreç ve Uygulamalar**	**Teknoloji Kullanımı**	**Uygunluk**	**Uzmanlık**
0	Yok	Yok	Yok	Yok	Yok	Yok
1	Farkındalık var	İhtiyaç olduğunda münferit iletişim sağlanıyor	İhtiyaç olduğunda münferit dokümantasyon ve süreç yaklaşımı var.	Yok	Yok	Yok
2	İhtiyacın Bilincine Varılmış	Genel konular ve ihtiyaçlar üzerine iletişim sağlanıyor	Ortak benzer ancak kişi insiyatifinde uygulamalar var	Ortak / benzer araçlar kullanılmaya başlanmış	Münferit durumlarda standart olmayan izleme yöntemleri kullanılıyor	Yok
3	Önlem alınması yönünde anlayış oluşmuş	Kişisel girişimler ve bireysel eğitimler mevcut	Prosedürler Oluşturulmuş ve Dokümante Edilmiş. Bunların İyileştirilmesine Başlanmış	Ortak Yöntemlerin kullanılması için standart oluşturulmuş	Standart olmayan izleme ve ölçme yöntemleri kullanılıyor. Kişiye bağlı sebep-sonuç ilişkileri gözlenebiliyor	İş süreçlerine teknoloji uzmanlarını n da katılımı Sağlanıyor
4	Tüm gereklilikler biliniyor	Program yönetimi ve resmi eğitim var	Süreç sahipliği ve sorumlulukları belirlenmiş, süreç olgunluğu sağlanmış. kurum içi en iyi uygulamalara geçilmiş	Teknolojik olgunluğa ulaşılmış, standart yöntemlerin kullanılması sağlanmış	Belirlenen süreçlerde kurumsal karne uygulaması yapılıyor. farklılıklar izleniyor; sebep-sonuç analizi **var**	Konuyla ilgili tüm uzmanların katılımı sağlanıyor
5	Üst düzey ve ileri görüşlü bir anlayış seviyesi var	İletişim ve eğitim konularında en iyi yöntemler uygulanıyor ve en yeni Gelişmeler takıp ediliyor	Sektör ve konu ile ilgili en iyi yöntemler uygulanmakta	En gelişmiş teknolojiler uygulanmakta, teknoloji kullanımı optimize edilmiş	Tüm süreçlerde kurumsal karne uygulaması yapılıyor, farklılıklar izleniyor ve iyileştirici önlemler alınıyor, sebep-sonuç analizi her durumda var	Yabancı Uzmanların ve Endüstri Liderlerinin Danışmanlığ ı Almıyor

Kaynak: Artinyan, E.N., **COBIT Çerçevesi,** Deloitte Kurumsal Risk Hizmetleri, 2008, s. 175

DÖRDÜNCÜ BÖLÜM
TEKNOLOJİ YÖNETİMİ

Teknoloji Yönetimi Amerikan Ulusal Araştırma Kurumu'nun raporuna göre, teknoloji yönetimi; "Bir organizasyonun stratejik ve taktik amaçlarının şekillendirilmesinde ve bunlara ulaşılmasında gereksinim duyulan teknolojik kapasitenin planlanması, geliştirilmesi ve uygulanmasıdır"(İnceler, H., "Teknoloji Yönetiminin Ekonomik ve Sosyal Etkileri", Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 1995). Başka bir ifadeyle, teknoloji yönetimi yöneticilik ile teknik uzmanlık arasında bağlantıyı kurmak ve teknoloji transferi teknoloji pazarlaması, teknolojik planlama Ar-Ge. tasarım imalat, prototip oluşturma, test etme gibi teknoloji teminine ve teknoloji geliştirilmesine yönelik faaliyetlerin planlanması, örgütlenmesi, yürütülmesi, koordinasyonu ve kontrolüyle ilgili faaliyetlerin tümüdür.

Teknoloji yönetimi organizasyonlar açısından en az teknoloji üretimi kadar kritiktir. Çünkü her zaman ileri teknoloji kullanmak organizasyonu hedefi doğrultusuna taşımaz, aksine bazen geleneksel olarak adlandırılan yöntemler daha iyi bir performans gösterir. Bazı organizasyonlar benzer iş sahası ve donanıma sahip olmasına rağmen elde ettiği sonuçların verimliliğine bakılınca bazı farklar görülmektedir. Bu sonuca sebep olarak yerleştirilmiş tezgah donanımı, is gücünü teknik dizeyi ve yönetimin yetkinliğindeki farklar gösterilebilir (Öğüt, 2001, 235).
Sadece en ileri teknolojiyi kullanmak organizasyon için yeterli olmadığından teknolojinin organizasyona adaptasyonu gereklidir. Bu adaptasyon iş hedefleri ve organizasyonun yapısal düzeni göz önünde bulundurularak yapılmalıdır. Buna bağlı olarak çok uluslu girişim alanı olan organizasyonlar uygulama kabiliyetlerini hesaba katarak birleşik teknoloji yörüngesi etrafında etkin bir yönetim zorunlu hale getirmektedir (Pearce 1999,125-148).

1.Teknoloji Yönetiminde Yaklaşımlar

Günümüzde teknoloji yönetimi ile ilgili olan yaklaşımlar teknolojinin stratejik ve operasyonel perspektiften sistematik olarak yönetilmesi ihtiyacım ortaya

çıkartmıştır. Bununla birlikte, teknolojinin değerlendirilmesi ile ilgili olan belirsizlik ve teknolojiyi yönetmenin zorluğu da karşılaşılan önemli sorunlar olarak görülebilir (Linn vd. 2000, ss.397-412).

Mikro yaklaşımda, yani firma bazında ele alınan teknoloji yönetiminde esas hedef, firmanın karını ve üretimini maksimize etmeye dönük olarak, teknik imkanlarıyla insan gücü kaynaklarını en optimum şeklinde planlama, örgütleme ve koordine etmek suretiyle yönetim faaliyetini gerçekleştirmektir. Makro yaklaşımda ise, teknoloji yönetimi ülkenin sosyo-ekonomik kalkınma hedeflerine uygun olarak, bilim-teknoloji planlaması, politika tespiti, teknolojik yatırımlar ve teknolojik altyapıyla ilgili faaliyetlerin yürütülmesi konuları ele alınmaktadır. Teknoloji Yönetimi'nin kapsamı içindeki konular şunlardır (TBD Kamu-BİB, 2008, 15-16):

- Teknolojik Tahmin
- Teknolojik Planlama
- Teknolojik Risk Analizleri
- Ar-Ge Yönetimi
- Teknolojik Yeniliklerin Yönetimi
- Teknolojik Rekabet Stratejileri
- Teknoloji Transferi
- Teknoloji Seçimi
- Teknolojinin Ticarileştirilmesi (Patent, Lisans Anlaşmaları, Copyrights, Ticari Markalar)
- Mühendislerin ve Bilim Adamlarının Yönetimi
- Teknoloji ve Organizasyonel Değişimler

Gerek ülkeler, gerekse firmalar hızla değişen teknolojik, ekonomik ve siyasi şartlarda devam eden acımasız uluslararası rekabette güçlü olabilmek için en iyi stratejiyi tayin etmek ve uygulayabilmek durumundadırlar. Teknolojik gelişme ve teknolojik yeniliklere sahip olmak rekabette en güçlü silahtır. Ar-Ge ve teknoloji geliştirme yatırımları uzun vadede karlı ve kalifiye, yetişmiş insan gücü gerektiren yatırımlardır. Teknoloji temini için farklı seçenekler söz konusudur (Karabacak 2009, 243):

- Firma içi Ar-Ge faaliyetleriyle ürün ve proses geliştirmek.

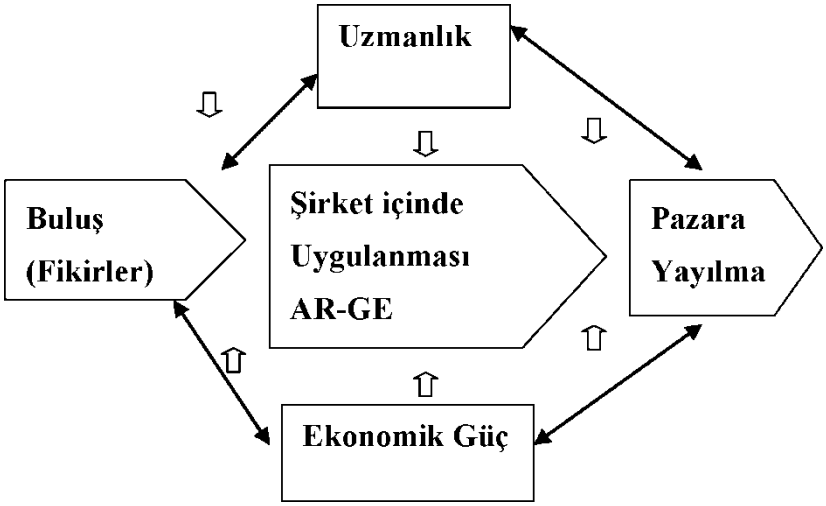
- Teknolojiyi transfer etme (Lisans alma, Yabancı sermaye ortaklığı, Joint Venture vb.)
- Mevcut teknolojiyi kullanmak

1.1.Teknoloji Yönetim Süreci

Teknolojik yenilik geliştirme süreci uzun bir süreci içerir. Buluş veya yeni bir fikir aşamasından başlayan bu süreç Ar-Ge faaliyetlerinin gerçekleştirilmesi ve Ar-Ge faaliyetleri sonucu ortaya çıkan yeni ürün ve hizmetlerin pazara ve müşterilere sunulmasına dek yapılan bütün faaliyetleri içerir. Bütün bu sürecin yönetimi esnasında verilen kararlar şirketin geleceği açısından son derece önemli kararlardır. (Yazıcı 2006, 88)

Teknolojik Yenilik sürecinin yönetimindeki stratejik karar noktaları şunlardır:

- Stratejik Teknolojik Planlama
- Teknolojik Tahmin
- Araştırma ve Geliştirme
- Teknolojinin Ticarileştirilmesi
- Teknolojinin Pazarlanması



Şekil 6. Teknoloji Yönetimi Süreci

Kaynak: Yazıcı, A., **Bilişim Teknolojilerinde Risk Yönetimi-2**. Çalışma Grubu, Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu VIII, İstanbul, 2006, 88.

Teknolojik bazlı işletmeler Teknoloji Yönetimi'ni işletmelerinde kullanırlarsa teknolojik faktörlü her hangi bir krizi de önceden fark edebilirler, meydana gelen teknoloji faktörlü bir krizden işletmelerini en az hasarla çıkarmalarını ve işletmelerinin bu krizden fırsat yaratabilmesini de sağlarlar. (Baraçlı 2001, 45).Buna yönelik bazı işletmeler tarafından hangi yönetimsel araçların kullanılacağın zamanla değişebileceği ile ilgili olarak yapılan araştırmada bilgi yönetiminin 1996- 2000 yılları arasında yukarı doğru olumlu bir şekilde ilerleme gösterdiği belirtilmektedir. Yakın zamana ait olan bu değerlendirme bize bilgi yönetimini ve bilgi teknolojileri ile birlikte teknoloji yönetimi kullanımının ileride artacağı bilgisi verir (Rigby ve Bilodeau 2007, 20).

1.2.Bankalarda Teknoloji Yönetimi ve Kontrolü

Teknolojinin önemini anlayamayan ya da teknolojiyi verimli bir şekilde kullanamayan bankalar zamanla küçülerek yok olma tehlikesi ile karşı karşıya kalabilmektedirler. Teknolojinin bu kadar önemli ve kritik bir hal alması, bankalar için beraberinde risklerini getirmektedir. Teknolojinin riski nedir? Nasıl ölçülür? Ne şekilde engellenebilir veya en aza indirilir? gibi soruların sorulması ve cevaplarına göre aksiyon alınması bankalar için gerekli hale gelmiştir. Çünkü teknolojide risk yoktur demek mümkün değildir. Önemli olan teknolojiyi kullanırken riskleri iyi belirlemek, hiçbir şekilde göz ardı etmemek veya küçümsememektir (Rosenblum M. ve T. Garfinkel, 2005, 38). Bankalar teknolojiyi bilinçsizce kullanmamalı, kısa vadeli ve dar açılı düşünmemeli, geniş bir perspektifte gerekli tüm koşulları ile birlikte ele almalıdır.

Bunu yapmanın yolu teknolojiyi iyi analiz etmek, işlemleri yaparken, projeleri geliştirirken kontrolleri ve riskleri düşünmek ve yapılması gerekenleri uygulamaktır. Yani teknolojinin kontrolü, risklerin en aza indirilmesinde en önemli araçlardanbirtanesidir.(http,s.//www.bddk.org.tr/WebSitesi/turkce/Basel/Basel_II.aspx, Erişim: 18.07.2014)

Teknoloji Operasyonlarında dört ana işlev mevcuttur (Güvener 2000, 69).

- Kesintisiz hizmet: Amaç, bankanın mevcut tüm sistemlerinin planlanan çalışma süreleri boyunca kesintisiz hizmet vermelerini sağlamaktır. Banka sistemlerinin servis dışı kalma süreleri yıllık olarak hedeflenen süreleri aşmamalıdır. Bankanın müşterisine "Sistemimiz çalışmıyor" şeklinde bir mazeret sunması hiçbir zaman kabul edilebilir bir durum olmamalıdır.
- Güvenlik: Bankanın tüm sistemlerinin her türlü güvenliği sağlanmalıdır. Fiziksel güvenlik, bilgilerin güvenliği, giriş kontrolü, virüs, yetkisiz erişim gibi tüm güvenlik sorunları bu gruptadır. Bankalar güvenlik unsurlarının hiç birinden, hiç bir durumda taviz verilmemelidir Çünkü bankalar için kurumsal bilgi en önemli varlıkları arasındadır ve bu nedenle çok iyi korunması gereklidir (Sahibudin vd. 2008, 749 –753).
- Destek ve Yardım Masası: Bankaların teknoloji operasyonlarında kullanıcıya (müşteriye yada banka içi kullanıcı) verilecek yardım ve destek çok önemli bir konudur. Destek olmadan sistemlerin sürekli ve verimli olarak hizmet vermeleri sağlanamaz. Kullanıcı desteği mutlaka yardım masası gibi yapılanmalar ile desteklenmelidir. Bunun sonucunda destek hizmetinin kalitesi artırılarak ve cevap verme süresi kısaltılarak iç müşteri memnuniyeti en üst düzeye getirilmelidir.
- Yedekleme: Yedekleme tüm teknoloji platformlarının operasyonları açısından çok önemlidir. Donanım, yazılım, işletim sistemleri ve data unsurlarının yedeklemelerinin sağlanması işin sürekliliği açısından şarttır. Bankalar mutlaka sistemlerini yedeklemeli, herhangi bir sorun meydana gelmesi durumunda data kaybına uğramamalıdır.

Bu dört ana işlevi eksiksiz yerine getirmek için takip edilmesi gerekli yöntemler 8 alt başlık altında ele alınabilir (Güvener 2000, 78).

Problem Yönetimi: Problem yönetimi banka içerisinde problemlerin tanımlanması, gruplandırılması, kayıt edilmesi, çözümlenmesi ve bir daha tekrar etmemesi için önlemlerin alınması konularını kapsar. Etkin bir problem yönetimi ile teknik aksaklıklar azaltılarak hizmet kalitesi artırılabilir. Bankada teknik anlamda aksayan ve zayıf yönler, etkin bir problem yönetimi ile kolayca tespit edilebilir ve gerekli önlemler alınabilir. Böylelikle müşteriye sunulan hizmetin olabildiğince istikrarlı ve kalıcı olması amaçlanır. Aksi olduğu takdirde devamlı olmayan hizmet bankaya

problem olarak dönecektir. Bu yüzden BT içerisinde hatalar gerçekleşmeden öngörülmeli bir çözüm planı çıkarılmalı ve problem doğmadan bunla başa çıkılmalıdır (http://itilorganizasyon.wordpress.com/2011/06/19/problem-yonetimi/, Erişim: 22/08/2014).

Değişim Yönetimi

Bilgi ekonomisinde organizasyonlar arasında rekabetin en çok yaşandığı durum bilgi ve bilgiye dayalı teknolojik yeniliklerdir. Bilişim sistemler, bilgi ekonomisinde bilginin ekonomik değer kazanmasındaki en büyük faktördür. Bilişim sistemlerinin hayatımıza bu kadar dahil olup bir çok alanını kaplaması da bilgi toplumuna ve bilgi ekonomisine geçiş giderek daha da kolay bir hale getirmektedir (Öğüt 2003, 235). Organizasyonların bilgi teknolojileri açısından bu denli bir yarış halinde olmaları sonucunda üstünlüğü örgütsel yapılarında yapacakları yenilik ve değişikliklere bağlıdır (Monger 1998, 13).

Değişim yönetimi, bankalarda kullanılan sistemlerde yapılacak her türlü değişimin planlanması, test edilmesi ve uygulamaya alınmasını kapsar. Burada ana amaç kullanımda olan tüm operasyonel sistemlerin güvenirliliğini sağlamak, yapılması gerekli değişiklik sırasında oluşabilecek riskleri en aza indirmektir. Öncelikle değişimle ilgili planlar oluşturulmalı ve yöneticilerden ilgili onaylar alınmalıdır. Yapılan her değişiklik bir süre takip edilmeli ve olası hatada değişim yenilenmelidir.

Bilgi Güvenliği

Bilgi güvenliği, değerli varlıkların kaybedilmesi, yanlış kullanılması, ifşa edilmesi ve zarar görmesini önlemekle ilgilidir. Değerli varlıklar; kaydedilen, işlenen, saklanan, paylaşılan, elektronik ortamda gönderilen bilgilerdir. Bu bilgiler tehditlere karşı korunmalıdır. Bilgi güvenliğinin amacı; bilgiyle ilgili olanları ve kullanılırlık, gizlilik, bütünlük unsurları ile ilgili başarısızlıklardan zarar görebilecek sistemleri bağlantıları korumaktadır (Uzunay 2007, 185).

Bu noktada bilgin güvenliği ve verimliliği adına yapılan çalışmalar geçmişe

baktığımızda aslında çok da hızlı gelişmemektedir. Çünkü her yeni teknoloji beraberinde bir problemi de getirmektedir. Kullanılan eski yapılar çoğu zaman probleme neden olur ve bilişim güvenliğiyle ilgili problem yaratabilir. Bilişim güvenliğiyle ilgili birçok bileşen bulunmaktadır fakat günümüzde en yaygın kullanılanı güvenlik duvarıdır. Güvenlik duvarı bir süzgeç gibidir, internetten yerel ağa gelen verileri süzgeçten geçirir ve yalnızca yetkilendirilmiş bağlantı noktaları için geçiş sağlar(Uzunay 2007, 185).

2.COBIT'te Bilgi Güvenliği

COBIT Güvenlik Dayanağı daha iyi güvenlik sağlama ihtiyacı üzerine tasarlanmış ve bilgi kullanıcılarını risklerden korumak için önemli tavsiyeler ve pratik araçlar içeren bir modeldir. COBIT Bilgi Güvenliği; 3 maddeden oluşur: Arka planın okunması, esaslı güvenlik dayanağı ve teknolojik güvenlik risklerinin yönetimi (http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx, Erişim: 14.04.2014)

COBIT Bilgi Güvenliği yüzde yüz güvenlik iddia etmez fakat oluşturulan tavsiyeleri takip edip çok etkili seviyede güvenlik sağlayabilir. Bilgi teknolojisi kullanılırken bilincin arttırılması, gerçekleşebilecek risklerin belirlenmesi ve hassas önlemlerin alınması çok az gayretle gerçekleştirilebilir. Bu model, kontrolün her safhasında ortaya çıkabilecek tüm riskleri teşhis etmez ama ne yapılması gerektiğini ve nasıl yapılması gerektiğini anlama yeteneğini geliştirir. İyi bir bilgi güvenliği sadece riskleri azaltmaz. İyi güvenlik, işletmenin bağlantıda bulunduğu diğer işletmeler üzerindeki itibarı, güveni de arttırır, zaman kaybını önleyerek ekinliği arttırır (Uzunay 2007, 233)

2.1.Beklenmedik Durum Planları

Bankaların müşterilerine vermekte olduğu hizmetlerin sürekliliğini sağlamak ve aksamalara engel olmak amacı ile beklenmedik durumlarda neler yapılacağının belirlendiği bir plan yapılması ereklidir. (Başarır 2006, 77)

2.2. Kaynakların Yönetilmesi

Bankalarda teknoloji yönetiminde kaynakların bilinçli kullanımı son derece önemlidir. Hem teknolojik sistemler/platformlar hem de bunları kullanacak, destekleyecek elemanların etkin bir maliyet kontrolü ile en verimli şekilde kullanımı gerekmektedir. (Sahibudin vd. 2008, 749 –753). Banka düzeyinde iş planları ve bunu destekleyen teknoloji planlarının yapılması gereklidir. Yıllık olarak yapılan planlara uyulmalı ve değişiklikler ancak üst yönetimin onayı ile yapılmalıdır. Mevcut sistemlerin performansları sürekli olarak ölçülmeli, kapasite planlaması yapılmalıdır. (Atan 2002, 97)

2.3.Uygulama Programlar Ve İşletim Sistemleri Alımı

Uygulama programlarını geliştirmek her zaman en uygun yöntem olmayabilir. Teknik olarak iyi düzeyde geliştirilmiş, maliyeti fazla olmayan ve bankanın ihtiyaçlarını karşılayacak uygulama programlarının piyasadan temin edilmesi de uygun bir çözüm olabilir. Bu durumda iyi bir araştırma yaparak bankanın ihtiyacını karşılayacak, ticari bir hazır paket çözümü yoluna gidilebilir. Burada dikkat edilmesi gereken en önemli nokta uyumluluktur. Alınan programların mevcut sistemler ile uyumlu olmaları hem destek hem de geliştirme açısından çok önemlidir. (Güvener 2000, 97)

2.4.Dış Kaynak Kullanımı

Bilgi sistemlerinin ve bilişim teknolojisinin içerdiği risklerin, bankaların faaliyetlerinin kesintisiz yürütülmesi ve muhtemel zararların önlenmesi amacıyla, etkin olarak kontrolü şarttır. Genel kontrol ve incelemeler, veri yedekleme ve ilgili diğer işlemleri, kullanılan temel yazılımlardaki ve diğer yazılımlardaki gelişmeleri, bilgi erişim politikalarını ve bilgi erişimine ilişkin fiziki ve mantıksal güvenlik kontrollerini kapsar. Uygulamaya yönelik kontrol ve incelemeler, işlemlerin kaydının

kontrolünü sağlayan ve yazılım uygulamalarının ve diğer el kitabı uygulama usullerinin içinde tanımlanan elektronik ortamdaki kontrol safhalarından oluşur. Uygulamaya yönelik kontrol ve incelemeler, mantıksal erişimler ile yazılımların özel kontrollerini ve benzeri diğer özel kontrol ve incelemeleri içerir (Türkiye Bilişim Derneği, 2005).

Teknoloji kontrol grubu, teknoloji yönetiminde kısaca vurgulanan tüm bu alt başlıklar için şablon kontrol noktaları belirlemeli, kontrol listeleri hazırlamalı ve belirli aralıklarla bu konular da denetlemeler yapmalıdır. Aksayan yönler tespit edildikten sonra gerekli tedbirler alınarak bu sorunların giderilmesine çalışılmalı daha sonraki denetlemelerde bu konularda ki gelişmeler gözlemlenmelidir. Tespit edilen aksaklıkların kısa sürede giderilmesi çok önemlidir. Eğer bu takip edilmez ve aksamalar devam ederse, alışkanlık haline gelir ve mevcut risk daha da büyür. Bunun sonucunda da hem bankanın hiç öngörmediği risklerle karşılaşması mümkün olabilir. Belli başlı teknoloji kontrol noktaları şu şekilde olmalıdır (Güvener 2000, 114):

- Logların kontrolü
- Kontrol listelerinin denetlenmesi
- Yedekleme işlemlerinin kontrolü
- Gün sonu ve gün başı işlemlerinin kontrolü
- Erişim haklarının denetlenmesi
- Projelerin takibi, zamanında ve belirtilen bütçeler çerçevesinde gerçekleşip, gerçekleşmediklerinin tespiti, hedeflerin karşılanıp karşılanmadığının kontrolü
- Değişim yönetimi kurallarına uyulup uyulmadığının kontrolü, gerekli onayların kontrolü
- Problem yönetimi prosedürlerine uyulup uyulmadığının kontrolü, istatistiklerin değerlendirilip değerlendirilmediğinin incelenmesi
- Virüs önleme mekanizması denetlenmeli aksamalar bildirilmesi
- Dış kaynak kullanımında kurallara uyulup uyulmadığı, destek alınan firmanın kaliteli servis verip vermediği denetlenmesi
- Beklenmedik durum planlarının yıllık olarak test edilmeleri kontrol edilmesi, testlerin kurallara uygun olarak ve gerçeği yansıtmaları sağlanması

- Kaynak kullanımı ve sistemlerin performanslarının izlenip izlenmediği denetlenmesi
- Kapasite planlamasının yapılması, teknoloji ve iş planlarının bulunup bulunmadığı kurum genelinde denetlenmesi
- Kontrol prosedürlerinde standardizasyon sağlanması
- Belirtilen bu kontroller hakkında detaylı şablonlar oluşturulmalı ve yazılı kontrol prosedürleri geliştirilmesi.

BEŞİNCİ BÖLÜM
RİSK ANALİZİ METODOLOJİSİ

1.Risk Değerlendirme ve Risk Yönetimi

İlerleyen teknolojiyle birlikte sayısal dünya daha genişlemekte ve bu da sonuç olarak bilginin güvenirliği ve uyumluluğu konusunda bazı riskleri beraberinde getirmektedir. Fakat tehdit ve risk analizi organizasyonlar tarafından hala çok yaygın olarak kullanılmamakta ve anlaşılmamaktadır. Yanlış bilgi kaynakları, organizasyonu beklentisi yönündeki iş hedefinden ayıracağı gibi ilgili çalışmalar esnasında harcanan emek, zaman ve para da organizasyonu mali anlamda büyük kayıplara uğratabilir. Organizasyonlar bu gibi olumsuz sonuçlardan kaçınmak için bazı önlemler alıp çeşitli testler veya etik bilgisayar korsanlığı yöntemini kullanıyor. Fakat burada önemli ve asıl kritik nokta geliştirilmiş birçok yöntemden organizasyonun hedeflerine en uygun ve en gelişmiş olan yöntemi kullanmaktır (Aktaş 2009, ss.72-74)

Risk analizi yaparken öncelikle karşılaşılan riskleri kabul edilebilir bir seviyeye indirmek üzere karşı önlemler tespit edilir. Daha sonra bir plan hazırlanıp bu plan çerçevesinde önlemlerin alınmasını sağlamak gerekir. Bu organizasyon için yeni yatırımlara sebep olabileceği gibi bazı zamanlar maliyetsiz bir şekilde bazı önlemlerin alınması söz konusu olabilir (Ersoy 2012, 64). Risk seviyesinin kabul edilebilir risk seviyesine çıkması durumunda, organizasyon içinde yönetim desteği ile iyileştirilme çalışması planlanır ve başlatılır.

Bilgi varlıklarının envanterinin çıkarılması, risk yönetiminin önemli bir parçasıdır. Ayrıca, varlığın içeriğinde veya yapısında bir değişiklik olması durumunda da risk değerlendirme süreci işletilir. Bilgi Güvenliği ile ilgili tüm politikalarda belirtilen kurallara uyumun teknik, finansal veya kaynak yetersizliği gibi nedenlerle sağlanamadığı durumlarda kontrollerin uygulanamaması temelli risk değerlendirilir

Varlık Risk Listeleri yılda bir kez dönemsel olarak gözden geçirilmesi gerekir. “Değişim Yönetimi”, “Vaka Yönetimi”, “İç ve Dış Denetim” ve “Dönemsel Gözden Geçirme” süreçleri çalıştıkça, süreç içerisinde yer alan ilgili varlıklar gözden geçirilir ve gerektiği durumda risk değerlendirme süreci tekrar işletilir.

1.1.Risk Değerlendirme

Bilgi varlıkları belirlendikten sonra bu varlıklar üzerindeki risklerin neler olduğunu belirlemek için risk değerlendirme çalışmalarına başlanır. Risk değerlendirme adımı, ISO/IEC 27001 Bilgi Güvenliği Standardının yapılmasını şart koştuğu işlemlerin en önemlilerinden biridir. Risk değerlendirme çalışmasında öncelikli olarak varlıklarla ilgili olabilecek zafiyetler belirlenir. Zafiyetler belirlendikten sonra, bu zafiyetleri kullanabilecek tehditlerin neler olduğu yazılır. Sonrasında ise bu zafiyet ve tehdidin gerçeklemesi olasılığı sonucu yaşanabilecek risk sonucu tanımlanır. Bu tanımlamalar zafiyet/ açıklık/ zayıflık/ kırılganlık/ yararlanabilirlik şeklinde değerlendirilebilir. Varlıklar ile ilgili tehdit, zafiyet ve risk tanımlanırken öncelikli olarak varlığın etiket değeri “Sır”, “Gizli” ve “Dahili” olanlar göz önüne alınır.

Bir varlıktaki zayıflıkları kullanarak varlığa kısmen ya da tamamen zarar veren etkenlere tehdit denilmektedir. Bir varlığı tehditlere karşı korumasız hale getiren bu zayıflıklar “zafiyet” olarak adlandırılır. Riskten bahsedebilmek için öncelikle bir zafiyetin olması gerekir buradaki eksiklik bir tehdidin oluşmasına yol açabilir ve bu gerçekleşirse risk de gerçekleşmiş olur. (Ersoy, 2012). Risk, tehdidin gerçekleşmesi, zafiyetin kötüye kullanılması ve varlığın GBK’ sının zarar görmesi, üçlemesinin oluşması durumudur. Riskin tanımlanmasından sonra Risk Değerlendirme Adımları” maddesine uygun olarak risk değerlendirme çalışmasına devam edilir.

1.2.Risk Değerlendirme Adımları

1.2.1.Birinci Adım: Riskin Derecelendirilmesi

Risk derecelendirilmesi risk yönetimi açısından en önemli, en hayati ve en fazla emek isteyen risk değerlendirme çalışmasıdır. Bu aşamada riskler tanımlanıp risk analizi yapıldıktan sonra olası etkiler de hesaba katılır ve değerlendirilir, bunlarla ilgili karşıt önlemler alınır. Böylelikle bir sonraki adım olan riske karsı yapılabilecekler için, riski düşürücü stratejilerin önerilmesine yardımcı olunur(Aktaş, 2009).

Risk değerlendirmede yapılması gerekenler şu şekilde sıralanabilir (NIST, 1997, 12; Swanson and Guttman 1996, 14; Dhillon 2007, 102):

a. Riskin etkisinin belirlenmesi (İşe Etkisi),

b. Riskin olasılığının belirlenmesi (Olasılık),

c. Risk skorunun hesaplanması (Risk Değeri)

1.2.1.1.Riskin etkisinin belirlenmesi (İşe Etkisi),

Etki, belirlenen zafiyetin kullanılması sonucunda tehdidin ortaya çıkmasıyla birlikte, ilgili varlığın G-B-K değerlerinden biri ya da aynı anda bir kaçının zarar görmesi ve etkilenmesi demektir. Bu etkilerin neler olabileceği yönünde bilgiler Tablo 1'de belirtilmiştir. Risk etkisi belirlenirken öncelikle hayati önem taşıyan, organizasyona büyük kayıplar yaşatabilecek riskleri tespit etmek adına önem derecesine göre riskler listelenir. Risk analizi, olasılığı yüksek ve büyük kayıplar yaşatabilecek risklere yönelmelidir. Bunu yaparken incelenecek bilgiler arasında gerekli olan bilgiyi bulmak adına öncelikle eleme yapılır. Böylelikle organizasyona önemli kayıplar yaşatabilecek kayıplara yönelinir. (Aktaş 2009, 5). Önem derecesi arttıkça sistem riski, dolayısıyla da organizasyonun riski artacaktır (NIST 1997, 12). Risk etkisini belirlemek için "Etki Değerlendirme Skalası" kullanılır. Burada yer alan "5"li seviyeden uygun olan değer seçilerek, listeye yazılır.

Tablo 3. Etki Değerlendirme Skalası

ETKİ DEĞERLENDİRME SKALASI					
Etkilenen Alan	**Etki Derecesi**				
Gizlilik, Bütünlük ve Kullanılabilirlik Riskinin Etkisi	5 Çok Yüksek	4 Yüksek	3 Orta	2 Düşük	1 Çok Düşük
Finansal Etki	500K TL finansal etki	300-500 K TL arasında finansal etki	100 – 300K TL arasında finansal etki	50 – 100K TL arasında finansal etki	50K TL'dan az finansal etki
Dış Müşteri Memnuniyeti Etkisi	%20+ müşterilerin etkilenmesi.	Müşteri portföyünün %20'sinin etkilenmesi	Müşteri portföyünün %10'unun etkilenmesi	Sadece bir müşterinin etkilenmesi	Dış Müşterilerin hiç etkilenmemesi.
Çalışan Memnuniyeti Etkisi	Çalışanların tümünün etkilenmesi Çalışanların günlük işlerinin tamamının etkilenmesi.	Çalışanların 75%'inin etkilenmesi. Çalışanların tümünün günlük işlerinin %70'inin etkilenmesi	Çalışanların 35%'ının etkilenmesi. Çalışanların tümünün günlük işlerinin %40'ının etkilenmesi	Çalışanların sadece 10%'unun etkilenmesi. Çalışanların tümünün günlük işlerinin %15'inin etkilenmesi.	Çalışanların günlük işlerinin aksamaması
İş/Servis Aksaması	8 saatten fazla iş/servis aksaması	6-8 saat arası iş/servis aksaması	4-6 saat arası iş/servis aksaması	2-4 saat arası iş/servis aksaması	2 saat iş/servis aksaması
İtibar Etkisi	Müşteri hedef kitlemiz içinde bulunan 10MIO+ kişinin fark edeceği, etkileneceği haber	Müşteri hedef kitlemiz içinde bulunan 5MIO+ kişinin fark edeceği, etkileneceği haber	Müşteri hedef kitlemiz içinde bulunan 1MIO+ kişinin fark edeceği, etkileneceği haber	Müşteri hedef kitlemiz içinde bulunan 100+ kişinin fark edeceği, etkileneceği haber	Kayda alınacak bir haber söz konusu olmaz.
Ceza/Hukuk	Şirket yönetiminin hapse girmesi. Lisans kaybı. Lisansın askıya alınması	Cironun %1'inden büyük maddi ceza ile sonuçlanacak risk	Cironun %1'inden küçük maddi ceza ile sonuçlanacak risk	Uyarı/kınama/mahkeme de hallolacak problemler	Herhangi kanuni/cezai bir problem yaratmaması
İnsan Sağlığı ve Güvenliği	Ölüm/kalıcı sakatlanma	Yatarak tedavi veya uzun süreli tedavi	Hastane/ayakta tedavi	Küçük yaralanma	Bir Etkisi yok.

Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 77.

İşe Etki Değeri; "Etki Değerlendirme Skalası" tablosuna bakılarak, uygun olan alanlarda görülebilecek etki değeri belirlenir.

1.2.1.2.Riskin olasılığının belirlenmesi (Olasılık),

Riskin olasılığının belirlenmesi için riskin gerçekleşmesine yönelik ortamdaki zafiyet ya da zafiyetler düşünülerek hareket edilir. Ortamda zafiyeti önleyecek yeterlilikte mevcut bir önlem, kontrol yoksa olasılık daha yüksektir.

Olasılık değerlerini belirlemek için "Tablo 4 Olasılık Değerlendirme Skalası" kullanılır. Burada yer alan "5"li seviyeden uygun olan seçilerek, listeye yazılır.

Tablo 4. Olasılık Değerlendirme Skalası

Risk Olasılık Değeri	Olasılık İhtimali	Oluşma Sıklığı
5 Çok Yüksek	Yılda 12+ kez gerçekleşir	Hemen hemen her seferinde meydana gelen
4 Yüksek	Yılda 2 – 12 kez gerçekleşir	Çoğu sefer meydana gelen
3 Orta	Yılda bir kez gerçekleşme olasılığı %70-100 arasında	Zaman zaman meydana gelen
2 Düşük	1 yıl içinde bir kez gerçekleşme ihtimali %30-%70 arasında olasılık	Nadiren meydana gelen
1 Çok Düşük	1 yıl içinde bir kez gerçekleşme ihtimali %30'dan küçük olasılık	Hemen hemen hiç meydana gelmeyen

Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 81.

Belirlenen işe etki değerinin mevcut koşullarda (zafiyet göz önüne alınarak) gerçekleşme ihtimali düşünülür ve tablo üzerinden uygun olasılık değeri belirlenir.

1.2.1.3.Risk skorunun hesaplanması (Risk Değeri)

Bu aşamanın amacı, analiz edilen sistemin risk seviyesini belirlemektir. Belirli bir tehdit-zayıflık ikilisi için risk, su üç parametrenin fonksiyonu olarak bulunur: tehdit kaynağının zayıflığı kullanma olasılığı, gerçeklesen kötü olayın yaptığı olumsuz etkinin şiddeti ve bu şiddeti azaltan veya ortadan kaldıran güvenlik kontrollerinin yeterlilik derecesi (Dhillon 2007, 108).

Risk, etki ve olasılığın bir bileşimi olarak ifade edilir ve risk skoru **“”Risk Skoru = İşe Etkisi X Olasılık”** formülüne göre hesaplanır.

Örneğin; varlığın “gizlilik” değeri yüksek (4), “bütünlük” değeri orta (3) ve “kullanılabilirlik” değer düşük (2) ise, bu durumda en yüksek değer yani “gizlilik” değeri (4) referans alınarak riskin etki değeri hesaplanır. “ETKİ DEĞERLENDİRME SKALASI” kullanılarak belirlenen etki değeri varlık değerinden yüksek olamaz. Etki değerinin varlık değerinden yüksek olması halinde varlık değerinin revize edilmesi öngörülür.

Risk hesaplanmasında etki ve olasılık değerleri atanırken aşağıdaki tablolardan faydalanılır. Birden fazla kriter değerlendirme için geçerliyse, yüksek olan değer hesaplama için baz alınır:

İşe Etki : Tablo 3 Etki Değerlendirme Skalası

Olasılık : Tablo 4 Olasılık Değerlendirme Skalası

Risk Skoru Hesaplama : Tablo 5 Risk Skoru Hesaplama Tablosu

Tablo 6 Örnek Risk Skoru Hesaplaması

Tablo 7 Risk Haritası (Etki ve Olasılık)

İşe etki değeri ve olasılık değerlerinin çarpımı ile Risk Skoru hesaplanır. Hesaplanan skor için “Risk Skoru Hesaplama Tablosu’ na bakılarak hangi aralığa denk geldiği görülür.

Tablo 5. Risk Skoru Hesaplama Tablosu

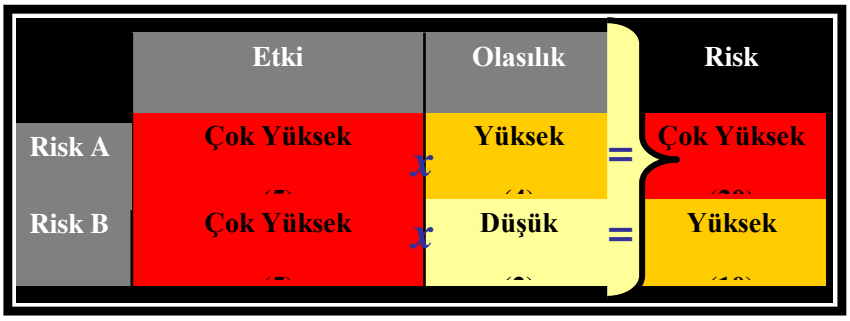
Etki x Olasılık Skoru	Risk Skoru
15 – 25	Çok Yüksek
9 – 12	Yüksek
5 – 8	Orta
1 - 4	Düşük

Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 76.

Tablo 5'de yer alan örnek Risk Skoru Hesaplamasında Risk A 5*4=20 olarak çıkmıştır. 20 "Risk Skoru Hesaplama Tablosuna göre "15-25" aralığında olduğu için "Çok Yüksek" değerindedir.

Risk B ise 5*2=10 olarak çıkmıştır. 10, "Risk Skoru Hesaplama Tablosuna göre "9-12" aralığında olduğu için "Yüksek" değerindedir.

Tablo 6. Örnek Risk Skoru Hesaplaması



Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 77.

İşe etki ve Olasılık değerlerinin çarpımı sonucu hesaplanan risk skoru "Tablo 5 Risk Haritasında hangi renk aralığına denk geldiği görülebilir. Burada yatayda eksenden etki değeri, düşey eksenden olasılık değeri bulunarak bu iki değerin kesiştiği alanda risk skorunun denk geldiği renk değeri görülür. Örneğin İşe etki

değeri 5, olasılık değeri 2 olan risk için risk skoru 10 dur ve Risk Haritasında Risk B (Turuncu) alana denk gelmektedir.

Tablo 7. Risk Haritası (Etki ve Olasılık)

RİSK ETKİ-OLASILIK TABLOSU (RİSK HARİTASI)						
O L A S I L I K (Oluşma Olasılığı)	Çok Yüksek **(5)**					
	Yüksek **(4)**					Risk A
	Orta **(3)**					
	Düşük **(2)**					Risk B
	Çok Düşük **(1)**					
RİSK ETKİ–OLASILIK TABLOSU (RİSK HARİTASI)		Çok Düşük **(1)**	Düşük **(2)**	Orta **(3)**	Yüksek **(4)**	Çok Yüksek **(5)**
		E T K İ				

Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 77.

1.2.2.İkinci Adım: Risklerin Önceliklendirilmesi

a) Skorları hesaplanan risklerin sıralanması

b) Kabul edilebilir risk seviyesinden yukarıda değere sahip risklerin belirlenmesi

Risk değerleri hesaplandıktan sonra riskler aldıkları değerlere göre sıralanarak kabul edilebilir risk seviyesinden (8) daha yüksek seviyede olan riskler belirlenir.

1.2.3.Üçüncü Adım: Risklerin Yönetimi ve Kontrolü

a) Her bir risk için risk yönetim yaklaşımının belirlenmesi.

Riskler belirlendikten sonra onlara karşı yapılabilecekler yetkili kişiler tarafından değerlendirilir ve hayata geçirilir. Bunu yaparken uygun kontrol süreçlerini takip etmek için yöneticiler birçok değişkeni göz önüne almalıdırlar. Organizasyonun iş

hedefleri, kalite beklentileri, teknik gereksinimleri, zaman, emniyet ve güvenirlik gibi unsurlar göz önünde bulundurulmalı (NIST, 1997).

Kabul edilebilir risk seviyesinden (8) yüksek risk değerine sahip riskler kabul edilemez, yönetim metodu olarak transfer, riskten kaçınma ya da riski azaltma seçeneklerinden biri uygulanmalıdır ("Riskin azaltılması", "Riskin transfer edilmesi", "Riskten kaçınma", "Riski kabullenme") Risklere uygulanan yönetim yaklaşımı riskin kabul edilebilir seviyeye indirgenmesini sağlar. Bunun için birden fazla kontrol veya birden fazla yaklaşım uygulanması tercih edilebilir. Riskin kabul edilebilir seviyeye inememesi durumlarında yeni yapılacak kontrol ve aksiyonlar için riskler gözden geçirilir.

b) Kabul edilebilir risk seviyesinin (8) üzerinde skora sahip riskler ile ilgili kontrol planlarının en yüksek puanlı riskten başlayarak yapılması

1.2.4.Kalan risklerin Yönetilmesi

Kurumun üst yönetimi tarafından kabul edilebilir risk seviyesi örneğin ;"8" olarak belirlenmesi dolayısıyla, skoru 9 ile 25 arasında yer alan risklerin yönetilmesi ve kabul edilebilir seviyeye çekilmesi sağlanır.

Risk skoru 1 ile 8 arasında olan ya da uygulanan kontroller sonucunda bu aralığa düşen artık riskler yönetime sunulur ve bu risklerle beraber yaşamak için yönetim onayı alınır.

Tablo 8. Artık Risklerin Yönetilmesi

Etki * Olasılık Skoru	Riski Onaylayan Yönetici Seviyesi
9-12	Müdür
15-16	Birim Yöneticisi
20	Genel Müdür Yardımcısı
25	Genel Müdür

Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 77.

1.2.5.Risk Değerlendirme Tablosu

Bilgi güvenliğine yönelik risklerin yönetimi kurumların ortak erişim alanlarında ulaşılan uygulamasından takip edilir.

Bu uygulamada kullanılanacak alanlar ve açıklamaları aşağıdaki gibi olması uygundur.

Tablo 9. Risk Değerlendirme Tablosu

ALAN ADI	ALAN AÇIKLAMASI
RİSK AYRINTILARI	
Zafiyet Kategorisi	Zafiyetin ait olduğu kategori
Zafiyet	Bir varlığı tehditlere karşı korumasız hale getiren zayıflıklara ait bilgi (Örnek: kilitsiz ortamda varlığın saklanması, parolaların herkesle paylaşılması vb. gibi)
Zafiyete bağlı risk	Zafiyetin oluşturabileceği risk
Tehdit	Bir varlıktaki zayıflıkları kullanarak varlığa kısmen ya da tamamen zarar veren etkenlerdir (Örnek: yetkisiz erişim, çalınma, vb.)
Riskin açıklaması	Zayıflık sonucu gerçekleşen tehdidin yaratacağı sonuç (Örnek: şirketin finansal zarar görmesi, bilgilerin ifşa olması vb.)
Risk Etkisi	Mevcut zafiyetle birlikte tehdidin ortaya çıkması durumunda riskin işe olan etkisi bilgisi (5li skala)
Risk Olasılığı	İlgili riskin bulunması olasılığı
Risk Seviyesi	İş etki ve olasılık değerlerinin çarpımı sonucundaki skor değeri bilgisi
Risk çözüm yaklaşımı	Riskin Kabul edilebilir seviyede olup olmadığı bilgisi (Kabul edilebilir seviyede ise "Kabul Et(Otomatik)", değilse "Yönet", "Kabul Et", "Transfer Et" seçeneklerinden biri seçilir.)
Riskin geldiği kaynak	Risk Analizi, İç Denetim, Dış Denetim gibi seçeneklerden biri seçilir.
AKSİYON BİLGİLERİ	
Aksiyon Adı	Kabul edilebilir seviyeye indirilmesi ya da yapılması gerekenler ile ilgili aksiyon bilgisi
Açıklama	Aksiyon ile ilgili açıklama
İş Yükü	Bu aksiyonun yapılması için oluşacak iş yükü
Tahmini Maliyet	Bu aksiyonun yapılması için gerekli tahmini bütçe
Sorumlu	Aksiyonu hayata geçirecek olan bölüm/birim
Son Tarih	Aksiyonun gerçekleşmesi gereken son tarih
Etkinlik Açıklaması	Risk skorunun azalmasına sebep olan etkinlik durumu açıklanabilir.
Aksiyon Durumu	Aksiyona başlanıp başlanmadığı, başlandı ise ne kadar ilerlendiği bilgisi
İLİŞKİLİ RİSK-KONTROL	
Aksiyon sonu risk olasılığı	Aksiyon alındıktan sonra oluşan revize olasılık değeri
Kontrol	ISO 27001 Standartındaki ilgili kontrol maddesi

Kaynak: Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı**, ODTU Yayıncılık, Ankara, 2012, 77.

2.Risk Aksiyon Planları

Risk aksiyon planı, belirlenen riskleri ortadan kaldırmak amacıyla organizasyonun tercih ettiği çözümlerden oluşur. Risk aksiyon planları tamamlandıktan sonra oluşacak muhtemel diğer risklere karşı da çözümler aranır. Bu risklerle daha iyi başa çıkmanın etkili bir yöntemidir. (Safe church Training Agreement, Towards Safer Churches, 2009).Riskleri kabul edilebilir seviyeye indirmek için belirlenen aksiyonlar İş Sahipleri ya da Bilgi Güvenliği Sorumlusu tarafından kurum BGYS sistemine eklenir ve aksiyonların gerçekleştirilmesine yönelik planlar oluşturulur. Planlar oluşturulurken, aksiyonların şirket içinden ya da dışından ilgili sorumluları da belirlenir. Aksiyonlar, Bilgi Güvenliği Sorumlusu tarafından ilgili sorumlularla paylaşılır ve bu aksiyonları gerçekleştirmek için yapılması gerekenler belirlenerek, planlama yapılır.

Aksiyonlar için yapılan bu planlar, Üst Yönetim tarafından değerlendirilir ve riskleri kabul edilebilir seviyeye indirmek, ortadan kaldırmak veya ilgili taraflara aktarmak/transfer etmek için gerekli çalışmalara başlanır. Üst Yönetim tarafından kabul edilebilir risk seviyesinin üzerinde çıkan risklerin düşürülmesi için gerekli aksiyonların alınması ve riskin kabul edilebilir seviyeye düşürülmesi hedeftir. Ancak riskin kabul edilir seviyeye indirilmesi için yapılması gerekli olan bazı aksiyonlar için Üst Yönetim bütçe, kaynak vb. ayıramayabilir ve bir süreliğine bu riskle yaşamayı kabul edebilir. Bu durumda aksiyon sahibinin yöneticisi tarafından kurumun BGYS sisteminde ilgili varlık için “Risk çözüm yaklaşımı” olarak “Kabul et” seçeneği seçilir ve gelen Risk Kabul İsteği sayfasında “Riskin kabul edilmesine yol açan iş gereksinimleri”, “Riskin kabulünün olası etkileri”, “Riskin gerçekleşmesini önlemek için yapılacaklar”, ve “Geçerlilik/Kontrol tarihi,” alanları doldurularak kaydedilir. Bu formlar kurumun BGYS sisteminde kayıt altında tutulur ve dönemsel kontrollerle risk durumu kontrol edilir. Bu tür aksiyonlar için ayrıca ilgili taraflarla birlikte alternatif yapılabilecekler de düşünülür.

ALTINCI BÖLÜM
GENEL KABUL GÖRMÜŞ DENETİM KONTROL VE UYGULAMA YÖNTEMLERİ

1.Genel Kabul Görmüş Denetim Modelleri

ISO/IEC 27001, BGYS çalışmalarında kullanılacak olan genel standartları içerir. Bilgilerin tehditle karşılaşması durumunda bunları tespit eder ve çalışmaları bu yöne yöneltir. Ayrıca bu tarz olumsuz sonuçları minimize etmek için çeşitli çalışmalar yapar. BGYS bilgileri kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için ISO/IEC 17799:2005 standardındaki kontrolleri uygular (Vural ve Sağıroğlu, 2008, 195).

1.2.BS7799 / ISO17799 / TS 17799 Güvenlik Standardı

ISO 17799, bilgi güvenliği yönetimi için uygulama prensiplerinin ortaya konulduğu dünyada kabul görmüş bir standarttır. ISO 17799 standardı bir kurumda bulunması gereken güvenlik önlemlerine yer vererek temel bir güvenlik çerçevesi çizer.

2002 senesinde çıkartılan BS 7799-2 (Bölüm 2) standardı ile ortaya konan kullanım kılavuzu ile kurumların ISO 17799 sertifikasyonu alması hedeflenmiştir. TSE, ISO 17799'u 2002 senesinde BS 7799-2'yi ise Şubat 2005'te Türkçe olarak yayınlamıştır. Yayınlanan BS7799 standardı organizasyon açısından önemli bir yeri olan bilgi güvenliği yönetimi sürecini açıklayan, tanımlayan ve bunlarla ilgili yönlendirici bilgiler içeren bir standarttır. Bu anlamda aşağıdaki 3 temel prensip çok önemlidir (Mandacı 2003, 94):

- Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi.
- Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesi.

- Elverişlilik: Yetkilendirilmiş kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin garanti edilmesi.

COBIT ve ISO 17799 içeriklerinin karşılaştırıldığı ilişki aşağıdaki Tablo 10'da görülmektedir.

Tablo 10. COBIT & ISO17799 ilişkisi

COBIT	**ISO 17799**
Kurumsal yönetişim	Bilgi güvenliği odaklı
İş strateji ve süreçlerinin değerlendirilmesi	Bilgi güvenliği standardı
Ölçüm yöntemi	Güvenlik kontrollerinin değerlendirilmesi

Kaynak:http://www.bddk.org.tr/WebSitesi/turkce/Basel/Basel_II.aspx Sarbanes Oxley, Erişim:26/07/2014.

Sarbanes-Oxley Yasası, 30 Temmuz 2002'de yürürlüğe girmiş olan, Özel Şirketler Muhasebe Yeniden Düzenlemesi ve Yatırımcının Korunması Yasası olarak da bilinen bir ABD federal yasasıdır. Amerika'da 2004 yılında uygulanmaya başlayan bu yasa aslında organizasyon paydaşlarını koruma amacıyla borsaya kayıtlı şirketlerin yönetimine ve çalışanlarına bir takım kural ve uygulamalar getiren bir yasadır. Bu yasa organizasyon içinde birçok işlemin ve iletişimin kayıt almasını gerektirir. Bunlara örnek olarak mailler, telefon görüşmeleri ve işlem kayıtları verilebilir. Amerika'da geliştirilen ve sadece oradaki organizasyonlar tarafından kullanılan SOX(Sarbanes-Oxley) yasasının global olarak bir çok organizasyon geçerliliğin olması beklenmektedir. Bu yasa SEC diye bilinen Amerika Menkul Kıymetler ve Borsa Kurulu'na ilave yetkiler ve sorumluluklar vermektedir. (Mandacı 2003, 103). Sarbanes-Oxley Yasasının başlıca hükümleri aşağıda belirtilmektedir: (British Standards Institute, 2005, 750- 780)

- Finansal raporların Genel Müdür ve Finans Müdürü tarafından tasdik edilmesi

- Tüm Yönetici ve Müdürlere kişisel kredinin yasaklanması

- İçeriden alınan bilgilerle hisse senedi alışverişinde bulunanların hızlandırılmış raporlanması

- Emeklilik fonlarını karartma zamanlarında içeriden alınan bilgilerle hisse

senedi alışverişinde bulunmanın yasaklanması

- Genel Müdür ve Finans Müdürü'nün tazminat ve karlarının halka açıklanması

- Denetim bağımsızlığı; bazı tür işlerden tamamen men edilmesi ve denetime tabii olmayan tüm işlerin Denetim Komitesi tarafından önceden tasdiklenmesi

- Menkul Kıymetler Yasasının çiğnenmesi için kriminal ve medeni cezalar verilmesi

- Bilerek ve isteyerek finansal tablolarını farklı gösteren şirket yöneticileri için çok daha uzun hapis cezaları ve büyük tazminat bedelleri uygulanması

- Müşterilerine hukuksal ve ya danışmanlık gibi denetim işleriyle ilgisi olamayan ekstra 'katma değerli' hizmetler sunan denetim firmalarının yasaklanması

- Halka açık firmaların finansal raporlama ile ilgili iç denetimlerinin varlığı ve durumuyla ilgili yıllık bağımsız raporlar vermeleri gereksinimi PCAOB (Özel Şirketler Muhasebe Gözetim Kurulu)'un Gereksinimleri

- Finansal tablolardaki belli başlı hesaplar ve açıklamalarla ilgili uygun teyitlerin kontrolünün planlanması

- Belli başlı hareketlerin nasıl başladığı, yetkilendirildiği, desteklendiği, yürütüldüğü ve raporlandığı hakkında bilgi

- Yanlışlık ya da kasıtlı olarak oluşmuş yanlış beyanların yerlerinin saptanması için hareketlerin akışıyla ilgili yeterli bilgi

- Sahtekarlığı önlemek ve saptamak için gerekli kontrollerin oluşturulması (kontrollerin kimin tarafından yapıldığı ve düzenlenmiş görev ayrımlarını da içeren)

- Dönem-sonu finansal raporlama işlevinin kontrolü

- Yönetimin testlerinin ve değerlendirmesinin sonuçları

1.3.COBIT ve Sarbanes Oxley İlişkisi

Bugünün iş çevresinde, kurumlarının çoğunun finansal raporlama süreçleri bilgi teknolojileri sistemlerinden alınmaktadır. Sadece az miktarda kurum verilerini elle yönetmektedir. Kurumların pek çoğu verinin, dokümanların ve anahtar operasyonel süreçlerin elektronik yönetimine geçmiştir. Bundan dolayı, iç denetimde bilgi teknolojilerinin hayati bir rol oynadığı görülmektedir. PCAOB şöyle demektedir (Hansche 2003, 213): "Bir kurumun bilgi sistemleri içinde bilgi teknolojilerini kullanma şekli, içeriği ve özellikleri kurumun finansal raporlama üzerindeki iç kontrolünü etkilemektedir."

Tüm bunları göz önüne alan Sarbanes Oxley finansal veri üretimi ile ilişkisi bulunan BT süreçlerinin COBIT te olduğu gibi denetlenmesini ve kontrol altında tutulmasını öngörmektedir.

1.4. COBIT ve Basel II ilişkisi

Basel Sermaye Uyumu adı verilen Basel II, ikinci Basel Anlaşmadır ve bankanın sermayesinin kifayetini ölçen uluslararası standartları gözden geçirmek için Bankacılık Denetimi üzerine kurulan 13 ülkeden merkez bankacıların oluşturduğu Basel Komiteyi temsil etmektedir. Basel II Basel II, operasyonel risklerin tanımlanması, değerlendirilmesi ve ölçülmesi için geliştirilmiş bir kurallar bütünüdür. Basel II, bankaların ve bankacılık düzenleyicilerinin ulusal sınırlar arasında risk yönetimine yaklaşım yöntemlerindeki tutarlılığı yükseltmek için yaratılmıştır. Yüksek standartlara sahip olan Basel II'ye uyum sağlamak için bankaların pek çok gerekliliği. yerine getirmesi gerekmektedir. (http, s.//www.bddk.org.tr/WebSitesi/turkce/Basel/Basel_II.aspx, Erişim: 28.07.2014)

"Basel II serbest rekabet ortamı ve risklere yönelik daha ayrıntılı çalışmalar yapma ve bunları yaparken finansal sistemin güvenirlik ve istikrarını arttırarak organizasyonları hedeflerine ulaştırma amacıyla hazırlanmıştır. Bu uzlaşıda - Kredi Riski - Operasyonel Risk - Riski Azaltma – Teminat bölümleri yer almakta olup Basel I uzlaşısında yer alan sermayeyle ilgili kısımlarda çeşitli düzenlemeler

yapılmıştır. Kredi riskine dair yeni hesaplamalar sunmakta ve operasyonel riski sermaye yeterliliği hesaplamasına dahil etmektedir" (Aykut 2008, 30)

Aşağıdaki tabloda Basel II olay çeşitlerinin COBIT kontrol hedeflerinden hangilerine karşı geldiği görülmektedir. BDDK' nın bilgi sistemleri denetim metodolojisi olarak COBIT seçmesinin nedenlerinden biriside bu uyumdur.

Tablo 11. COBIT ve Basel II İlişkisi

Basel II Olay Çeşitler	**BT ile ilgili alanlar**	**COBIT Kontrol Hedefleri**
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 dokümanları 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 (İK 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 arızalan 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)

Kaynak: http, s.//www.bddk.org.tr/WebSitesi/turkce/Basel/Basel_II.aspx, Erişim: 18.07.2014

2. COSO (Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi)

Amerika Birleşik Devletleri'nde 2002 yılında çıkarılan Sarbanes-Oxley Yasası, kanuna tabi işletmelerden bir iç kontrol yapısını izlemelerini istemektedir. Sarbanes-Oxley Yasasını yürütmekle görevli Menkul Kıymetler ve Borsa Komisyonu (SEC - Securitiesand Exchange Commission) COSO' nun iç kontrol modelini kabul edilebilir bir model olarak görmektedir. Komisyon, COSO' nun öngördüğü yapının, kendi kriterlerini karşıladığı ve yönetimlerin yıllık iç kontrol değerlendirme ve açıklama görevleri için bir değerlendirme aracı olarak kullanılabileceğini açıklamıştır. SEC kuralları yönetimlerden belli bir değerlendirme yapısını kullanmalarını istemese de, SEC, yönetimlerden işletmenin finansal raporlama üzerindeki iç kontrollerinin etkililiğini değerlendirmede hangi yapıyı kullandıklarını belirlemelerini istemektedir. (Perry ve Warner 2005, 52)

COSO modeli içerisinde organizasyonların iç kontrol sistemlerine yönelik bazı standartları barındırır. COSO Modeli denetim sürecine dahil edilmiş bir model olmakla birlikte bunu yaparken İç Denetçiler Enstitüsü tarafından hazırlanan İç Kontrole İlişkin İşletme Raporunun Hazırlanmasında İç Denetçilerin Rolü' başlıklı raporu kaynak alır. Böylelikle organizasyonun etkili işler yapıp iş hedeflerine yaklaşmasını sağlar. Ayrıca güvenilir mali raporlar hazırlayıp mevzuata uyum sağlar (http://www.icdenetimmerkezi.com/bilgibankasi_alt.php?mn=1&p=33, Erişim: 25/08/2014).

COSO Modeli;

- Kontrol Ortamı
- Risk Değerlendirme
- Kontrol Faaliyetleri
- Bilgi ve iletişim
- İzleme olmak üzere 5 unsurdan oluşmaktadır. (http: //www.coso.org/, Erişim: 18.01.2014)

Kontrol Ortamı: Yönetim ve çalışanlar bütün bir örgüt içinde, iç kontrole ve dikkatli bir yönetime yönelik olarak pozitif ve destekleyici bir tavrı geliştiren ortamı oluşturmalı ve sürdürmelidirler.

Risk değerlendirme: Amaçlara ulaşılırken karşılaşılabilecek risklerin tanımlanıp analiz edilmesi ve risklerin ne şekilde yönetilmesi gerektiğine karar vermek için bir temel oluşturulmasıdır.

Kontrol Faaliyetleri: Yönetimin talimatlarının yerine getirilmesini sağlamaya yardımcı olan politikalar ve yöntemlerdir. Kurumun hedeflerine ulaşırken karşılaştığı riskleri işaret etmek için gerekli önlemlerin alınmasını sağlamaya yardımcı olur.

Bilgi ve İletişim: Uygun bilgi, kişilerin sorumluluklarını yerine getirebilmelerini sağlayacak şekilde tanımlanmalı, elde edilmeli ve paylaşılmalıdır. Etkili iletişim, kurumun en altından en üstüne dolaşacak şekilde geniş anlamda gerçekleşmelidir. Tüm çalışanlara iç kontrol sistemindeki rolleri anlatılmalıdır.

İzleme: İç kontrol izlemesi zaman dilimi içindeki performansın kalitesini değerlendirmeli ve denetim ya da diğer inceleme bulgularının derhal çözüme bağlanmasını güvence altına almalıdır.

2.2. COBIT & COSO İlişkisi

COSO' nun geliştirmiş olduğu denetim standartları ile COBIT standartları arasındaki ilişki aşağıdaki tabloda görülmektedir.

Tablo 12. COBIT & COSO ilişkisi

	COBIT	**COSO**
Birincil Takipçiler	Yönetim, kullanıcılar ve BS denetçileri	Yönetim
(Bütünleşme Konsorsiyumu) BK gözüyle	Politikaları, süreçleri, uygulamaları ve organizasyonel yapıları içeren süreçler kümesi	Süreç
BK hedefleri - Organizasyonel	Etkin & Verimli operasyonlar, Gizlilik, Bilginin Uyumluluğu ve Ulaşılabilirliği, Kanun ve düzenlemelerle uyumlu güvenilir finansal raporlama	Etkin &Verimli operasyonlar, Kanun ve düzenlemelerle uyumlu güvenilir finansal raporlama
Bileşenler ve Alanlar	**Alanlar.** Planlama ve Organizasyon Tedarik ve Uygulama Hizmet Sunumu ve Destek İzleme ve Değerlendirme	**Bileşenler.** Kontrol ortamı Risk yönetimi Kontrol eylemleri Bilgi ve haberleşme takibi
Ana Alan	Bilişim Teknolojisi	Sektörün tamamı

Kaynak: http, s.//www.coso.org/ , Erişim: 18.01.2014

2.3. COBIT ve ITIL İlişkisi

BT Altyapı Kütüphanesi ITIL ile COBIT kontrol hedefleri karşılaştırma tablosuna aşağıda yer verilmiştir. COBIT' in yönetime yönelik yaklaşımı ITIL' dan daha farklıdır. Ancak, ikisi de birbirini tamamlamaktadır ve COBIT' in son versiyonu ITIL ile daha da entegre hale gelmiştir. ITIL, BT 'de süreçlere daha odaklıdır. COBIT ise ITIL süreçlerini içerir, ancak olay yönetimini bir üst seviyeye taşıyarak, iş ihtiyaçlarının nasıl karşılanacağını hedef alır. İkisi birlikte uygulandığında ihtiyaçlarının BT ile örtüşmesi sağlanmış olur. Böylece masrafların ölçülmesi ve hizmet seviyeleri ile performans hedeflerinin bütünlüğü daha rahat sağlanmış olacaktır. COBIT en iyi uygulamaları bir araya getirerek BT birimlerine katma değerlerini sunma imkanı tanımaktadır. (Nicho and Cusack 2007, 1).COBIT 'i, ITIL' ın standartlarından ayıran en önemli özelliği tüm BT fonksiyonlarını kapsayan genel bir çerçeve sunmasıdır. Diğer bir deyişle COBIT' in kapsadığı 34 süreci genel olarak incelediğimizde aslında BT yönetimin bir çok alanını kapsamış

oluruz. Yani ITIL' a göre daha kapsamlı ve özet bir çalışmayı 34 süreç altında ele alır (Güneş vd. 2002, 12)

Tablo 13. COBIT & ITIL ilişkisi

ITIL Süreci	Süreç Kontrol	Detay	COBIT Süreci
Hizmet (Seviye) Yönetimi	DS 1	DS 1.0	Hizmet seviyelerini tanımla ve yönet
Hizmet Yönetimi Süreci	DS 1	DS 1.1	SLA çerçevesi
Sürecin Planlanması	DS 1	DS 1.2	SLA lerin görüşleri
Sürecin Uygulanması	DS 1	DS 1.2	SLA ve sözleşmelerin gözden geçirilmesi
Sürecin Devamı	DS 1	DS 1.5	SLA lerin görüşleri
Müşteri Hizmet Anlaşmalarının (SLA) içerik ve hedefleri	DS 1	DS 1.2	SLA lerin görüşleri
Hizmet Yönetimi etkinlik ve verimliliği için Anahtar Performans Göstergeleri (KPI) ve metrikler	DS1	DS 1.4	İzleme ve raporlama
BT hizmetleri için Finansal Yönetim	PO 5	PO 5.0	BT yatırımlarını yönet
Bütçeleme	PO 5	PO 5.1	Yıllık BT yürütüm bütçesi
BT Muhasebe sistemini geliştirme	PO 5	PO 5.1	Yıllık BT yürütüm bütçesi
Sorumluluk yükleme sistemi geliştirme	DS 6	DS 6.2	Maliyetlendirme prosedürleri
BT muhasebe ve yüklemeleri için planlama yapma	DS 6	DS 6.1	Yüklenebilecek bileşenler
Uygulama	DS 6	DS 6.0	Maliyetleri tanımlama ve dağıtma
Süregiden yönetim ve operasyon	DS 6	DS 6.3	Kullanıcı faturalandırma ve geri ödemeleri
Kapasite Yönetimi	DS 2	DS 2.0	3. Parti hizmetleri yönet
Kapasite Yönetim süreci	DS 3	DS 3.0	Performans ve kapasiteyi yönet
Kapasite yönetiminde aktiviteler	DS 3	DS 3.7	Kaynak kapasite yönetimi
Maliyet, fayda ve olası problemler	DS 3	DS 3.7	Kaynak kapasite yönetimi

Kaynak: www.itil-officialsite.com 18.01.2014

COBIT ve Diğer BT Denetimi Kontrol ve Uygulama Yöntemlerinin Kıyaslanması

Tüm BT standart ve yöntemlerinin COBIT kontrol hedeflerinde var olan karşılıklarının dağılım sıklığını aşağıdaki tabloda gösterilmiştir.

Tablo 14. COBIT &Diğer BT Standartları Karşılaştırma Tablosu

	COBIT Proseslerinin Diğer Standartlardaki Karsılıkları												
CobiT Process	COSO	ITIL	ISO/IEC 17799	FIPS PUB 200	ISO/IEC TR 13335	ISO/IEC 15408	PRINCE2	PMBOK	TickIT	CMMI	TOGAF 8.1	IT BPM	NIST 800-14
PO 1	+	-	-	-	-	-	-	-	-	-	-	-	-
PO 2	+	-	+	+	+	-	-	-	-	-	+	-	+
PO 3	+	+	+	+	+	-	-	-	-	-	+	+	+
PO 4	+	+	+	+	+	-	-	-	-	-	+	-	+
PO 5	+	+	-	-	-	-	+	+	-	-	-	-	-
PO 6	+	-	+	+	+	-	-	-	-	-	-	+	+
PO 7	+	-	+	+	-	-	-	-	-	-	-	-	+
PO 8	-	-	-	-	-	+	+	+	+	+	-	-	-
PO 9	+	-	+	+	+	-	+	+	-	+	-	-	+
PO 10	-	-	-	-	-	-	+	+	-	+	-	-	-
AI 1	+	-	-	-	+	-	-	-	+	-	+	-	+
AI 2	+	-	+	+	-	+	-	-	+	+	-	-	+
AI 3	+	-	+	+	-	+	-	-	+	-	-	+	+
AI 4	+	+	+	+	-	+	-	-	+	-	-	-	+
AI 5	-	-	-	-	-	-	-	+	+	-	-	-	-
AI 6	+	+	+	+	+	-	-	-	+	+	-	-	+
AI 7	+	+	+	+	+	-	-	-	+	+	-	-	+
DS 1	+	+	-	-	-	-	-	-	-	-	+	-	-
DS 2	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 3	+	+	+	+	-	-	-	-	-	-	-	-	+
DS 4	+	+	+	+	+	-	-	-	-	-	-	+	+
DS 5	+	+	+	+	+	+	-	-	-	-	-	+	+
DS 6	-	+	-	-	-	-	-	-	-	-	-	-	-
DS 7	+	-	+	+	+	-	-	-	-	+	-	-	+
DS 8	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 9	+	+	+	+	-	-	+	-	-	+	-	-	+
DS 10	-	+	-	+	-	-	-	-	-	+	-	-	+
DS 11	+	+	+	+	+	+	-	-	-	+	-	+	+
DS 12	+	-	+	+	+	+	-	-	-	-	-	+	+
DS 13	-	-	+	-	-	-	-	-	-	-	-	-	+
ME 1	-	-	+	-	-	-	-	-	+	+	-	-	+
ME 2	-	-	+	+	+	+	-	-	+	-	-	+	+
ME 3	+	-	-	-	-	-	-	-	-	-	-	-	-
ME 4	+	-	+	+	-	-	-	-	-	-	-	-	+

(+) Sıkça adreslenen (-)Seyrek / hiç adreslenmeyen

Kaynak: www.itgi.org , Erişim:20/07/2014

YEDİNCİ BÖLÜM
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN BİR FİNANS KURUMU ÜZERİNE UYGULANMASI

1.Uygulamanın amacı

Bu uygulamanın amacı, şirketin bilgi güvenliği ihtiyaçlarını yönetmek için üst yönetimin onayı ile oluşturulan bilgi güvenliği yönetim sisteminin işletilmesiyle, tüm servis ve servis yönetim aktivitelerinde bilgi güvenliği politikalarının efektif bir şekilde yönetilerek bilgi varlıklarının risklere karşı güvenliği, doğruluğu ve sürekli kullanılabilirliğini, COBIT, ITIL ve ISO/IEC 27001 uyumluluğu altında sağlamayı amaçlamıştır. Bu kapsamda süreçler belirlenmiş ve sonrasında BGYS (ISO 27001) iç denetimi gerçekleştirilmiştir.

Süreçler direkt olarak bütün şirket yönetim kademelerini ve çalışanlarını, bölümleri, mevkileri, rolleri, teknolojileri, stratejileri, hedefleri, süreçleri, aktiviteleri, operasyonları, kararları, yatırımları, programları, planları, projeleri, ürünleri, hizmetleri, varlıkları ve bilgi sistemleri ile ilgili iç ve dış hizmet ve teknoloji sağlayıcılarını kapsamaktadır.

1.1. Kurum Profili

Uygulama yurtiçi ve yurtdışı alanda finansal faaliyeti gerçekleştiren bir bankanın bilişim teknolojileri departmanında gerçekleştirilmiştir. Kurumun yurt içinde 900 civarında şubeleri üzerinden müşterilerine hizmet vermektedir.

Güvenlik sebeplerinden dolayı kurum ismine araştırmada yer verilmemiştir.

1.2.BGYS Süreç Metodolojisi :

Şekil 7. BGYS Süreç Metodolojisi

1.3.Kapsamın tanımlanması:

Kurum bilgi iletişim teknolojileri fonksiyonunun, insan, süreç, bilgi ve altyapı sistemlerinin tamamını kapsayan Bilgi Güvenliği Yönetim sistemi kurulmuştur. Bilgi Teknolojileri servis politikasına uygun olarak gerçekleştirilen yeni ve mevcut hizmet ve ürünlerin geliştirilmesi, uyarlanması, değerlendirilmesi ve süregelen aktiviteleri yönetimi BGYS 'nin kapsamındadır. Yapılan çalışma Bilgi Teknolojileri bünyesinde bulunan tüm departmanlar ve bu departmanların bulunduğu tüm lokasyonları kapsamaktadır.

1.4.Süreç Prosedür Dokümanlarının Hazırlanması

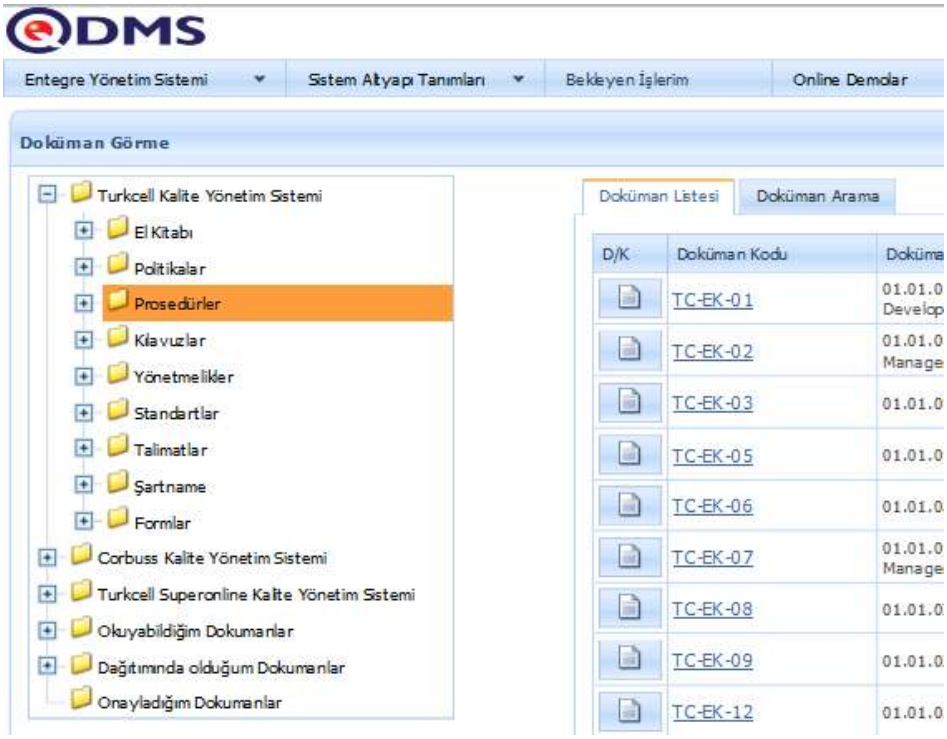
Bilgi Güvenliği Süreç prosedürleri tanımlanırken ISO 27001, COBIT ve ITIL standartları referansları gösterilmiştir. Tanımlanan süreç prosedürleri formatı aşağıdaki gibidir. Süreç prosedürleri kurumun QDMS (bkz. 7.6) sisteminde Tablo 15'deki formata uygun olarak tanımlanmıştır.

Tablo 15. Süreç Prosedürü Doküman Formatı

Şirket Logosu ve İsmi **Bilgi Güvenliği Süreç Prosedürü**		Doküman Kodu: Tarih Revizyon No:
1.Amaç		
2. Kapsam		
3. Tanımlar		
4. Kullanılan Standart Formlar		
5. Refere Dokümanlar		
6. Uygulama		
7.İş Akışı		
8. Revizyon Nedeni		
9. Gözden Geçirme		
Hazırlayan	Onaylayan	Yayınlayan

1.5.QDMS Sistemi:

QDMS uygulaması şirketin kalite dokümanlarının elektronik olarak güvenli yönetilmesi ve doküman bazlı iş akışlarının yürütülmesi amacı ile kullanılmaktadır.



Şekil 8. QDMS Sistemi

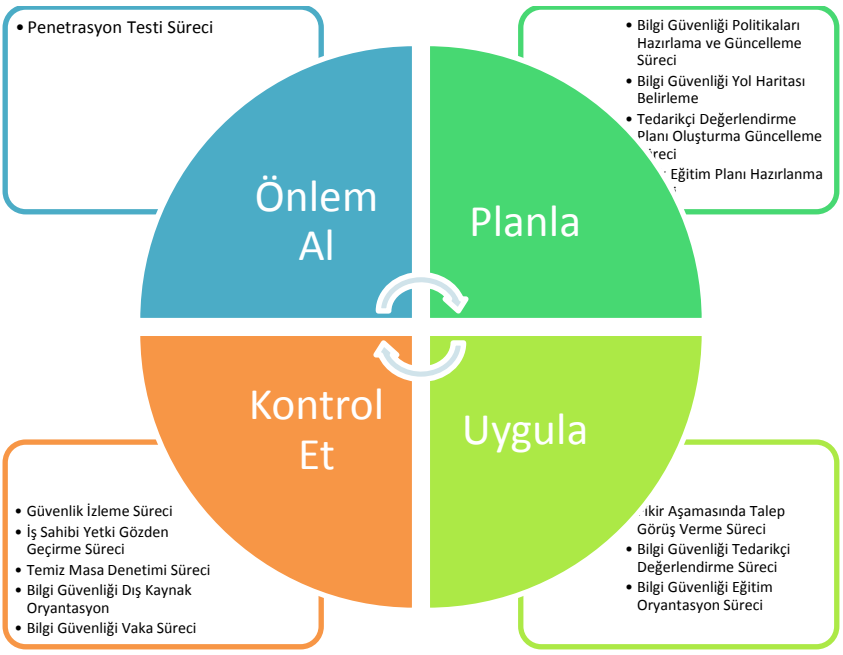
2.BGYS Sistemi

Kurumun bilgi güvenliği sistemin takip edildiği yine kurum bünyesinde yer alan web tabanlı arayüzdür. Bu arayüzde kurumun bilgi güvenliği varlıkları ve varlıkların risk analizlerinin yapıldığı ilgili kurum çalışanlarının erişebildiği ortak alandır. Bu sisteme kurum çalışanların http://bgys adresi ile ulaşabilmekte ve ilgili sorumlu oldukları varlıklarının envanterini ve risk analizlerini bu alandaki dokümalar üzerinde yapmakla yükümlüdürler.

2.1.Şirket Bünyesinde Oluşturulan Bilgi Güvenliği Yönetim Süreçleri

- Bilgi Güvenliği Politikaları Hazırlama ve Güncelleme Süreci
- Fikir Aşamasında Talep Görüş Verme Süreci
- Tedarikçi Değerlendirme Planı Oluşturma Güncelleme Süreci
- Bilgi Güvenliği Tedarikçi Değerlendirme Süreci
- Penetrasyon Testi Süreci
- Güvenlik İzleme Süreci
- Bilgi Güvenliği Eğitim Oryantasyon Süreci

- Bilgi Güvenliği Dış Kaynak Oryantasyon
- İş Sahibi Yetki Gözden Geçirme Süreci
- Bilgi Güvenliği Vaka Süreci
- Yıllık Eğitim Planı Hazırlanma Süreci
- Temiz Masa Denetimi Süreci
- Bilgi Güvenliği Yol Haritası Belirleme



Şekil 9. BGYS Süreç Döngüsü

Kaynak: https://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/neden-bgys-3.html, 15.08.2014

BGYS süreç döngüsü aşamalarına göre sınıflandırılan süreç dokümanları Bilgi Güvenliği standartlarındaki (ITIL, COBIT ve ISO) kontrol maddelerine göre oluşturulmuş ve QDMS sistemine yüklenmiştir.

2.1.1.Planla

BGYS ‘nin ilk aşaması planlamadır. Planlama sürecindeki süreçler Tablo 16 ‘daki gibidir.

Tablo 16. BGYS Planla Aşaması Süreçleri

PLANLA	
SÜREÇ	**REFERANS**
Bilgi Güvenliği Politikaları Hazırlama ve Güncelleme Süreci Tüm şirketi kapsayacak şekilde bilgi güvenliği politikalarını belirlenmesini, yayınlanmasını ve güncelliği yansıtacak şekilde revize edilerek yayınlanmasını ve değişiklik ile ilgili bilgilendirme yapılmasını hedefler.	• ITILv3 SD 4.6.4 Politikalar / İlkeler/ Temel /Kavramlar • ITIL V3 SD 4.6.5.1 Güvenlik Kontrolleri • COBIT DS5.2 IT Güvenlik Planı • ISO/IEC 27002:2005 5.1.1 Bilgi Güvenliği Politika Belgesi • ISO/IEC 27002:2005 5.1.2 Bilgi Güvenliği Politikalarını Gözden Geçirme • ISO/IEC 27002:2005 6.1.2 Bilgi Güvenliği Koordinasyon
Bilgi Güvenliği Yol Haritası Belirleme Belirlenen fonksiyon ve grup şirketler ile yıl içinde takip edilecek strateji, gündem, projelerin belirlenerek uygulamaya konulmasının sağlanmasını hedefler.	• COBIT DS5.2 IT Güvenlik Planı • ITIL V3 SD 4.6.4 Politikalar / İlkeler/ Temel /Kavramlar • ISO/IEC 27002:2005 A.6.1.2 Bilgi Güvenliği Koordinasyon
Tedarikçi Değerlendirme Planı Oluşturma Güncelleme Süreci Satın alma, İş Birimleri tarafından iletilebilecek ya da Bilgi Güvenliği tarafından doğrudan eklenerek yıl içinde değerlendirmeye dahil edilecek tedarikçilerin belirlenmesini hedefler.	• COBIT DS2.3 Tedarikçi risk yönetimi • COBIT ME2.6 Üçüncü Taraflarda İç Kontrol • ITIL V3 SD 4.7.5.3 Yeni tedarikçiler ve sözleşmelerinin oluşturulması • ITIL V3 SD 4.7.5.5 Kontrat yenileme ve / veya sonlandırma • ISO/IEC 27002:2005 6.2.1 Dış kaynaklara ilişkin risklerin tanımlanması • ISO/IEC 27002:2005 6.2.3 Dış kaynak güvenlik sözleşmesini belirleme
Yıllık Eğitim Planı Hazırlanma Süreci Yıl içinde verilecek eğitim planının belirlenerek buna göre kaynak planı yapılmasını hedefler.	• COBIT DS7.1 Eğitim ve Öğretim Gereksinimlerinin Tanımlanması • COBIT PO7.4 Personel Eğitimi • ISO /IEC 27002:2005 8.2.2 Bilgi Güvenliği farkındalığı, eğitim ve öğretim

2.1.2.Uygula

Planlanan BGYS süreci uygulanmak üzere süreçlere oturtulur.

Tablo 17. BGYS Uygula Aşaması Süreçleri

UYGULA	
SÜREÇ	**REFERANS**
Fikir Aşamasında Talep Görüş Verme Süreci İş Birimleri tarafından projelendirilmiş, henüz projelendirilmemiş ya da projelendirilmeyecek konular için iletilen görüş alma taleplerine karşılık bilgi güvenliği politikalarına uygunluğun değerlendirilmesini hedefler. Uygunluğu sağlayacak öneri ve yorumların uygulanabilirliğini teyit ederek plana/projeye dahil edilmesini ya da Risk Bulgu Kayıt sürecini tetiklemesini sağlar.	• COBIT DS5.2 IT Güvenlik Planı
Bilgi Güvenliği Tedarikçi Değerlendirme Süreci Tedarikçi Değerlendirme Planına uygun olarak belirlenen tedarikçilerin ISO 27001 standartları, tedarikçi ile yapılan sözleşme koşulları kapsamında yerinde ziyaret ile değerlendirilmesini hedefler. Değerlendirme öncesi İş birimi ve ilgili paydaşlar ile hazırlık yapılması, değerlendirme sırasında bulguların sözlü olarak, ardından yazılı rapor olarak yayınlanmasını ve bulguların takibinin yapılmasını kapsar.	• COBIT DS2.3 Tedarikçi risk yönetimi • COBIT ME2.6 Üçüncü Taraflarda İç Kontrol • ITIL V3 SD 4.7.5.3 Yeni tedarikçiler ve sözleşmelerinin oluşturulması • ITIL V3 SD 4.7.5.5 Kontrat yenileme ve / veya sonlandırma • ISO/IEC 27002:2005 6.2.1 Dış kaynaklara ilişkin risklerin tanımlanması • ISO/IEC 27002:2005 6.2.3 Dış kaynak güvenlik sözleşmesini belirleme
Bilgi Güvenliği Eğitim Oryantasyon Süreci Yıllık Eğitim Planın kapsamında çalışanların Bilgi Güvenliği ile ilgili eğitim ve farkındalığın ilgili eğitim birimleri ile planlama ve sağlama faaliyetleri sağlar. Yeni işe başlayan çalışanlara verilen oryantasyonu kapsadığı gibi mevcut çalışanların farkındalığını korumaya yarayacak iç ya da dış kaynaklar ile sağlanabilecek tüm eğitim faaliyetlerini kapsar.	• COBIT DS7 Kullanıcıların Eğitimi ve Öğretimi • COBIT PO7.4 Personel Eğitimi • ITILV3 SO 5.13 Bilgi güvenliği yönetimi ve servis operasyon • ISO /IEC 27002:2005 8.2.2 Bilgi Güvenliği farkındalığı, eğitim ve öğretim

2.1.3.Kontrol Et

Uygulanan süreçler izlenmeli ve denetlenmelidir. Bu kapsamda Kontrol süreçleri tanımlanmıştır.

Tablo 18. BGYS Kontrol Et Aşaması Süreçleri

KONTROL ET	
SÜREÇ	**REFERANS**
Güvenlik İzleme Süreci Belirlenen SOX kritik uygulamalarda yapılan veritabanı kullanıcı hesabı ile erişim, kritik işlemler ve müşteri özeli uygulamalarda yapılan veritabanı sorgu işlemlerinin ile gizli dosya paylaşımlarının ve mail sunucu üzerinde manuel olarak yapılan işlemlerin uygunluğunun değerlendirilmesini hedefler. Uygunsuz bulunan durumlarda Etik Vaka süreci, Bilgi Güvenliği Vaka Yönetim süreci ve güvenlik güvence komitesi süreçlerinin tetiklenmesini sağlar.	• COBIT ME2 Dahili İzleme ve Değerlendirme • COBIT DS5.5 Güvenlik Testi, Gözetim ve Gözlem • ITIL V3 SD 4.2.5.10 Şikayetler ve Övgüler • ITIL V3SO 4.5.5.5 Erişimleri izleme ve kayıt altına alma • ISO/IEC 27002:2005 6.1.8 Bilgi güvenliğinin bağımsız gözden geçirilmesi • ISO/IEC 27002:2005 10.10.2 Sistem kullanımını izleme • ISO/IEC 27002:2005 12.5.4 Bilgi sızması
İş Sahibi Yetki Gözden Geçirme Süreci SOX kritik uygulamaların teknik sahipleri tarafından yetkilerin düzenli olarak gözden geçirilmesi ve düzenlenmesini hedefler.	• COBIT DS5.4 Kullanıcı Hesabı Yönetimi • ITILV3 SO 4.5.5.6 İzinleri kaldırma veya kısıtlama • ISO/IEC 27002:2005 11.2.4 Erişim haklarının gözden geçirilmesi
Temiz Masa Denetimi Süreci Kurum çalışanlarının temiz masa temiz ekran kurallarına uyduğunun mesai saatleri sonrası kontrolünün yapılarak kullanıcıların bu konuda farkındalığını arttırmayı hedefler.	• COBIT DS5.7 Güvenlik Teknolojisinin Korunması • COBIT PO6 Yönetim Hedefleri ve Yönünü Bildirme • COBIT DS5 Sistem Güvenliğinin Sağlanması • ISO /IEC 27002:2005 11.3.3 Temiz masa ve temiz ekran politikası
Bilgi Güvenliği Dış Kaynak Oryantasyon İş birimleri tarafından iletilen talepler doğrultusunda Dış Kaynak çalışanlara verilecek oryantasyonla Bilgi Güvenliği ile ilgili farkındalık kazanmasını hedefler.	• COBIT DS7 Kullanıcıların Eğitimi ve Öğretimi • COBIT PO7.4 Personel Eğitimi • ITILV3 SO 5.13 Bilgi güvenliği yönetimi ve servis operasyon • ISO /IEC 27002:2005 8.2.2 Bilgi Güvenliği farkındalığı, eğitim ve öğretim
Bilgi Güvenliği Vaka Süreci Bilgi Güvenliği politikaların ihlali sonucu oluştuğu iletilen vakaların analiz edilerek ihlalin ortadan kaldırılması için gerekli aksiyonun alınmasın ve durumun raporlanmasını hedefler.	• ITILV3 SD 4.6.5.2 Güvenlik ihlalleri ve olayların yönetimi • COBIT DS5.6 Güvenlik Olayı Tanımı • ISO/IEC 270001 A.13.1 Bilgi güvenliği olaylarının raporlanması • ISO/IEC 270001 A.13.2 Bilgi güvenliği ihlal olayları ve iyileştirmelerin yönetilmesi

2.1.4.Önlem Al

Kontrol et aşamasındaki bulguların önlenmesi için önlem alma süreçleri tanımlanmıştır.

Tablo 19. BGYS Önlem Al Aşaması Süreçleri

ÖNLEM AL	
SÜREÇ	**REFERANS**
Penetrasyon Testi Süreci Şirket bünyesindeki sistemler ve süreçlerdeki güvenlik açıklarının tespit edilmesi ve bu açıkların giderilmesi için aksiyon alınmasını hedefler. Test seçilen bir dış kaynağa yaptırılabileceği gibi iç kaynak tarafından da yapılabilir. Kritik açıklık tespit edilmesi durumunda Risk Bulgu Kaydı sürecinin tetiklenmesini sağlar.	• COBIT DS5.5 Güvenlik Testi, Gözetim ve Gözlem • COBIT AI3.3 Altyapının Bakımı (Sürdürülmesi) • COBIT AI6.2 Etki Değerlendirmesi, Önceliklendirme ve Yetkilendirme • COBIT DS5.7 Güvenlik Teknolojisinin Korunması • COBIT DS9.2 Konfigürasyon Maddelerinin Tanımlanması ve Korunması • ITIL V3 SO 4.5.5.6 İzinleri kaldırma veya kısıtlama • ITIL V3 SO 5.13 Bilgi güvenliği yönetimi ve servis operasyon • ISO/IEC 27002:2005 12.6.1 Teknik açıkların kontrolü

Tanımlanan süreçler daha sonra örnek olarak aşağıda verilen "bilgi güvenliği vaka süreci" de olduğu gibi detaylandırılarak her bir süreç için roller, aktiviteler ve iş akışları tanımlanmıştır.

2.2.Bilgi Güvenliği Vaka Yönetim Süreci

Bilgi Güvenliği politikaların ihlali sonucu oluştuğu iletilen vakaların analiz edilerek ihlalin ortadan kaldırılması için gerekli aksiyonun alınmasın ve durumun raporlanmasını hedefleyen süreçtir. Vaka yönetimi kurumdaki çalışanlardan oluşan etik komite tarafından değerlendirilir.

2.2.1.Roller ve Aktiviteler

Bilgi Güvenliği vaka yönettimi sürecindeki roller ve alması gereken aksiyonlar aşağıdaki tabloda gösterilmiştir.

Tablo 20. Roller ve Aktiviteler

Roller	Aktiviteler
Bilgi Güvenliği Uzmanı	Bilgi Güvenliği vaka kaydının çalışmak üzere alınması İnceleme yapılması gerektiğinin değerlendirilmesi Kaydı açana bilgi vererek kaydın kapatılması Vakanın detaylı analizinin yapılması Acil müdahale/ hizmetin geçici olarak durdurulması gereken durum gereksinimi var mı değerlendirilmesi Servis Hizmet sahibine ve iş birimine bilgi verilmesi Vakayı iletilenin bilgilendirilmesi Alınacak aksiyonların belirlenerek vaka raporunun yayınlanması Aksiyonların belirlenmesi
Kurum Çalışanı	Bilgi Güvenliği vaka kaydının açılması
Paydaşlar	Vaka kaydına ek veri ve analiz sonuçlarının eklenmesi Vaka kaydının detaylı analizinin yapılması Vakayı ortadan kaldıracak geçici çözümüm uygulanması
Hizmet Süreç Yöneticisi	Hizmet servisin geçici olarak durdurulması Hizmet servisin tekrar devreye alınması

2.2.2.RACI

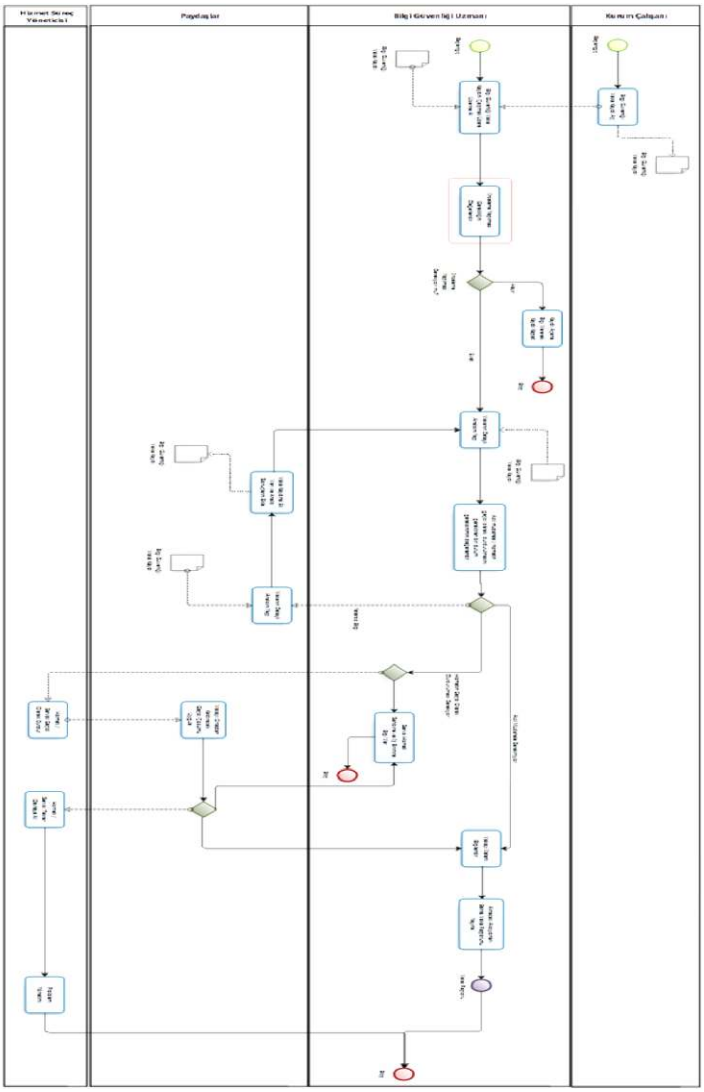
R = (Responsible) İşi yapmakla sorumlu olan kişi, A=(Accountable)İşin yapılması ile ilgili hesap sorulan kişi, C=(Consulted) İşin yapılırken danışılan kişi , I= (Informed) İşin yapılması ile ilgili bilgi verilen kişi.

Tablo 21. RACI Tablosu

Aktiviteler	Bilgi Güvenliği Uzmanı	Paydaşlar	Kurum Çalışanı	Hizmet Yöneticisi
Bilgi Güvenliği Vaka kaydının açılması	**R/I**	**-**	**R/A**	**-**
Bilgi Güvenliği vaka kaydının çalışmak üzere alınması	**R/A**	**-**	**-**	**-**
Kaydı açana bilgi vererek kaydın kapatılması	**R/A**	**-**	**I**	**-**
Vakanın detaylı analizinin yapılması	**R/A**	**-**	**-**	**-**
Acil müdahale/hizmetin geçici olarak durdurulmasını gereken durum gereksinimi var mı değerlendirmesi	**A**	**-**	**-**	**R/A**
Vaka kaydına ek veri ve analiz sonuçlarının eklenmesi	**A**	**R**	**-**	**-**
Vaka kaydının detaylı analizinin yapılması	**A**	**R**	**-**	**-**
Vakayı ortadan kaldıracak geçici çözümün uygulanması	**A**	**R**	**-**	**R**
Servis hizmet sahibine ve iş birimlerine bilgi verilmesi	**R/A**	**I**	**-**	**I**
Hizmetin servisin geçici olarak durdurulması	**A**	**-**	**-**	**R/A**
Hizmetin servisin tekrar devreye alınması	**A**	**I**	**-**	**R/A**
Vakayı iletenin bilgilendirilmesi	**R/A**	**-**	**I**	**R/A**
Alınacak aksiyonların belirlenerek vaka raporunun yayınlanması	**R/A**	**I/C**	**-**	**I/C**
Aksiyonların belirlenmesi	**R/A**	**R**	**-**	**R**

İş Akış Diyagramı :

Vaka yönetim sürecinin iş akışı çizilerek süreç dokümanına eklenir.



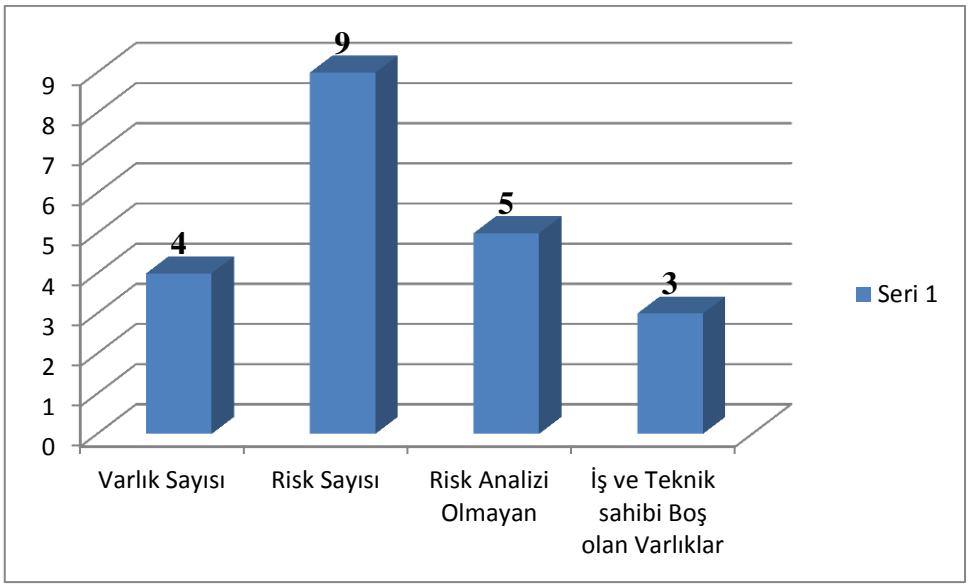
3.ISO 27001 İç Denetimin Yapılması

Bilgi Teknolojileri direktörlüğünde konumlandırılan veri tabanı yönetimi ekibinden ilgili temsilci ile BGYS ISO/27001 iç denetlemesi gerçekleştirilmiştir. Denetleme toplantı ortamında yapılarak bulgular tespit edilip, düzenleyici ve önleyici faaliyetler ilgili temsilciye atanmıştır. Denetim tüm bilgi teknolojileri direktörlüğünde yapılıp olup veri tabanı operasyon ekibi örneklem olarak alınmıştır.

Tablo 22. İç Denetim Formu

Denetlenen Bölüm/Birim: Veri Tabanı Operasyon			
İç Denetçi: Bilgi Güvenliği		**Katılımcılar:** Bilgi Teknolojileri Operasyon Çalışanları	
Denetleme Yeri: İstanbul		**Denetleme Tarihi:** 20 Nisan 2014	
ISO 27001 Kontrol No ve Adı	**Kontrol Açıklaması**	**Bulgular**	**DÖF (Düzeltici ve Önleyici Faaliyet)**
4.2.1 BGYS'nin kurulması	d) Riskleri tanımlama.(Riskler tanımlanmış mıdır? e) Riskleri çözümleme ve derecelendirmesi yapılmış mıdır?	BGYS Varlık envanterinde listelenen bir varlık görülememiştir.	Bazı kurum varlıklarının BGYS 'ye (http://bgys) girişlerinin ve risk analizlerinin yapılması gerekmektedir
4.3.2 Dokümanların kontrolü	d) Uygulanabilir dokümanların ilgili sürümlerinin kullanım noktalarında kullanılır olmasını sağlanmış mı? e) Dokümanların okunaklı ve hazır olarak tanınabilir olmasını sağlanmış mı?	Ekibin kullandığı aşağıdaki dokümanlar ile baz alınan QDMS üzerindeki taslaklar karşılaştırmalı olarak incelendi.	-
A.6.1.5 Gizlilik anlaşmaları	Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da açıklamama anlaşmalarının gereksinimleri tanımlanmalı ve düzenli olarak gözden geçirilmekte midir?	. Bu partilerle gizlilik anlaşmalarının yapılmasının İnsan Kaynakları sorumluluğunda olduğu beyan edildi.Doküman kaydederken Gizlilik opsiyonları çıkmamaktadır	
A.6.1.6 Otoritelerle iletişim	İlgili otoritelerle uygun iletişim kurulmakta mıdır?	BTK ile olan iletişimin Business ekipleri vasıtasıyla yapıldığı beyan edildi.	
A.6.2.2 Müşterilerle ilgilenirken güvenliği ifade etme	Tanımlanmış tüm güvenlik gereksinimleri, müşterilere kuruluşun bilgi ve varlıklarına erişim vermeden önce ifade edilmekte midir?	Müşterilerle birebir temasta bulunulmadığı beyan edildi.	
A.7.1.1 Varlıkların envanteri	Tüm varlıklar açıkça tanımlanmış ve önemli varlıkların bir envanteri hazırlanmış ve tutulmakta mıdır?	BGYS (http://bgys) 'den varlık envanteri incelendi. Herhangi bir varlığa rastlanmadı.	Kullanılan varlıkların BGYS (http://bgys) sistemine girişlerinin ve risk analizlerinin yapılması gerekmektedir.
A.7.1.2 Varlıkların sahipliği	Bilgi işleme olanakları ile ilişkili tüm bilgi ve varlıklar kuruluşun belirlenmiş bir bölümü tarafından sahiplenilmiş midir?	BGYS (http://bgys) 'den varlık envanteri incelendi. Herhangi bir varlığa rastlanmadı.	Kullanılan varlıkların BGYS (http://bgys) sistemine girişlerinin ve risk analizlerinin yapılması gerekmektedir.
A.8.1.1 Roller ve sorumluluklar	Çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların güvenlik rolleri ve sorumlulukları kuruluşun bilgi güvenliği politikasına uygun olarak tanımlanmış ve dokümante edilmiş midir?	Rol ve sorumlulukların tanımlanmış olduğu görülmüştür.	
A.8.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi	Kuruluştaki tüm çalışanlar ve ilgili olan yerlerde yükleniciler ve üçüncü taraf kullanıcılar, kendi iş fonksiyonları ile ilgili olduğunda, kurumsal politikalar ve prosedürlerle ilgili uygun farkında olma eğitimi ve düzenli güncelleme almaktadırlar mı?	Bilgi Güvenliği farkındalık eğitimlerine katılım gerçekleştirilmediği görüldü. Bilgi Güvenliği politikalarına BGYS sistemi üzerinden bilgi sahibi olunduğu tespit edildi.	
A.10.1.1 Dokümante edilmiş işletim prosedürleri	İşletim prosedürleri dokümante edilmeli, sürdürülmeli ve ihtiyacı olan tüm kullanıcılara ulaşılabilmesi sağlanmış mıdır?	İşletim prosedürlerinin yazılıp qdms sistemine konulmuştur.	.

Bulgular: Bilgi Teknolojisi varlık ve risk yönetim değerlendirilmelerinde gelişim alanları olduğu tespit edilmiş olup ilgili çalışmalar başlatılmıştır.



Şekil 10. Bulgu Grafiği

Kurum çalışanlarının ilgili iç denetimler sonrası düzenleyici ve önleyici faaliyetleri yerine getirmek için referans alınması gereken süreçler ve yöntemler Bilgi Güvenliği Ekibi tarafından aşağıdaki adımlar kullanılarak oluşturulmuş ve sonrasında varlık ve risk yönetimi çalışmaları yapılmıştır.

3.1.Varlık Risk Analizlerinin Yapılması

ISO 27001 BGYS iç denetim sonucu bulgu olarak tespit edilen risklerin analizi için risk değerlendirme tabloları yapılıp skorlarının hesaplanması için risk analizleri gerçekleştirilmiştir. Kurumdaki bilgi güvenliğine yönelik risklerin yönetimi http://bgys linkinden ulaşılan bgys uygulamasından takip edilir.

Tablo 23. Risk Analizi

	1.Varlık için Risk Analizi	2.Varlık için Risk Analizi	3.Varlık için Risk Analizi
Aksiyon Adı	Proje	Proje	Proje
Son Tarih	31.12.2014	31.12.2014	31.12.2011
Sorumlu Organizasyonu	Sistem Yöneticisi	Sistem Yöneticisi	Sistem Yöneticisi
Sorumlu	Varlık Sahibi	Varlık Sahibi	Varlık Sahibi
Aksiyon Durumu	%50 Yapıldı	%50 Yapıldı	%50 Yapıldı
Varlık Kategorisi	Kurum Servisleri	Uygulama Yazılımları	Uygulama Yazılımları
Varlık	Müşteri Bilgileri Veritabanı	Çağrı Merkezi Müşteri Bilgileri Yönetimi Ekranları	Çağrı Merkezi Müşteri Bilgileri Yönetimi Ekranları
Teknik Sahibi	Sistem Yöneticisi	Sistem Yöneticisi	Sistem Yöneticisi
Gizlilik	Yüksek	Yüksek	Yüksek
Bütünlük	Çok Yüksek	Yüksek	Yüksek
Erişilebilirlik	Orta	Yüksek	Yüksek
Sınıflandırma	Dahili Kullanım	Dahili Kullanım	Genel Kullanım
Zafiyet Kategorisi	Erişim Kontrolü	İletişim & Operasyonel Güvenlik	İletişim & Operasyonel Güvenlik
Zafiyet	Açık bırakılmış bağlantılar / Kullanıcı bilgisayarları	Log üretilememesi/istenilen kriterlerde olmaması	Log üretilememesi/istenilen kriterlerde olmaması
Zafiyete Bağlı Risk	Yetkisiz erişim sağlanması	Hesap verilebilirliğin sağlanamaması/vakaların çözülememesi	Hesap verilebilirliğin sağlanamaması/vakaların çözülememesi
Tehdit	Şirket menfaatlerine aykırı niyet	Hata ve kötü niyete açık çalışma ortamı	Hata ve kötü niyete açık çalışma ortamı
Risk Çözüm Yaklaşımı	Yönet	Yönet	Yönet
Risk Kaynağı	Risk Analizi	Risk Analizi	Risk Analizi
Risk Olasılığı	Düşük	Düşük	Düşük
Risk Etkisi	Çok Yüksek	Yüksek	Düşük
Risk Seviyesi (Skoru)	10.0	8.0	4.0
Kontrol Kategorisi	A.11 Erişim kontrolü	A.10 Haberleşme ve işletim yönetimi	A.10 Haberleşme ve işletim yönetimi
Kontrol	A.11.3.2 Gözetimsiz kullanıcı teçhizatı	A.10.10.1 Denetim kaydetme	A.10.10.1 Denetim kaydetme

Risk analizleri yapılırken aksiyonlar projelendirilerek varlıkların risk analizleri yapılmıştır. Risk Analizlerinde aşağıdaki adımlar uygulamıştır.

3.2.Riskin Derecelendirilmesi

- **Riskin etkisinin belirlenmesi:**

➢ Birinci varlık için risk etkisi, aşağıdaki risk etki tablosuna göre değerlendirildiğinde "çok yüksek (5)" olarak tespit edilmiştir.

➢ İkinci varlık için risk etkisi, aşağıdaki risk etki tablosuna göre değerlendirildiğinde "yüksek (4)" olarak tespit edilmiştir.

➢ Üçüncü varlık için risk etkisi, aşağıdaki risk etki tablosuna göre değerlendirildiğinde "düşük (2)" olarak tespit edilmiştir.

Tablo 24. Risk Etki Tablosu

Riskin Etkisi	Finansal Etki	Dış/İç Müşteri Memnuniyet Etkisi	İş/Servis Aksamaması	İtibar Etkisi	Pazar Değeri Etkisi
5 Çok Yüksek	10 Milyon TL finansal etki	Dış müşteri /Çalışan memnuniyetinin kritik düzeyde etkilenmesi	24 saat iş/servis aksaması	Yurtiçi/dışı basında geniş haber etkisi ile ciddi itibar kaybı	Pazar değerinin kritik düzeyde etkilenmesi
4 Yüksek	5-10 Milyon TL arasında finansal etki	Dış müşteri /Çalışan memnuniyetinin önemli orada etkilenmesi	12-24 saat arası iş/servis aksaması	Geri kazanımı güç itibar kaybı	Pazar değerinin önemli oranda etkilenmesi
3 Orta	1-3 Milyon TL arasında finansal etki	Dış müşteri /Çalışan memnuniyetinin kısmi olarak etkilenmesi	6-12 saat arası iş/servis aksaması	Geri kazanabilir itibar kaybı	Pazar değerinin kısmi olarak etkilenmesi
2 Düşük	500.000-1 Milyon TL arasında finansal etki	Dış –İç müşteri/Çalışan memnuniyetinin kabul edilebilir düzeyde olması	2-6 saat arası iş /servis aksaması	Göz ardı edilebilir itibar kaybı	Pazar değerinin kabul edilebilir düzeyde etkilenmesi
1 Çok Düşük	500.000 den az finansal etki	Dış –İç müşteri/Çalışan memnuniyetinin hemen hemen hiç etkilenmemesi	2 saat iş /servis aksamaması	İtibar zedeleyici etkisi bulunmayan	Pazar değerinin hemen hemen hiç etkilenmemesi

- **Riskin olasılığının belirlenmesi:**

Tüm varlıklar için risk olasılığı yıl içinde gerçekleşme oranı göz önüne alındığında "düşük (2)" olarak belirlenmiştir.

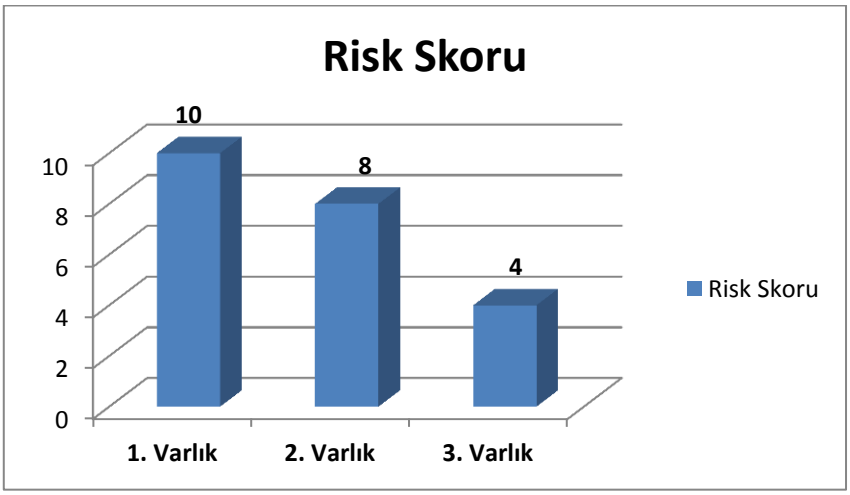
Tablo 25. Risk Olasılık Tablosu

Riskin Oluşma Olasılığı	Oluşma İhtimali	Oluşma Sıklığı
5 Çok Yüksek	1 Yıl içine gerçekleşme ihtimali %80 'den fazla	Hemen hemen her seferde meydana gelen
4 Yüksek	1 Yıl içine gerçekleşme ihtimali % 50-%80 arasında	Çoğu sefer meydana gelen
3 Orta	1 Yıl içine gerçekleşme ihtimali %30-%50 arasında olasılık	Zaman zaman meydana gelen
2 Düşük	1 Yıl içine gerçekleşme ihtimali %10-%30 arasında olasılık	Nadiren meydana gelen
1 Çok Düşük	1 Yıl içine gerçekleşme ihtimali % 10 dan küçük olasılık	Hemen hemen hiç meydana gelmeyen

- **Risk skorlarının hesaplanması**

"Risk Skoru= Riskin Oluşma Olasılığı* Riskin Etkisi" formülünden risk skorları

- 1. Varlık için 5 *2 =10
- 2. Varlık için 4*2=8
- 3. Varlık için 2*2=4 olarak hesaplanmıştır.



Şekil 11. Risk Skoru Grafiği

Varlıklara ait risklerden en üst skordan başlanıp analizleri yapılarak risklerin azaltılması yöntemi seçilmiştir. Bu analizler sonrası kabul edilebilir risk seviyesine ulaşılmıştır.

3.3.Risk İndirgeyici Analiz Çalışmaları

ISO 27001 Bilgi Güvenliği İç denetimi sonrası tespit edilen risklerin azaltılması amacı ile 3 varlık için riskin indirgeyici analiz çalışmaları yapılmıştır. Risklerin analizleri aşağıdaki formatta yapılarak kurum intranet alanındaki http://bgys sisteme yüklenmiştir.

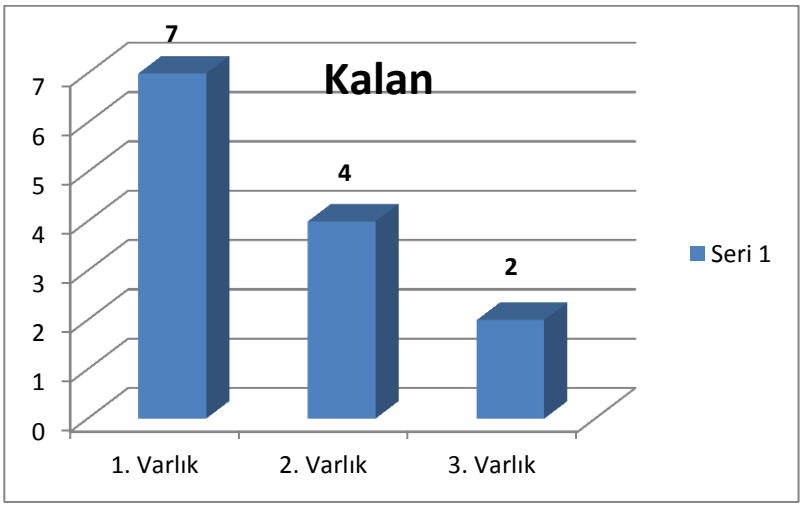
Tablo 26. Risk Analiz Çalışmaları

Risk No:	1
Risk Tanımı	Yetkisiz üçüncü şahısların servise erişip hizmet veremez duruma getirmesi, kullanıcıların yaptıkları işlemler hakkında bilgi alması
Servis İsmi	Müşteri Bilgileri Veritabanı
Risk Önem Derecesi	Çok Yüksek
Risk İşleme Yöntemi	Riskin Azaltılması
Aksiyon Durumu	Tamamlandı.
Aksiyon Sahibi	Servis Sahibi.

Risk No	2
Risk Tanımı	Yapılan bir işlemin izinin sürülememesi, vaka oluşması durumunda kimin tarafından yapıldığının bilinememesi ile sonuçlanır.
Servis İsmi	Çağrı Merkezi Müşteri Bilgileri Yönetimi Ekranları
Risk Önem Derecesi	Yüksek
Risk İşleme Yöntemi	Riskin Azaltılması
Aksiyon Durumu	Tamamlandı.
Aksiyon Sahibi	Servis Sahibi.

Risk No	3
Risk Tanımı	Yapılan bir işlemin izinin sürülememesi, vaka oluşması durumunda kimin tarafından yapıldığının bilinememesi ile sonuçlanır.
Servis İsmi	Müşteri Online İşlem Merkezi
Risk Önem Derecesi	Düşük
Risk İşleme Yöntemi	Riskin Azaltılması
Aksiyon Durumu	Tamamlandı.
Aksiyon Sahibi	Servis Sahibi.

4.Adım : Kalan riskin yönetimi:



Şekil 12. Kalan Risk Grafiği

. Kabul edilebilir risk seviyesine indirilen riskler belirtilen risk skoruna göre ilgili iş sahibi yöneticisinden onay alınır. Planlanan kontroller üst yönetime raporlanarak bilgilendirme yapılır.

3.4.Yönetime Gözden Geçirme Raporunun Sunulması

BİLGİ GÜVENLİĞİ İÇ DENETİM YÖNETİM SONUÇ RAPORU	
ÇALIŞMANIN AMACI	Bilgi Güvenliği Yönetimi kapsamında Kurumun ITIL, COBIT ve ISO27001 standartlarına uygunluğunun denetlenmesi ve değerlendirilmesi. Değerlendirme neticesinde varsa güncellemelerin ve eksikliklerin tespit edilerek, bunların giderilmesi
DEĞERLENDİRİLEN SÜREÇLER	BGYS Kapsamında, Risk Yönetimi, Varlık Yönetimi, Bilgi Güvenliği Farkındalığı, İşletim Prosedürlerinin Yönetimi
ÇALIŞMA EKİBİ	(Gizlilik çerçevesinde isimler paylaşılmamıştır)
SÜREÇ DEĞERLENDİRMELERİ SONUCU	
Bilgi Güvenliği Yönetimi kapsamında gerçekleştirilen süreç gözden geçirme çalışmalarında hayata geçen veya henüz hayata geçmemiş olan tüm süreçlerin ITIL, COBIT ve ISO27001 standartlarına göre doğru tasarlanıp tasarlanmadığının kontrolü amacı ile ISO 27001 iç denetimi gerçekleştirilmiştir. İç denetim ile tespit edilen eksikliklerin giderilmesi için gerekli çalışmalar planlanmıştır	

SONUÇ

Bilgi teknolojileri gün geçtikçe daha da önem kazanan ve ihtiyacın giderek arttığı organizasyonel olarak birçok faydası yöneticiler tarafından da kabul edilmiş bir uygulamadır. İşletmelerin bilgileri diledikleri gibi kontrol edebilmeleri için öncelikle elindeki bilgilerin güvenliğini sağlamalı ve risklere karşı korumalıdır. Kurumsal bilginin sağlanabilmesi için bilgi güvenliği standartlarının uygulayıcılar tarafından bilinmesi ve olası risklere karşı önlemler alınmalıdır. Organizasyonların bilgiyi idare edip yüksek seviyeli koruma sağlayabilmeleri için teknolojiyi etkili biçimde kullanmaları ve ilgili kişileri iyi seçip eğitmeleri gerekir.

Organizasyonların çağımızda güvenilirliğini sınamaya yönelik çalışmaların faydası vardır. İşletmelerin iş hedefleri doğrultusunda gerçekleştirdikleri operasyonların stratejisi hizmet kalitesini arttırmaya yönelik olmalıdır. Fakat günümüz rekabet ortamında her organizasyon kendine hizmet kalitesi arttırıcı stratejiler belirlemeyebiliyor ve bu da zaman zaman skandallara sebep oluyor. Bu yüzden kurumların iç denetimlerinin yanında bağımsız kuruluşlarca denetlenmesini de zorunlu kılmıştır. Denetime tabi olan kuruluşların başında da finansal kuruluşlar olan bankalar gelmektedir.

Bilgi teknolojileri gün geçtikçe daha da önem kazanan ve ihtiyacın giderek arttığı organizasyonel olarak birçok faydası yöneticiler tarafından da kabul edilmiş bir uygulamadır. İşletmelerin bilgi diledikleri gibi kontrol edebilmeleri için öncelikle elindeki bilgilerin güvenliğini sağlamalı ve risklere karşı korumalıdır. Kurumsal bilginin sağlanabilmesi için bilgi güvenliği standartlarının uygulayıcılar tarafından bilinmesi ve olası risklere karşı önlemler alınmalıdır. Organizasyonların bilgiyi idare edip yüksek seviyeli koruma sağlayabilmeleri için teknolojiyi etkili biçimde kullanmaları ve ilgili kişileri iyi seçip eğitmeleri gerekir.

Organizasyonların çağımızda güvenilirliğini sınamaya yönelik çalışmaların faydası vardır. İşletmelerin iş hedefleri doğrultusunda gerçekleştirdikleri operasyonların stratejisi hizmet kalitesini arttırmaya yönelik olmalıdır. Fakat günümüz rekabet ortamında her organizasyon kendine hizmet kalitesi arttırıcı

stratejiler belirlemeyebiliyor ve bu da zaman zaman skandallara sebep oluyor. Bu yüzden kurumların iç denetimlerinin yanında bağımsız kuruluşlarca denetlenmesini de zorunlu kılmıştır. Denetime tabi olan kuruluşların başında da finansal kuruluşlar olan bankalar gelmektedir.

"Bilgi Teknolojileri Yönetim Sistemleri" olarak anılan COBIT, ISO ve COSO gibi standartların, bilgi teknoloji hizmetlerinin müşterilere arzu edilen seviyede ulaşmasını sağlama, bilgi teknolojileri sistemlerinin denetimini, gözlemlenebilirliğini, ölçeklenebilirliğini, işlevselliğini, verimliliğini, güvenilirliğini ve sürekliliğini sağlama anlamında kurumlara birçok katkısı vardır.

Bilgi teknolojileri için kritik uygulamalar olan COBIT ve ITIL birçok kişi tarafından fonksiyonel olarak aynı sayılsa da COBIT' i, ITIL' ın standartlarından ayıran en önemli özelliği tüm BT fonksiyonlarını kapsayan genel bir çerçeve sunmasıdır. Diğer bir deyişle COBIT' in kapsadığı 34 süreci genel olarak incelediğimizde aslında BT yönetimin birçok alanını kapsamış oluruz. Yani ITIL' a göre daha kapsamlı ve özet bir çalışmayı 34 süreç altında ele alır.

Güvenlik politikası organizasyonlarda olması gereken güvenlik seviyesinin oluşmasına ve tanımlanmasına yardım eden ve tüm çalışanların, ortak çalışma içerisinde bulunulan diğer organizasyon çalışanları dahil, herkesi kapsayan uyulması gereken kurallardan oluşmalıdır.

Bilgi teknolojileri kapsamında yapılan risk analizleri de en az bilgi güvenirliği kadar önemlidir. Bilgi Güvenliği Yönetimi kapsamında gerçekleştirilen süreç gözden geçirme çalışmalarında hayata geçen veya henüz hayata geçmemiş olan tüm süreçlerin ITIL, COBIT ve ISO27001 standartlarına göre doğru tasarlanıp tasarlanmadığının kontrolü amacı ile ISO 27001 iç denetimi gerçekleştirilmiştir. İç denetim ile tespit edilen eksikliklerin giderilmesi için gerekli çalışmalar planlanmıştır. Olası riskleri listeleyip olma olasılıkları verip bunları değerlendirme şansı tanıyan bu analizler organizasyonlara hem zaman, hem finansal, hem de itibar açısından birçok katkıda bulunur. Sistematik ve plan çerçevesinde yapılan analizler sonucu risklerin belirlenip müdahale edilmesiyle organizasyon iş hedefleri doğrultusundan şaşmaz. ITIL tarafından tanımlanan süreçler, prosedürler, işler ve denetim listeleri organizasyon tarafından stratejilerini, değer teslim ve yetkinlik

seviyeleri entegrasyonunu korumak amacıyla kullanılır. ITIL organizasyonlara planlanabilir, uygulanabilir ve ölçülebilir kriterler sağlamada önemli bir rol oynar.

Bilgi güvenliği, kurumların bilgi envanterindeki varlıkların güvenliğinin sağlanması, bu konuda risk yönetimi gereklerinin yapılmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olabilirliğine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir; riskin azaltılması, riskin kabul edilmesi, tamamen üçüncü bir tarafa devredilmesi (sigorta etmek gibi) veya risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir. Risklerin tanımlanması ISO 13335-115 standardında da gösterilmektedir. Bu standardın tanımı itibariyle bilgi güvenliği, bilginin risk yönetimini yapmaktır

KAYNAKÇA

ABH Aylık e- bülteni, **ITIL tabanlı konfigürasyon yönetimi**, Nisan 2011, sayı: 55.

Akıncı, H., Alıç, E., Er, C., **Türk Ceza Kanunu ve Bilişim Suçları**, İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yay, 2004.

Aktaş, F.Ö. **Bilgi Güvenilirliği Risk Yönetiminin Belirlenmesi**, Türkiye Bilişim Vakfı Dergisi, Sayı: 3, 2009, s. 53-62,

Alberts, C. ve Dorofee, A. **Managing Information Security Risks: The OCTAVE Approach**. Boston, MA: Addison- Wesley, 2003

Artinyan, E.N., **COBIT Çerçevesi,** Deloitte Kurumsal Risk Hizmetleri, 2008, 1-6.

Atan, M., **Risk Yönetimi Ve Türk Bankacılık Sektöründe Bir Uygulama**, Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara. 2002, 97

Aykut C. "**Basel II Standartları**", Türkiye Cumhuriyeti Dışişleri Bakanlığı Yayınları: Uluslararası Ekonomik Sorunlar Dergisi, Sayı: 30, 2008, s.8

Baraçlı, H., **Kriz ve Teknoloji Yönetimi**, İstanbul: Yıldız Teknik Üniversitesi 3 Gen Dergisi, 2001

Başarır, M., **Bankalarda Teknoloji Riski Ve Yönetimi**, Yüksek Lisans Tezi, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü, İstanbul, 2006.ç

BDDK, **Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**, Ankara. 2006.

Beydağlı vd. **Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler**, 4. Ulusal Yazılım Mühendisliği Sempozyumu - UYMS'09, 2009.

Birengel, S., **Başarılı Bilgi İşlem Merkezi Modeli-5.** Çalışma Grubu Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu VIII, İstanbul, 2006.

British Standards Institute, "**İnformation Technology — Security Techniques — Code of Practice for information Security Management**", BSI BS 7799-1, Bristol. 2005, 750-780.

Canberk G. ve Sağıroğlu Ş., **Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme**, Politeknik Dergisi ,Cilt: 9, Sayı: 3, 2006, s.165-174.

Canlı, C., **Saldırı Tespit Sistemlerinin İncelenmesi ve bu Bağlamda Bilgi Güvenliği, 2**009.

Çekiç, Burak "**İnternet Aracılığı İle İslenen Suçların Yapısı Ve Alınması Gereken Tedbirler",** Yayınlanmamış Yüksek Lisans Tezi, (Marmara Üniversitesi) 2006.

Değirmenci, O., **Bilişim Suçları,** Yayınlanmamış Yüksek Lisans Tezi (Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı), 2002.

Değirmenci, O., **Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi**, Legal Hukuk Dergisi, S. 11, 2003, s.2750

Dhillon, G. **Principles of Information Systems Security: text and cases**, 2007, s. 97-129.

Dinç, E., Abdioğlu, H., **İşletmelerde Kurumsal Yönetim Anlayışı ve Muhasebe Bilgi Sistemi ilişkisi: İMKB-100 şirketleri Üzerine Ampirik Bir Araştırma**, Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt: 12, Sayı: 21, Haziran 2009, s.159.

Doğan, A., E., **Bilişim Suçları ve Hukukuna Giriş**, Doruk Yayınları, Ankara, 1992.

Doğantimur, F.. **ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği**. Mesleki Yeterlilik Tezi, TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara, 2009.

Ersoy, E. V., **ISO/IEC 27001 Bilgi Güvenliği standardı,** Ankara, 2012, 74-75.

Ersoy, E., **Bilgi güvenliğinin kurumsal bazda uygulanması**, Bildiriler Kitabı uluslararası katılımlı bilgi güvenliği ve kriptoloji konferansı, 2007.

Ersoy, Y., **Genel Hukuki Koruma Çerçevesinde Bilişim Suçları**, Ankara Üniversitesi Siyasal Bilgiler Fakültesi, C. 49, S. 3-4, 1994, s. 152,

Fasanghari, R. & Kamal, C. **Assessing the impact of information technology on supply chain management** .World applied sciences journal, 4(1), 2008. 87-93

Fikirkoca, M., **Bütünsel Risk Yönetimi**, Kalder Yayınevi, Ankara, 2003.

Guldentops vd., **COBIT**, 3rd Edition Usage Survey: Growing Acceptance of COBIT", Information Systems Control Joumal, Vol. 6, 2002, pp. 25-31.

Güneş F., Kızıldeniz S., Selçuk S., Suna B., Coşkun S., **Bilgi Teknolojileri Denetimi ve COBIT' in Sektörel Uygulanabilirliği**, 2002, 12

Güvener, E., **Teknoloji Yönetimi Ve Teknoloji Kontrolü**, Active Bankacılık ve Finans Dergisi, Şubat-Mart (11) 2000.

Haleh B., E., Hassan G., Shahram S., S., **2nd International Conference on Computer Technology and Development**, Strategic Alignment: ITIL Perspective, 2010, 158.

Hansche, S. **Official (ISC2) Guide to the CISSP Exam**, Auerbach Publication, 2003, 19

Herr D., **Seven Steps to Developing an Effective IT Strategic Plan Chief Technology and Security Officer**, The Asbury Group Integrated Technologies, 2006, 410

Heschl, J., **COBIT Mapping: Overvıew Of Internatıonal IT Guıdance** 2nd Edition, Illinois , USA, 2006, 157- 168

IT Governance Institute, **COBIT Executive Summary**, 3rd Edition, Released by COBIT Steering Committee, pp. 3, July 2000, 20

ITGI (Information Technologies Governance Institude - Bilgi Teknolojileri Yönetim Enstitüsü), PriceWaterhouseCoopers-ITGI. 2006, 250

İlbaş, Ç. **Bilişim Suçlarının Sosyo-kültürel Seviyelere Göre Algı Analizi**, Yüksek Lisans Tezi, Ankara, 2009.

İnceler, H., **Teknoloji Yönetiminin Ekonomik ve Sosyal Etkileri**, Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 1995.

J. Lainhart, **An IT Assurance Framework for the Future**, Ohio CPA Journal, 2001, 191–193

Johnson, B., **Hizmet Yönetimi Süreç Haritaları**, Paloma Yayınevi, İstanbul, 2007.

Kahraman S., **Yönetimde Bilgi Güvenliği Sisteminin yapısı, İşleyişi ve Aselsan A.Ş'de Uygulanması**, 2006, 22-28

Karabacak, B., **Türkiye'de Bilişim Güvenliğiyle İlgili Yasal Altyapının Analizi**", TÜBİTAK-UEKAE. 2009, 243

Kardaş, Ü., **Bilişim Dünyası ve Hukuk**, Karizma Dergisi, S. 13, Y. 2003, s. 7.

Kovacich, G. L., **The information Systems Security Officer's Guide: Establishing and Managing an İnformation Protection Program**. 2003, 4

Kurt, L., **Açıklamalı- İçtihatlı Tüm Yönleriyle Bilişim Suçlamaları ve Türk Ceza Kanundaki Uygulaması**, Seçkin Yayınevi, Ankara, 2005.

Latif A.A., Din M.M. and Ismail R., "**Challenges in adopting and integrating and CMMI in ICT Division of a public utility company**", Second International Conference on Computer Engineering and Application, 2010, 112.

Lehtinen, R., **Computer Security Basics**, 2nd Edition, ABD: O'Reillly Publishing, 2006.

Linn R.J., **An intelligent management system for technology management**, Cilt: 38, Sayı: 3, 2000, s. 397-412

Maiwald, E., **Network Security: A Beginner's Guide**, Second Edition, ABD Kaliforniya: McGraw-Hill, ISBN 0-07-222957-8, 2003.

Mandacı, P.E., **Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Kriz Aşmada Kullanılan Risk Ölçüm Teknikleri**, İzmir: 9 Eylül Üniversitesi SBE Dergisi, 2003, 5(1):67-84.

Marquis H**., ITIL: what it is and what it isn't**, Business Communication Review,

vol. 36, Issue 12, 2006, pp. 49-52.

Memiş, T., Hukuki Açıdan Kitlelere E-Posta Gönderilmesi (Spamming), http://hukukcu.com/modules/ smartsection/item.php?itemid=29.Erişim tarihi: 25/07/2014.

Nabiollahi and Sahibuddin, **Considering Service Strategy in ITIL V3 as a Framework for IT Governance**, 2008, s.2

NIST, **An Introduction to Computer Security**:The NIST Handbook Special Publication, 1997.

Osborne, M., **How to Cheat at Managing information Security**, Syngress Publishing Inc. Rockland. 2006.

Öğüt, A. **Bilgi Çağında Yönetim**, Nobel Basımevi, Ankara, 2003.

Önel D. ve Dinçkan A., **Bilgi Güvenliği Yönetim Sistemi Kurulumu**, TÜBİTAK ÜEKAE Doküman kodu: BGYS 0001, Kocaeli.2007.

Pearce, Pearce R., **The evolution of technology in multinational enterprises: the role of creative subsidiaries**, International Business Review 1999,s. 125 – 148.

Pekel, A., **Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT)**, Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu X, İstanbul, 2008, 35.

Pengwen XU., Yanmei WU., Ziran LI, **Research on the Equipment Acquisition Information,** 2008.

Rosenblum M. ve T. Garfinkel, **Virtual Machine Monitors: Current Technology and Future Trends.** IEEE Internet Computing, 2005, 38

Sahibudin, S.; Sharifi, M.; Ayat, M., **Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations;Modeling & Simulation,** AICMS 08. Second Asia International Conference, 2008, 749 –753

Sağıroğlu Ş., Bulut H., **Mobil Ortamlarda bilgi ve Haberleşme Güvenliği Üzerine Bir İnceleme**, Gazi Üniv. Müh. Mim. Fak. Der. Cilt 24, No 3, 2009, 499-507.

Sağıroğlu, Ş. ve Say, M.ve Alkan, M., **Bilgisayar Sistemlerinde Güvenlik**, Telekom Dünyası, Ekim 2004, s.49

Saleh J. M. , Almsafir M. K., **The Drivers of ITIL Adoption in UNITEN**, 2013 International Conference on Advanced Computer Science Applications and Technologies, 2013.

Sharifi M., Ayat M., Ibrahim S. and Sahibuddin S., **The most applicable KPIs of problem management process in organizations**, International Journal of Simulation: Systems, Science & Technology, Cilt :10, No :3, 2009, ss. 77-83.

Swanson and Guttman, (1996), **Generally accepted principles and practices for securing information technology systems**, Cilt 13, Sayı 10,1996, s.800

Şahinaslan, E., Kantürk, A., Şahinaslan Ö. ve Borandağ E., **Kurumlarda Bilgi Güvenliği Farkındalığının Önemi ve Oluşturma Yöntemleri**, 2009, 325.

TBD Kamu-BİB, "**Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri**", Kamu Bilişim Platformu, Sürüm 1.0., 2008, 156-160.

Tekerek, M. **Bilgi Güvenliği Yönetimi**, KSU Journal of Engineering Sciences *11(1)*, 2008, 132-137.

The IT Governance Institute, **COBIT 4.1 Framework**, 2007, 156

Turhan, O., **Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)**, (Yayınlanmamış Planlama Uzmanlığı Tezi, T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği), 2006.

Türk Standartları Enstitüsü, "**Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler**", TSE- TS ISO/IEC 27001, Ankara, 2006, 250-262.

Türkiye Bilişim Derneği, **E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları 4. Çalışma Grubu Sonuç Raporu**, TBD Kamu-BİB IV, Ankara, 2005, 15-16.

Tyler, R. **Implementing COBIT in New South Wales Health**, Information Systems Control Journal, 2000, 30–32.

Uzunay, V**., CobiT (Control Objectives for Information and related Technology**, İç Kontrol Merkezi Uyumlaştırma Dairesi, Ankara, 2007, 185.

Vural, Y. ve Sağıroğlu, Ş., **Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme**, Gazi Üniv. Müh. Mim. Fak. Der. Cilt 23, No 2. 2008, 195.

Wagner, D. & Soto, P. **Mimicry Attacs on Host- Based Intrusion Detection Systems. Communications of the ACM**:, 2000, 255-264

Yazıcı, A., (2006), **Bilişim Teknolojilerinde Risk Yönetimi-2**. **Çalışma Grubu**, Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu VIII, İstanbul, 2006.

Yazıcıoğlu, R. Yılmaz, **Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi**, Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, C:2, 2005, S:2.

Yıldız, B., **Bilgi güvenliği ve e-devlet kapsamında kamu kuramlarında bilgi güvenliği yönetimi ve standartların uygulanması**, Yüksek Lisans Tezi, Gebze Yüksek teknoloji Enstitüsü, Gebze, 2007.

Yılmaz, S., **5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen bilişim alanındaki Suçlar**, TBB Dergisi S.91, 2011, s.64.

Yi Gao, (2005), **Efficient Trapdoor-Based Client Puzlzle System Against DoS Attacks**, (Master Tezi, University of Wollongong.

İNTERNET KAYNAKLARI

http://www.bddk.org.tr/WebSitesi/turkce/Basel/Basel_II.aspx, (Erişim tarihi: 25/07/2014)

http://www.coso.org/, (Erişim tarihi: 15/01/2014)

www.itgi.org, (Erişim tarihi: 18/08/2014)

http://www.ubak.gov.tr/BLSM_WIYS/UBAK/tr/dokuman_ust_menu/bakanlik/20131030_152852_204_1_64.pdf (Erişim tarihi: 19.07.2014)

http, s.//www.bddk.org.tr/WebSitesi/turkce/Basel/Basel_II.aspx , (Erişim tarihi: 16.07.2014)

http:// acikarsiv.atilim.edu.tr/browse/280/ fatma_burcu_nacar.pdf (Erişim tarihi: 18.09.2014)

http://www.icdenetimmerkezi.com/bilgibankasi_alt.php?mn=1&p=33 (Erişim tarihi: 18.07.2014)

ÖZGEÇMİŞ

1 Şubat 1978 tarihi, İstanbul Kadıköy ilçesi doğumluyum. İlk, Orta ve Liseyi Gebze ilçesinde tamamladıktan sonra, Kocaeli Üniversitesi MYO, Kontrol Sistemleri Teknolojisi bölümünde önlisans eğitimimi tamamladım. Bu bölümden 2000 yılında mezun olduktan sonra, Anadolu Üniversitesi İşletme Fakültesinde Lisans eğitimimi 2004 yılında tamamlayarak, askerlik görevimi Osmaniye' de yaptım. 2005 yılından beri, özel bir şirkette teknik süreç yönetimi kapsamında çalışmaktayım. 2012 yılında da, Beykent Üniversitesi, İşletme Anabilim Dalında yüksek lisans eğitimine başladım.

Özel ilgi alanlarım, teknik süreç yönetimi, bilgi güvenliği ve müşteri algı yönetimidir.

Yabancı dilim İngilizce olup, evli ve bir çocuk babasıyım.

Aday: Orhan YILMAZ