T.C.

BAYINDIRLIK VE İSKAN BAKANLIĞI

Tapu ve Kadastro Genel Müdürlüğü

(Teftiş Kurulu Başkanlığı)

İnceleme-Araştırma Konusu

Bilgi Sistemleri Denetimi, e-Teftiş, Ülkemizde ve Diğer Ülkelerde Uygulamaları, Bilgi Sistemleri Denetimi ile e-Teftişin Müfettişler Tarafından Yapılabilmesi İçin Gerekenlerin Belirlenmesi

Hazırlayan

İlker ÇOBANOĞULLARI

Müfettiş Yardımcısı

Danışmanlar

Başmüfettiş - İzzet SEVİNÇ

Müfettiş - Mustafa KARAATMACA

ANKARA

2011

ÖNSÖZ

Bilgi sistemlerinin yoğun olarak kullanıldığı kurumlar arasında bulunan Tapu ve Kadastro Genel Müdürlüğünde, veri üretiminde bilgi sistemlerinin önemi göz önüne çıkmaktadır. Bu sebeple denetim faaliyetleri kapsamında bilgi sistemleri denetimi ile bilgi sistemine entegre olarak denetim faaliyetlerinin yürütülebilmesi, günümüz teknolojik gelişmelerine ve kurumda yürütülen bilgi sistemi yapısına bağlı olarak kaçınılmaz hale gelmiştir. Bu sebeple çalışmamızda bilgi sistemleri denetiminin ve bilgisayar destekli denetim araçların kullanımının artık kaçınılmaz olduğu ortaya konmuştur.

Tapu ve Kadastro Bilgi Sistemlerinin ve bu sistemlerin denetiminin dünyaca kabul görmüş standartlara bağlanması, bilgi sistemlerinin sağlam bir yapıya kavuşturulması sağlanmalıdır.

Bu suretle sistematiğe bağlanan bilgi sistemleri denetimi yanında, Teftiş Kurulu Başkanlığınca başlatılacak çalışmalar ile TAKBİS'e entegre edilecek denetim modülü ve altlıkları ile mevcut sistem üzerinden denetimin sağlanması, günümüz ihtiyaçları arasına giren bilgisayar destekli denetim fonksiyonun geliştirilmesi yönünde çalışmaların başlatılması gerekmektedir.

Ankara; 2011

İÇİNDEKİLER

GİRİŞ

Yaşadığımız bilgi çağının ve küreselleşmenin bir sonucu olarak artan rekabet, bilginin önemini artırmıştır. Kurumlar ve işletmeler bu rekabet ortamında ayakta kalabilmek ve koşullara olabildiğince çabuk tepki verebilmek için detaylı bilgi ve raporlama sistemlerine ihtiyaç duymaktadırlar. Bu ihtiyaç üzerindeki artış, günümüz çağındaki bilgi artışı ile bir araya geldiğinde, hemen hemen tüm kuruluşların iş süreçlerini bilgi sistemleri desteği ile yürütmeleri gerçeğini ortaya çıkarmaktadır.

Bilgi sistemleri denetimi; İdarenin, amaçlarına ve kontrol hedeflerine ulaşmasına yönelik olarak Bilgi sistemlerinin yeterliliği hakkında makul bir güvence sağlamak amacıyla bilgi sistemlerinin incelenmesi, gerekli kanıtların toplanması, değerlendirilmesi ve sonuçların raporlanması süreci olarak tanımlanabilir.

* Bilgi teknolojilerinin kötüye kullanımı
* Kişisel bilgilerin korunması
* Yanlış karar alma
* Veri kaybının kurumsal maliyeti
* Bilgi sistemleri hatalarının yüksek maliyeti
* Donanım, yazılım ve çalışanların yüksek maliyeti
*Bilgi sistemleri kullanımının kontrol edilemez bir şekilde sürekli değişime uğraması gibi risk ve olumsuzluklar Bilgi Sistemleri Denetiminin gerekliliğini ortaya koymaktadır.

Bu kapsamda araştırmanın önemi, Tapu ve Kadastro Genel Müdürlüğü ve bilgi sistemlerinin yoğun kullanıldığı sektörlerde bilgi sistemleri denetiminin önemini vurgulamak ve denetim amaçlarının sağlıklı olarak karşılanması için bilgi sistemleri denetim faaliyetlerinden ve bilgisayar destekli denetim araçlarından yararlanmanın kaçınılmaz olduğunu ortaya koymaktır.

BİRİNCİ BÖLÜM

1. BİLGİ SİSTEMLERİNİN YÖNETİMİ VE TEMEL KONTROL KAVRAMLARI[1]

Bilgi sistemleri ("BS") denetiminin doğru yapılabilmesi için bilgi teknolojileri ("BT") denetçisinin öncelikle bilgi teknolojileri yönetimi kavramını ve bilgi teknolojileri içerisinde yer alan kontrol kavramlarını yeterli düzeyde anlaması gerekmektedir. Bu nedenle çalışmaya öncelikle bilgi sistemleri yönetimi ve temel kontrol kavramları açıklanarak başlanmaktadır.

1.1. BİLGİ SİSTEMLERİNİN TEMEL FONKSİYONLARI

Bilgi sistemi yönetimine ve bilgi sistemi tanımlarına geçmeden önce günümüzde vazgeçilmez bir yeri olan bilgisayar kavramını tanımlamak gerekmektedir. Temel olarak bilgisayar, belli bir sonuç üretmek amacıyla verilen girdilerle çeşitli işlemleri gerçekleştirmek üzere tasarlanmış çeşitli elektronik manyetik ve mekanik donanımın oluşturduğu bir sistemdir. Diğer bir ifadeyle çok temel olarak tanımlamak gerekirse, bilgisayar önceden tanımlanmış biçimde veriler kabul eden, sonrasında bu verileri işleyen ve işlem sonuçlarını da yine belirlenen amaçta ve şekilde kullanıcılara sunan veya diğer sistemlere aktaran yazılım ve donanım birimlerinden oluşan bir makinedir.[2]

Teknolojide yaşanan hızlı gelişime paralel olarak, organizasyonlarda kullanılan bilgisayar sistemleri de her geçen gün daha karmaşık bir hal almaktadırlar. Yaşanan bu hızlı gelişim ile açık sistemler, mobil sistemler, yapay sinir ağları, uzman sistemler, bilgi güvenliği, kurumsal kaynak yönetimi sistemleri gibi birçok yeni kavram hayatımıza girmiştir. Bu kadar hızlı gelişen bir sektör içinde en zor görevlerden biri de bilgi sistemleri denetçilerini beklemektedir. Söz konusu organizasyonda bilgi sistemleri denetimini gerçekleştirebilmek için öncelikle organizasyonun bilgi sistemlerini anlayabilmek, iş süreçlerini tanımlayabilmek ve

[1] Mustafa Cem Akocak, Bilgi Teknolojileri Denetiminin Esasları ve Türk Bankacılık Sektöründeki Uygulamaları (Y.L.T.2009)

[2] Melih Erdoğan, **Denetim Kavramsal ve Teknolojik Yapı**, 3. baskı (Ankara: Mal. ve Huk. Y. 2006)

bu bilgilere hangi yollar ile ulaşabileceğini bilmesi gerekmektedir. Bu nedenle bilgi sistemleri denetçisi öncelikle temel bilgisayar kavramlarına hakim olmakla birlikte gelişmelere uygun olarak bilgilerini de güncel olarak tutmak zorundadır.

Bilgisayarın tanımına paralel olarak bilgi sistemi kavramını tanımlamak gerekirse, ulaşılması istenen ortak amaca uygun olarak, girdileri kabul ederek çıktılar üreten ve birbirleriyle ilişkili bileşenlerden oluşan bir süreçtir. Daha yalın anlatımla bilgi sistemi verileri girdi olarak kabul ederek işleyen, kontrol eden, saklayan ve bilgi çıktısı olarak veren bir sistemdir.

Bilgi sistemleri yönetimi temel olarak tanımlamak gerekirse, organizasyonun amaçlarına paralel olarak bilgi sistemleri kaynaklarının etkin kullanılması ile birlikte verimli olarak yürütülmesidir[3]. Bu noktada hem organizasyonun amaçlarına destek olunması hem de organizasyona değer katılması amaçlanmaktadır. Bu yönetim sürecinin doğal bir parçası da bilgi sistemlerinin denetimi ve kontrol altında tutulmasıdır. Bilgi sistemlerinin denetim ilkelerine ve yöntemlerine diğer bölümlerde yer vermeden önce, temel bilgi sistemleri kavramlarını değinmekte yarar vardır.

1.1.1. Veri Giriş Süreci

Veri girişi süreci, işlemlerin kayıt altına alınması ile birlikle başlangıç aşamasını temsil etmekte ve bilgi sistemi sürecinin en önemli kısmını oluşturmaktadır. Zira sisteme başından yanlış olarak girilen bir verinin doğru bir sonucu vermesi de imkansız hale gelmektedir.

Günümüz teknolojisinde bir sistemin çıktısının başka bir sistemin girdisi haline geldiği bütünleşik sistemlerden oluşmaktadır. Verilerin sisteme girişi temel olarak üç aşamada ele alınabilmektedir:

1. Kaynak belgelerin içeriğinin incelenerek bilgi işlem süreci için gerekli olan bilgi türleri belirlenmektedir.
2. Verilerin sisteme girişinin yapılmasına uygun hale getirilmesi veya düzenlenmesidir.
3. Verilerin sisteme doğru bir şekilde aktarıldığından emin olmak için giriş işlemleri kontrol edilmesidir.

[3] Shelly Cashman Rosenblatt, **System Analysis and Des.** 5. Edition (USA: Thomson Learning, 2002)

Verilerin kaynağından bilgi sistemlerine ya da uygulamaya ait programlara aktarılmasındaki temel amaç değişmese de günümüzde veri girişi ile ilgili olarak birçok yöntem ve araç geliştirilmiştir. Başlıca veri giriş tekniklerden aşağıda örnekler verilerek bahsedilmiştir:[4]

1. Bar Kod Sistemi: Bilginin makineler tarafından okunabilir şekilde görsel olarak bir yüzey üzerinde sunulması, optik okuyucular ve özel veri tanıma programları aracılığıyla bu verilerin otomatik olarak bilgisayara aktarılmasını sağlayan sistemlerdir.
2. Elektronik Veri Değişimi: Genel olarak bir sistemdeki bilginin diğer bir sisteme entegre olması sağlanmaktadır. Daha geniş bir tanımla, organizasyonlar arası bilgi paylaşma ve değişim yeteneğine sahip olan bir iletişim paketi kullanılarak, bir bilgisayar ve diğeri arasında elektronik olarak bilgi değişiminin yapıldığı bir sistemdir. Bu noktada TAKBİS'e MERNİS'ten çekilen verilerin uygulamaları güzel bir örnek teşkil etmektedir.
3. Terminaller: Ana bilgisayar sistemine bağlı olarak çalışan, üstünde veri ve uygulama bulundurmayıp kullanıcının genellikle sisteme sadece veri giriş amacıyla ve ana bilgisayar sisteminden çıktı olarak gönderilen bilgileri görüntülemek amacıyla kullanılan bilgisayarlardır.
4. Görüntü Tarama ve İşleme Birimleri: Kağıt üzerindeki görüntülerin belirli formatta optik okuyucular vasıtasıyla taranması ve bilgisayara girdi olarak aktarılmasıdır. Bankalarda, kredi kartı başvuru formlarının optik okuyucular ile okunarak sisteme aktarılması bu veri girişi tekniğine güzel bir örnek oluşturmaktadır.
5. Ses Tanıma Sistemleri: Konuşmaların otomatik olarak bilgisayar sistemine girdi olarak aktarılması tekniğidir. Günümüzde gelişme aşamasında olan bir tekniktir. Özellikle bankaların dağıtım kanallarından biri olan telefon bankacılığında gelişim göstermektedir.

Yukarıda da görüldüğü gibi veri girişleri ile ilgili olarak birçok farklı ortam, süreç ve kontrol söz konusudur. Özellikle kontrol açısından bakıldığında, verinin hangi kaynaktan girdiğinin, en az verinin sisteme nasıl girdiğinin bilinmesi kadar önemli

[4] Tamer Saka, **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, Yayın:224 (İstanbul: Türkiye Bankalar Birliği, 2001), 8

olduğu unutulmamalıdır. Bilgi sistemindeki tüm süreçlere yönelik işlemler girilen bilgiler esas alınarak işleneceğinden, verilerin eksiksiz, güncel olması, verilerin doğruluğu ve bütünlüğü büyük önem taşımaktadır.

Sonuç olarak bilgi sistemleri denetçisinin en yoğun biçimde önem vermesinin gerektiği alanlardan biri girdi kontrolleridir. Daha sonraki bölümlerde açıklanacak olsa da genel olarak girdi kontrolleri; kaynak belge kontrolleri, veri kodlama kontrolleri, yığın işlem kontrolleri, girdi geçerlilik kontrolleri ve yetki kontrolleri gibi bölümlerde sınıflandırılabilmektedir.

1.1.2. Veri İşleme Süreci

Veri işleme süreci, veri girişinin tamamlanmasından sonra istenen formatta çıktı elde edilmesi amacıyla bilgisayar tarafından gerçekleştirilen tüm faaliyetleri kapsamaktadır. Gerçekleştirilen bu faaliyetleri, düzenleme, hesaplama, özetleme, sınıflandırma, güncelleştirme ve kaydetme olarak sınıflara bölebiliriz. Sırasıyla bu faaliyetleri açıklamak gerekirse;[5]

1. Düzenleme: Girilen verinin geçerliliğinin, doğruluğunun ve istenen formatta uygunluğunun kontrolü amacıyla sisteme girişi yapılan verilerin önceden tanımlı kriterlere uygunluğunun kontrol edilme işlemidir. Örneğin sisteme toplu olarak aktarılan verinin uygun veri formatında ve deseninde sisteme iletildiğinin kontrol edilmesidir.
2. Hesaplama: Bilgi sistemlerinin veri işleme süreci içinde temel olarak gerçekleştirdiği faaliyettir Veri girişi yapılan bilgiler üzerinde aritmetik hesaplamaların yapılarak istene sonuca ulaşılması faaliyeti olarak tanımlanabilir. Örneğin vadeli hesap açılışı bilgilerinden ana bankacılık sistemi üzerindeki programlar vasıtasıyla birikmiş faiz tutarının hesaplanmasıdır.
3. Özetleme: Genel olarak tanımlamak gerekirse, düzenleme ve hesaplama faaliyetlerinden sonra verinin istemem biçimde özetlenmesi ve toplamların alınmasıdır. Örneğin, müşteri bazında hesaplanan birikmiş faiz tutarlarından, aylık olarak bankanın faiz borcu rakamına ulaşması için alınan genel toplamlardır.
4. Sınıflandırma: Çeşitli dosyalarda hesaplanmış verilerin istenen çıktı formatında sınıflandırılması faaliyetidir. Yukarıdaki örneklerin devamı olarak birikmiş faiz

[5] Saka, **age**, 10

borcunun şubeler bazında ara toplamlarının alınması ve sınıflandırılması örnek olarak verilebilir.

5. Güncelleştirme: Sistem içinde mevcut olan bilgiler üzerinde yapılan ekleme, değiştirme veya silme faaliyetleriyle söz konusu bilgilerin içeriklerinde veya biçimlerinde gerçekleştirilen düzenleme faaliyetlerini ifade etmektedir. Örneğin, vadesi dolan vadeli hesap bilgilerinin ana bankacılık sistem üzerinde otomatik olarak güncellenerek ilgili hesabın kapatılması veya temdit edilmesidir.

6. Kaydetme: Herhangi bir işlemin gerçekleştirilmesinden sonra nihai sonucun elde edilmesine kadar sistem üzerinde kayıt altına alınması işlemidir. Bilgi sistemlerinin işlemleri gerçekleştirirken temel olarak tümünde gerçekleştirdiği faaliyetlerden biridir.

En az veri girişi süreci kadar, verinin doğru olarak işlenmesi de doğru ve geçerli bilgiye ulaşmak için önemlidir. Bilgi sistemleri denetçisi veri girişi kontrollerini incelediği gibi verinin doğruluğu, güvenliği ve bütünlüğü açısından aynı şekilde veri işleme sürecine yönelik kontrolleri de incelemek zorundadır. Daha sonraki bölümlerde açıklanacak olsa da genel olarak veri işleme kontrolleri; geçiş kontrolleri, işletmen kontrolleri ve denetim izi kontrolleri gibi genel sınıflara ayrılabilmektedir.

1.1.3. Veri Çıkış Süreci

Bilgi sistemi süreçlerinin son aşamasını olan veri çıkış süreciyle girilen verilerin işlenmesi sonucunda çıkan bilgiler çıktı olarak adlandırılmaktadır. Çıktılar;

- Güncellenmiş veri dosyaları
- Bilgisayar ekranındaki görüntüler
- Basılı halde olan rapor veya dokümanlar olabilmektedirler.

Çıktılar temel olarak bilgi sisteminin amacına uygun olarak işletmenin faaliyetlerini yürütmesi ve bu faaliyetleri analiz etmesi için gerekli bilgileri içeren ürünlerdir.

Çıktılar bilgi sistemlerinde kullanılan çıkış birimleri vasıtasıyla kullanılabilir hale getirilmektedir. Genel olarak bilgisayar ekranları, yazıcılar, çiziciler, ses çıktı birimleri, taşınabilir bellek ve diskler gibi kayıt ortamları çıktı birimi olarak sayılabilir.[6]

[6] Saka, **age**, s. 11

Bilgi sistemleri denetçisi olarak, çıktıların amaca uygun olarak dağıtılması, çıktı verilerinin kullanılabilirliği ve çıktılar üzerinde güvenlik sağlayıcı yöntemlerin incelenmesi temel olarak önem verilmesi gereken başlıklardır. Bu aşamada genel olarak denetçi, bilgi sistemini tanıyabilmek için öncelikle girdilerin kaynağını, yapısını ve hangi çıktıların hangi süreçler sonunda elde edildiğini en iyi şekilde anlamak zorundadır.

Her şeyden önce anlaşılmadır ki, çıktıların doğruluğu ve güvenilirliği yüksek oranda veri girişi ve veri işleme süreçlerindeki kontrollerin etkinliğine bağlıdır. Ancak kesin doğruluğu ve güvenilirliği sağlamak amacıyla çıktıların bilgisayardan alınma aşamasında da kontroller oluşturmak gerekmektedir. Çıktıların kontrolü açısından üzerinde durulması gereken üç temel nokta çıktıların doğrulanması, çıktıların dağıtımı ve özel bilgilerin veya raporların yönetimidir.

1.2. BİLGİ TEKNOLOJİLERİ YÖNETİMİ

Bilgi sistemleri yönetimi, organizasyon içindeki bilgi sistemlerinin organizasyonun hedef ve amaçlarına destek olacak şekilde idare edilmesini ve bununla birlikte organizasyona amaçları doğrultusunda değer katmaya yönlendirilmesini ifade etmektedir. Bilgi sistemlerinin yönetimine yönelik faaliyetler genel olarak dört alana ayrılarak açıklanabilmektedir:[7]

1. Sistem ve Alt Yapı Yönetimi
2. Bilgi Sistemleri Servis Sunumu ve Destek
3. Bilgi Varlıklarının Korunması
4. İş Sürekliliği ve Felaketten Kurtarma Süreci

1.2.1. Sistem ve Alt Yapı Yönetimi

Organizasyon içindeki bilgi sistemlerinin iyi bir şekilde yönetilmesi için sistem ve uygulamaların geliştirilmesi, edinilmesi veya yenileme projelerinin yürütülmesi gibi süreçlerin kontrol altında tutularak iyi yönetilmesi gerekmektedir.

Öncelikle bilgi sistemleri yönetiminin bir parçası olarak program ve proje yönetimi anlayışının bilgi teknolojileri yönetimi içinde oluşturulması gerekmektedir. Bu

[7] Everett C. Johnson, Robert D. Johnson, **CISA Review Manual 2007** (USA: ISACA, 2007), 1-2

noktada program ve proje kavramlarını birbirinden ayırarak tanımlamak gerekmektedir. Program, bir grup birbirine bağlı ve ilişkili olan projeden oluşan, genel amaçları ve bütçesi olan, bununla birlikte belirli bir zamanlamaya bağlı olarak genel bir stratejiye bağlı olarak sistem ve alt yapı yönetimi için oluşturulmuş bir plandır. Diğer taraftan, proje ise bir proje yöneticisine bağlı olarak bir alt amacı gerçekleştirmek için yönetilen sistem geliştirme veya alt yapı planının bir parçasıdır.[8] Genel olarak bilgi sistemlerinin yönetiminde yukarıdaki faaliyetlerin takibi ve belirlenen kalite kriterleri doğrultusunda proje ve programların yönetilmesi için proje yönetimi ofisleri kurulmaktadır. Kuruluşundaki esas amaç proje ve program yönetimindeki kalitenin iyileştirilmesi ve projelerin önceden belirlenen aktiviteler kapsamında başarılı olarak tamamlanmasını sağlamaktadır.

Proje yönetiminde temel olarak üç ana organizasyon yapısı kullanılmaktadır:[9]

1. Etkileme Yollu Proje Organizasyonu: Bu organizasyonda proje yöneticisi proje ekibi içinde yer alıp mutlak otoriteye sahip olmak yerine proje ekibine aktiviteleri hakkında yol gösterici tavsiyeler bulunarak projeyi yönetmektedir.
2. Temel Proje Yönetimi Organizasyonu: Genelde uygulanan bu tip proje organizasyonunda proje yöneticisi tüm proje aktivitelerinde sorumlu olup tüm ekip üzerinde mutlak otoriteye sahiptir.
3. Matris Proje Organizasyonu: Bu tip proje yönetimi organizasyonunda ise otorite proje yöneticisi ile çalışanın bağlı olduğu bölüm müdürünün arasında paylaşılmaktadır.

Proje organizasyonu türlerine ek olarak proje yönetiminin temel aşamalarından da bahsedilmesi gerekmektedir:[10]

1. Proje Başlangıcı: Proje yöneticisinin veya sponsorunun gerekli bilgiyi toplamasından sonra iş sahiplerinin proje başlatılmasına dair onayından sonra başlatılmalıdır. Genellikle proje talep dokümanının onaylanması ile projeye başlanmaktadır.

---

[8] Johnson, age, 125
[9] Johnson, age, 128
[10] Shankar Swaroop, "Managing Multiple Medium and Small Scale Projects in Large IT Organization", **Information Systems Control Journal**, volume 4 (2007), 24

2. Proje Planlaması: Talep edilen sistem geliştirmesi, iyileştirmesi veya alt yapı projesini gerçekleştirmek için gerekli proje adımlarının öncelikle proje yöneticisi tarafından ekip ile birlikte görüşerek belirlemesi gerekmektedir. Sonrasında bu proje adımlarının önceliğinin belirlenmesi, zamanlama planlaması, her birinin bütçe ve maliyet analizinin yapılması, sağlanması gereken bilgi teknolojileri kaynakları vb. gibi konularda proje yöneticisi tarafında planlama yapılması ve dökümante edilmelidir. Bu aşamada proje yöneticisine proje planı yapmasında ve proje aşamalarının ilerleyişini izlemede çeşitli teknikler yardımcı olabilmektedir. GANNT şeması, fonksiyonel nokta analizi, kritik yol metodolojisi, yazılım maliyeti ve bütçe analizi gibi teknikler kullanılabilmektedir.[11]

3. Projenin Kontrol Edilmesi: Projenin kontrol edilmesinde, belirlenen kapsamda ilerlenip ilerlenmediği, kaynak kullanımının öngörülen miktarda olup olmadığı ve projenin risk değerlendirmesinin yapılması adımlarını kapsamaktadır.

4. Projenin Kapatılması: Son adım olarak gerekli testlerden sonra proje sponsorunun ve ilgili iş sahiplerinin projeden memnun olması durumunda proje teslim edilerek kapatılmaktadır. Tabi diğer yandan projenin yanlış planlamasından ve yönetilmesinden ötürü proje maliyetlerinin artması ve istenen amaca ulaşılamayacağının anlaşılması durumunda da başarısız olarak ilgili proje durdurulup kapatılabilmektedir.

Şimdiye kadar yukarıda anlatılan kısımda proje ve programların yönetilmesini ve proje organizasyonlarının detaylarını vermiş bulunmaktayız. Tüm alt yapı / sistem geliştirme ve iyileştirme çalışmaları bir proje kapsamında ele alınarak organizasyonun amaçları doğrultusunda yönetilmelidir. Bunun yanında yazılım geliştirme veya iyileştirme (değişiklik yönetimi) sürecinin ek olarak belirli aşamalar vasıtasıyla yönetilmesi gerekmekte ve bu aşamalara bağlı olarak proje yönetimi sağlanmalıdır.

Bilgisayar uygulama sistemlerinin geliştirilmesi ve/veya iyileştirilmesi birçok faaliyeti kapsamakta olup belirli ve yazılı olan standartlara göre yönetilmelidir. Bu standartlardan en çok kullananı ve genel olanı ise şelale yönetimidir. Bu standarda göre bir yazılım geliştirme süreci minimum olarak aşağıdaki fazları sırasıyla

[11] Ian Sommerville, **Software Engineering**, 6. Edition (England: Pearson Educated Limited, 2001), 82

tanımlamalı ve yönetmelidir[12]:

1. Uygulanabilirlik Tespiti: Bu faz içinde yeni uygulamanın stratejik avantajları, sağladığı faydaları ve katlanılan maliyetleri geri ödeme zamanı analiz edilir. Sağladığı faydalar, gelecek yıllardaki maliyet azalması, üretimdeki artış imkanları gibi somut faydalar olabileceği gibi, iş süreçlerinin geliştirilmesi, kullanıcıların hazır olmaları gibi soyut faydalar da göz önünde bulundurularak genel olarak projenin uygulanabilirliği analiz edilmektedir.
2. Gereksinimlerin Belirlenmesi: Yeni bilgi sistemi geliştirme veya iyileştirme çalışmasının uygulanabilirliği onaylandıktan sonra iş gereksinimlerinin detaylı olarak belirlenmesi bu fazda yapılmaktadır. Ayrıntılı olarak iş ihtiyaçlarının tespiti projeyi bu aşamada üçüncü taraftan yeni uygulama alıp kullanmaya, alınan uygulamanın ihtiyaca uygun olarak uyarlanmasına veya sıfırdan bir uygulama geliştirmeye götürebilmektedir.
3. Tasarımın Belirlenmesi: İş gereksinimleri belirlendikten sonra bu gereksinimlere uygun olarak geliştirilecek uygulamanın teknik gereksinimleri ve tasarımı oluşturulur. Uygulamanın sistem ve alt sistemler olarak tanımlamaları, önyüzleri, üzerinde çalışacağı donanımlar, programların tasarımı, veritabanı tanımlamaları ve güvenlik ihtiyaçları gibi yazılım geliştirme aşamasını besleyecek tüm detaylar bu aşamada belirlenmektedir.
4. Yöntem Tespiti (Geliştirme veya Satın Alma): Bu safha içinde seçilen yöntem sıfırdan yazılım geliştirme ise, yazılım teknik tasarım detaylarına göre proje ekibi tarafından geliştirilir ve yine proje ekibi içindeki test işlemlerinden görevli kişiler tarafından birim ve sistem testleri gerçekleştirilir. Diğer taraftan seçilen yöntem satın alınan bir uygulamanın uyarlanması ise satın alınan uygulama iş ihtiyaçlarına ve teknik tasarım dokümanına göre üçüncü taraf firma tarafından uyarlanmakta ve test edilmektedir.
5. Yazılımın Test Edilmesi ve Uygulanması: Bu aşamada yazılımın geliştirmesi veya uyarlaması tamamlanmış olup teknik taraftaki testler de gerçekleştirilmiştir. Son kullanıcı testleri ve iş tarafının onayı alındıktan sonra uygulamanın test ortamından üretim ortamına geçişi bu safha içinde tamamlanmaktadır.

[12] Johnson, age, 140

6. Sonradan Gözden Geçirme: Uygulamanın üretim ortamına geçişinden ve organizasyon içinde kullanılmaya başlanmasından itibaren geçen ve genelde üç ay olarak belirlenen izleme evresidir. Uygulamanın üzerinde olası hataların tespit edilip düzeltilmesi ve olası iyileştirme ihtiyaçlarının tespiti için gerçekleştirilen izleme evresidir.

Bu aşamalardan en kritik olanı yeni bir uygulama ya da fonksiyon gereksinimi için alımdan ya da geliştirmeden önce iş ihtiyaçlarının etkin ve verimli bir yaklaşımla karşılandığı bir analiz gerçekleştirilmesidir. Süreç ihtiyaçların tanımlanmasını, alternatif kaynakların göz önüne alınmasını, teknolojik ve ekonomik yapılabilirliklerin gözden geçirilmesini, risk analizi ve maliyet-kazanç analizinin uygulanmasını ve 'geliştirme' ya da 'alma' son kararının neticesini içermektedir. Bütün bu adımlar, organizasyonların hedeflerini başarmaya yönelik ortamı sağlarken çözüm alma ve uygulama maliyetini düşürmesini sağlamaktadır. Yukarıdaki açıklanan şelale metodolojisinde ilk iki faz bu işlevi yerine getirmektedir.

1.2.2. Bilgi Teknolojileri Servis Sunumu ve Destek

Bilgi sistemleri operasyonun günlük olarak yönetimi ve bilgi sistemleri kapsamında organizasyonun ihtiyaçlarına göre desteklenmesi bilgi sistemleri yönetiminin servis sunumu ve destek başlıklı bölümünü oluşturmaktadır. Bilgi sistemleri operasyonunun yönetimi ve servis sunumu ile ilgili olarak gerçekleştirilen başlıca faaliyetler şu şekilde açıklanabilmektedir[13]:

1. Bilgi Teknolojileri Servis Yönetimi: Dış tedarikçiler tarafından sağlanan servislerin iş taleplerine uygun olduğundan emin olabilmek için dış tedarikçi yönetim sürecine gereksinim bulunmaktadır. Bu süreç, dış tedarikçi anlaşmalarında rol, sorumluluk ve beklentilerin açıkça tanımlanmış olması gerektiği kadar anlaşmaların yararlılığının ve uygunluğunun gözden geçirilmesi ve izlenmesiyle de başarılmaktadır. Örneğin bankaların ATM ("Automatic Teller Machine") alımı yaptığı firmalar ile ilişkileri ihtiyaca uygun olarak belirlemesi ve takibini yapması bu kapsama girmektedir. Bunun yanında organizasyon içindeki iç müşterilere sunulan hizmetlerin tanımlanması, her servisin belirli servis seviyesi anlaşmasına bağlanması, takibinin yapılması ve raporlamasının yapılması ikinci bu faaliyetlerin diğer kısmını

[13] Johnson, age,256

oluşturmaktadır. Bu alanda da örnek vermek gerekirse bilgi teknolojileri bölümünün banka içindeki bölümlere ve/veya holding içindeki diğer iştiraklere sağladığı servisleri tanımlı olan servis seviyesi anlaşmalarına göre yönetmesidir.

2. Alt Yapısal Bilgi Sistemleri Operasyonları: Genel olarak bilgi sistemleri için önceden tanımlı olan ve belirli bir zamanda çalışması gereken işlerin tam, etkin ve zamanında çalışmasını sağlanmasıdır. İlgili işlerin çalıştırılması, olası hatalara karşı bu işlerin takibinin yapılması, oluşabilecek sistem durmalarına karşı sistemin tekrar ayağa kaldırılması, sistem yedeklerinin zamanında ve belirlenen sıklıkta alınması ve sistem kaynaklarının verimli kullanılmasının, performansın, kapasitenin ve erişilebilirliğin izlenmesi gibi bilgi sistemleri operasyonları gerçekleştirilmektedir. Genel olarak organizasyon içindeki mevcut bilgi sisteminin çalışır durumda tutulması ve organizasyon içindeki desteğinin kesintiye uğramaması için bu kapsamda hizmet sunumu gerçekleştirilmektedir.

3. Vaka ve Problem Yönetimi: Bu faaliyet kapsamını açıklamadan önce vaka ve problem kavramlarını tanımlamak gerekmektedir. Vaka, bilgi sistemleri üzerinde meydana gelen ve olağan olmayan her türlü durum tespitidir. Örneğin banka şubesinin ağ üzerideki bağlantısının kısa süreli olarak kesilmesi veya sistemdeki boş kapasitenin eşik değerinin üzerine çıkması gibi. Problem ise tespit edilen vakaların kendini tekrar etmesi ile kendini açıkça belli eden ve ilerleyen safhalarda kronik duruma gelen olağan dışı durumlardır. Aynı örneğimize devam edecek olursak, belirli bir şubenin ağ bağlantısı her gün kopuyorsa mevcut kronik bir problemin tespiti yapılmalıdır. Bu kapsamda öncelikle mevcut bilgi sistemlerin olası vakalara karşı izlenmesi ve bu sürecin de yine etkin bir problem ve değişiklik yönetimi ile desteklenmesi gerekmektedir. Etkin problem yönetimi problemlerin belirlenerek sınıflandırılmasını, sebep-sonuç analizini ve problemlerin çözümünü gerektirir. Problem yönetim süreci aynı zamanda iyileştirme çalışmaları için gelen önerilerin kaydedilmesi, problem kayıtlarının saklanması ve kayıt üzerine yapılan düzeltici hareketlerin statülerinin gözden geçirilmesini içerir. Etkin problem yönetim süreci bilgi sistemlerinin hizmet kalitesini artırır, maliyetleri azaltır ve kullanıcıların memnuniyetini artırır[14].

4. Değişiklik Yönetimi: Son kullanıcılardan gelen taleplere veya tespit edilen bir

[14] ISACA**, IT Assurance Guide** (USA: 2007), 205

probleme göre mevcut sistemlerde bazı yazılımsal veya donanımsal değişikliklere gidilebilmektedir. Mevcut sistemler üzerinde gerçekleştirilen yazılım veya alt yapı değişiklikleri de belirli bir yönteme uygun olarak tasarlanmış değişiklik yönetimine bağlı olarak gerçekleştirilmelidir. Üretim ortamı içinde altyapı ve uygulamalarla ilgili tüm değişiklikler, acil bakım ve yamalar da dahil olmak üzere, resmi olarak kontrollü bir şekilde yönetilmelidir. Değişiklikler (prosedürler, prosesler, sistem ve hizmet parametreleri dahil olmak üzere) uygulamadan önce kayıt altına alınmalı, değerlendirilmeli, yetkilendirilmeli ve uygulamayı müteakip planlanmış sonuçlara göre incelenmelidir. Bu kapsamda gerçekleştirilen hizmetler ise değişiklik yönetimi faaliyetleri adı altında yer almaktadır.

5. Kütüphane Yönetimi ve Kalite Kontrol: Bilgi sistemlerinin kaynak kodlarının bütünlüğünün ve güvenliğinin sağlanması açısından aktarımın, saklamasının ve güncellenmesinin yönetilmesidir. Genel olarak kütüphane yönetim uygulamaları yardımıyla test ve üretim ortamı kütüphaneleri ayrılarak kaynak kodların güvenliği sağlanmakta ve yetkili onaylardan sonra kütüphanelerdeki kaynak kodlar güncellenmektedir. Bunun dışında sistem üzerindeki değişikliklerin onaylanması, test edilmesi ve kontrollü bir şekilde üretim ortamında uygulaması gibi konularda kalite kontrolün yapılması ve gözlenmesi de hizmet sunumu faaliyetleri kapsamında gerçekleştirilmektedir.

1.2.3. Bilgi Varlıklarının Korunması

Bilgi varlıklarının korunması bilgi sistemleri yönetimin en kapsamlı ve en önemli faaliyetlerinden biridir. Varlıklara sistem odalarındaki fiziksel erişimlerimden başlayarak son kullanıcının bilgi güvenliği konusunda bilinçlendirilmesi ve mantıksal erişim kontrollerine kadar çok geniş bir kapsamı içine almaktadır. Genel olarak sekiz faaliyet alanına bölünerek bilgi varlıklarının korunması kapsamında bilgi teknolojileri bölümünün gerçekleştirdiği görevler aşağıda açıklanmaktadır.

1. Bilgi Güvenliği Yönetimi: Bilgi bütünlüğünün sağlanılması ve bilgi teknolojileri varlıklarının korunması için öncelikle bir güvenlik yönetim süreci bulundurulmaktadır. Bu süreç, bilgi teknolojileri güvenlik rollerinin oluşturulması ve rollerin düzenli gözden geçirilmesi ve bakımını içermektedir. Ayrıca ilgili politikaların, standartların ve prosedürlerin oluşturulması gerekmektedir. Güvenlik

yönetimi bunların dışında, güvenlik izlemesini, periyodik güvenlik testlerinin yapılmasını ve belirlenmiş güvenlik açıklarının kapatılması uygulamalarını da kapsamaktadır. Etkin olarak işleyen bir bilgi teknolojileri güvenlik yönetimi güvenlik açıklarından doğabilecek olumsuz etkileri en düşük seviyede tutmalı ve bilgi varlıklarını etkin bir şekilde korumalıdır[15].

2. Bilgi Teknolojileri Güvenlik Planı: Bilgi teknolojileri güvenliğinin en yüksek organizasyon seviyesinde yönetilmesi gerekmekte birlikte, organizasyon içinde yürürlükte bulunan bir bilgi teknolojileri güvenlik planı oluşturulur. Bu plan kurumsal bilgi işlem kullanımı, bilgi teknolojileri yapılanışı, bilgi risk ve hareket planları ile bilgi güvenlik kültürünü içermektedir. Bilgi teknolojileri güvenlik planı, organizasyonun güvenlik politika ve prosedürlerinde uygulanır; şirket hizmet, personel, yazılım ve donanıma gerekli yatırımı yaparken bu plan göz önüne alınır.

3. Kimlik Yönetimi: Bilgi teknolojileri güvenlik planı ve prosedürlerinin yanı sıra, bilgi sistemleri üzerinde tüm kullanıcıların aktiviteleri (iş uygulamaları, sistem operasyon, geliştirme ve bakım) tek başlarına tanımlanabilir hale getirilir. Kullanıcıların sistemlere ve veriye erişim hakları; tanımlanmış ve dökümante edilmiş iş ihtiyaçları ve görev gereksinimleri ile uyumlu olarak tasarlanmaktadır. Kullanıcı erişim hakları; kullanıcının yöneticisi tarafından talep edilmeli ve sistem sahibi tarafından onaylanmalıdır[16].

4. Kullanıcı Hesaplarının Yönetimi: Kullanıcı hesaplarının ve ilgili kullanıcı haklarının talep edilmesi, oluşturulması, kullanıcılara atanması, askıya alınması ve kapatılması işlemlerinin ne şekilde gerçekleştirileceği kullanıcı hesapları yönetimi sürecinde belirlenmiştir. Veri veya sistem sahiplerinin onayıyla talep edilen erişim haklarının kullanıcılara verilmesi süreci kullanıcı hesapları yönetimi dahilindedir. Kurumsal sistemler ve bilgi kaynaklarına erişim ile ilgili haklar ve yükümlülükler her tip kullanıcı için sözleşmeye dayalı olarak düzenlenir. Ek olarak tüm hesaplar ve ilgili erişim hakları düzenli olarak yönetim tarafından gözden geçirilir.

5. Güvenlik Testleri: BT güvenlik uygulamaları test edilmeli ve aktif olarak gözlemlenmelidir. BT güvenliğinin; onaylanmış güvenlik seviyesinin sürdürülmesini sağlamak için düzenli aralıklarla kalitesi arttırılır. Arşivleme ve fonksiyon

[15] ISACA, **COBIT: Control Objectives for Information and related Technology 4.1** (USA, 2007), 118

[16] ISACA, **COBIT**, 118

gözlemlenmesi; tespit edilmeye gerek duyabilecek seyrek veya olağandışı aktiviteleri erken tanısını bu faaliyetler yardımıyla mümkün kılınmaktadır. Arşiv verisine erişim; erişim hakları ve alıkoyma gereksinimleri açısından, iş gereksinimleri ile uyumlu olmalıdır.

6. Güvenlik Vakalarının Yönetimi: Potansiyel güvenlik vakalarının karakteristikleri açık şekilde tanımlanır ve bildirilir; bu şekilde güvenlik vakaları, vaka ve problem yönetimi süreci vasıtasıyla uygun şekilde düzeltilir. Karakteristikler, neyin güvenlik vakası olarak tanımlanacağını ve etki seviyesini içerir. Kısıtlı sayıdaki etki seviyeleri açıklanır ve ihtiyaç duyulan her belirli aksiyon ve bildirime ihtiyaç duyulan kişiler için tanımlanır.

7. Zararlı Yazılımların Önlenmesi: Organizasyon bünyesinde bilgi teknolojileri sistemlerini, virüs, solucan, casus yazılım ve iç veya dış kullanıcılar tarafından geliştirilmiş diğer zararlı yazılımlardan koruyacak, önleyici, tespit edici ve düzeltici sistemlerin mevcut olması sağlanmaktadır.

8. Ağ Güvenliği: Güvenlik tekniklerinin ve ilgili yönetim prosedürlerinin (örneğin firewall, güvenlik cihazları, ağların bölümlenmesi ve istenmeyen girişlerin tespiti) girişleri onaylamak ve ağ içinde akan bilginin kontrol edilmesi için kullanılması sağlanmaktadır[17].

Yukarıdaki faaliyet alanlarından da anlaşılacağı gibi bilgi güvenliği ve varlıkların korunması ayrı alanlarda ancak aynı amaca paralel olarak sürdürülmesi geren bir bilgi sistemleri yönetim faaliyetlerinden birisidir.

1.2.4. İş Sürekliliği ve Felaketten Kurtarma Süreci

Organizasyon için iş sürekliliğinin sağlanması diğer bir deyişle faaliyetlerinin sürdürebilmesi, belirlediği hedeflerin gerçekleştirilebilmesi için hayati önem taşımaktadır. Günümüz teknolojisinde mevcut operasyonel faaliyetlerin bilgi teknolojileri servislerine oldukça bağımlı olduğu düşünülürse bilgi teknoloji servislerinin devamlılığını sağlamak da hayati önem taşımaktadır.

Bu sebepledir ki, bilgi teknolojileri ("BT") hizmetlerinin sürekliliğini sağlamak amacıyla BT süreklilik planı geliştirilmeli ve bu plan belli aralıklarla gözden geçirilmelidir. Ayrıca bu plan test edilmeli ve ilgili kişilere süreklilik planı ile ilgili

[17] ISACA, **COBIT**, 118

eğitimler verilmelidir[18].

Ek olarak alınan sistem ve veri yedekleri ofis dışında saklanmalıdır. Etkin olarak işleyen sürekli hizmet süreci, temel iş fonksiyonları ve süreçleri üzerindeki BT hizmetinin kesilmesinden doğan negatif etkiyi azaltmaktadır.

İşletmenin yönetim desteğinin devamlılığının için tutarlı bir süreçle bilgi sistemleri sürekliliği için yapı geliştirilmelidir. Yapının amacı; karar verilmiş altyapı gereksinimlerine yardımcı olmak, felaket kurtarma ve bilgi sistemleri olasılık planlarını yürütmektir. Yapı; yönetim devamlılığı için organizasyon yapısını, rolleri, görevleri ve iç ve dış tedarikçileri, onların yönetimini ve müşterilerini, kuralları, doküman hazırlanışı, felaket kurtarma ve bilgi sistemleri olasılık planlarının test edilip uygulanmasını da kapsamalıdır. Bu plan aynı zamanda kritik kaynakların tanımı, erişilebilir kritik kaynakların izlenmesi ve raporlanması, alternatif süreçler, kurtarma ve yedekleme kuralları gibi konular hakkında bilgi vermelidir[19].

Bilgi sistemleri devamlılık planları geliştirilirken anahtar iş fonksiyonlarındaki ana bozulmaların etkisini azaltacak şekilde tasarlanmalıdır. Esneklikle oluşturulmuş bilgi sistemleri devamlılık planında en kritik olarak belirtilen konulara dikkat edilmelidir ve felaket durumlarında öncelikler belirlenmelidir. Planlar; esneklik, alternatif işleyiş, tüm kritik bilgi sistemleri hizmetleri için kurtarma kapasitesi için gereksinimleri kapsamalıdır[20].

Ayrıca, kullanım kılavuzları, görevler ve sorumluluklar, prosedürler, iletişim süreçleri ve test yaklaşımı hakkında bilgi de içermelidir. Bilgi sistemleri devamlılık planı içinde masraflar kabul edilebilir bir seviyede tutulurken, sözleşmeler ile yasal gereksinimlere uyulurken; daha az kritik olan noktaların kurtarılmasından kaynaklanan dikkat dağınıklığından kaçınılmalı, tepkilerin ve kurtarmanın öncelikli iş gereksinimleriyle aynı doğrultuda olması sağlanmalıdır. Dört saatte bir, 24 saatte dört kez, 24 saatten daha fazla ve kritik işlerin operasyon süreleri gibi farklı diziler için esneklik, tepki ve kurtarma gereksinimleri plan içinde hesaba katılmalıdır.

---

[18] TUBİTAK UEKAE, **Yedekleme ve İş Sürekliliği Kontrol Listesi**, 1

[19] ISACA, **COBIT**, 114

[20] Edward S. Devlin, Cole H. Emerson ve diğerleri, "**Business Resumption Planning**" (USA: AUERBACH, 2000), II-2

Bilgi sistemleri süreklilik planı oluşturduktan sonra işletmenin görevi sona ermemektedir. Plan her daim güncel tutulması için ve devamlı olarak gerçek iş gereksinimlerine yanıt verdiğinden emin olmak amacıyla, değişiklik kontrolü prosedürlerinin tanımlanması ve uygulanması gerekmektedir. Prosedürdeki değişikliklerin ve sorumlulukların açık bir şekilde ve zamanında tartışılması önemlidir. Bu noktada bilgi sistemleri süreklilik planının; bilgi sistemlerinin etkili olarak kurtarıldığından, noksanlıkların belirlendiği ve planın hala uygun olduğundan emin olmak amacıyla periyodik olarak test edilmelidir. Bu test; dikkatli hazırlığı, belgelemeyi, test sonuçların raporlanmasını ve sonuçlara göre eylem planı hazırlanmasını gerektirmektedir. Tek uygulamaların kurtarılmasının testinden, tüm test aşamalarını baştan sona kapsayan test senaryolarına ve tedarikçi testine kadar olan kapsam değerlendirilmelidir[21].

Bunun yanında ilgili tüm birimlerin; prosedürler, sahip oldukları roller ve kaza ya da felaket anında yerine getirecekleri sorumluluklar hakkında düzenli eğitim almaları temin edilmelidir. Planların uygun ve güvenli bir şekilde dağıtıldığından ve ihtiyaç duyulan yerde ve zamanda yetki verilmiş ilgili birimlerin uygun bir şekilde erişebildiğinden emin olmak adına tanımlanmış ve gözetilmiş bir dağıtım stratejisi bulunmalıdır. Tüm felaket senaryoları durumunda planların erişilebilir olmasına dikkat edilmelidir[22].

İş sürekliliğinin sağlanması ve BT kaynaklarının, bir ciddi sorun veya felaket durumunda tekrar çalışır hale gelmesi için, bütün kritik yedekleme üniteleri, ilgili dokümantasyon ve kritik BT kaynakları ofis dışında saklanmalıdır. Alınacak yedekler ve içerikleri iş süreç sahipleri ve BT personeli işbirliği ile kararlaştırılmalıdır. Ofis dışındaki yedekleme ünitesi, kurumun veri sınıflandırma politikasına ve genel veri depolama uygulamalarına uygun olmalıdır. BT Yönetimi ofis dışı düzenlemelerinin periyodik olarak, en azından yıllık olarak; içerik, genel güvelik ve fiziksel güvenlik açısından kontrol edildiğinden emin olmalıdır. Arşivlenmiş verinin geri döndürülebilmesi için kullanılan donanım ve yazılımın kurumun temel sistemlerine uyumluluğu kontrol edilmeli ve periyodik veri geri döndürme testleri yapılmalıdır.

---

[21] ISACA, **IT Continuity Planning Audit/Assurance Program**, www.isaca.org [01.03.2009], 33

[22] ISACA, **IT Continuity Planning Audit/Assurance Program**, www.isaca.org [01.03.2009], 35

Bilgi sistemleri yönetiminin; felaket sonrasında, bilgi sistemlerinin işlevini başarılı şekilde devam ettirilmesinde, planın yeterliliği ve düzenli olarak güncellendiğini değerlendirmek için prosedürler oluşturup oluşturmadığına karar verilmelidir.
Sonuç olarak yukarıda bahsettiğimiz faaliyetleri, bilgi teknolojileri birimi ile yönetim eş güdümlü olarak çalışması sonucu iş sürekliliği servisi sunulmaktadır. Bu noktada bilgi teknolojileri bölümünün görevi iş tarafından gelen iş sürekliliği ihtiyaçlarına göre bilgi sistemlerini ayağa kaldırmak ve devamlılığını sağlayabilmektedir.

1.3. BİLGİ TEKNOLOJİLERİ KONTROLLERİNİN KAPSAMLARINA GÖRE SINIFLANDIRILMASI

Bilgi sistemleri denetçisi organizasyonun bilgi sistemleri faaliyetlerini değerlendirirken, kapsamlarına göre inceleyeceği bağlıca iki tip kontrol alanı vardır. Bunlardan ilki bilgi teknolojileri genel kontrol ortamına yönelik genel kontroller, diğeri ise spesifik bir uygulamaya yönelik uygulama kontrolleridir.
Her iki kapsamda da denetçi önleyici veya belirleyici kontrolleri tespit edip değerlendirmesini yapacaktır. Önleyici kontrol isminden de anlaşılacağı gibi problem çıkmadan önce problemi önleyen kontrollerdir. Örneğin güvenlik önlemi olarak şifrelerin belirli sayıda hatalı giriş denemesinden sonra hesabın kilitlenmesidir. Diğer kontrol tipi ise belirleyici kontrol olup olası meydana gelen bir hatanın tespitini sağlamaktadır. Buna örnek olarak sistem üzerinde gerçekleşen veri aktarımlarına yönelik girdi ve çıktı alanları arasında otomatik mutabakat kontrollerinin yapılması verilebilir.
Kapsamlarına göre bilgi teknolojileri kontrolleri ikiye ayrılarak sonraki bölümlerde ayrıntılı olarak açıklanmaya çalışılacaktır.

1.3.1. Bilgi Teknolojileri Genel Kontrol Ortamı

Kurum/İşletme içerisinde kullanılan tüm sistemlerde meydana gelebilecek hataları veya yoksulsuzlukları önlemeyi ve/veya belirlemeyi hedefleyen politikalara, prosedürlere veya uygulamalara bilgi teknolojileri genel kontrolleri adı verilmektedir. Genel kontrollerin amacı organizasyon genelinde mevcut bilgi sistemleri faaliyetleri üzerinde etkin bir kontrol sistemi tesis ederek iç kontrol ortamı ile ilgili belirlenmiş amaçlara ulaşılmasına yardımcı olmaktır. Genel olarak

bağımsız finansal denetim kapsamından da bilindiği üzere iç kontrol ortamının etkinliği sonradan yapılacak olan maddi doğruluk testlerinin kapsamını ve harcanacak zamanı etkilemektedir. Benzer olarak bilgi sistemleri genel kontrol ortamının etkinliği de uygulama kontrollerinin kapsamını ve güvenilirliğini de aynı şekilde etkilemektedir. Şekil ile daha açık anlatılması gerekirse[23];

Şekil 1: Zayıf BT Genel Kontrol Ortamı

BT genel kontrol ortamı zayıf olan bir ortamda uygulama kontrollerinin etkinliği de zayıf olacaktır. Bunun asıl sebebi tasarlanan uygulama kontrollerinin mevcut BT genel kontrol ortamının üstüne tesis edilmesidir.

Şekil 2: Güçlü BT Genel Kontrol Ortamı

Bir önceki şeklin aksine BT genel kontrol ortamı sağlam olan bir organizasyon içinde uygulama kontrollerinin etkinliği ve güvenilirliği de aynı derecede artacaktır.

[23] KPMG, **KPMG IT Audit Methodology Presentation**, www.kworld.com, [05.03.2009]

Genel kontrol ortamı kontrolleri sınıflandırarak anlatılmadan önce özet olarak organizasyon genelindeki bilgi sistemleri kontrol ortamının şekil yardımıyla açıklanması yerinde olacaktır[24].

Şekil 3: BT Kontrol Ortamları

Şekilden de anlaşılacağı gibi örgütsel BT kontrol ortamı üzerine BT genel kontrol ortamı onunda üzerine BT uygulama kontrolleri organizasyon içinde tesis edilmektedir. Aynı bir binanın temelinin sağlam olmasının gerekliliğine benzer bir şekilde bir alt bölüm üsttekinin etkinliğini ve güvenilirliği destek olmaktadır.

[24] KPMG, **KPMG IT Audit Methodology (KAM)**, www.kworld.com [23.03.2009]

İKİNCİ BÖLÜM

2. BİLGİ SİSTEMLERİ DENETİMİ STANDARTLARININ SAĞLANMASI

Bilgi sistemleri denetimi ile ilgili olan faaliyetleri düzenleyen standart ve prensipleri temel olarak üç grupta inceleyebiliriz. Bu noktada bilgi teknolojileri denetçisi kaliteli bir denetim faaliyeti yürütebilmek için işlemlerinde öncelikle;

1. Genel kabul görmüş denetim ilkeleri ve denetim standartlarına uyması,
2. Ayrıntılı denetim çalışmaları için uzmanlarca hazırlanmış denetim standartları ve işlemlerine uyması,
3. Son olarak ise bilgi teknolojisi süreçlerinin zorunlu kıldığı denetim tekniklerini kullanması gerekmektedir.

Genel kabul görmüş denetim ilkeleri ve denetim standartları, her bir denetim faaliyeti için denetçilere ayrıntılı olarak yol gösteren ve onlara denetim sırasında neler yapmaları, hangi denetim işlemlerine başvurmaları gerektiği gibi hususlarda ayrıntılı bilgi veren standartlar olmasa da, tüm denetim çalışmalarında olduğu gibi genel belirleyici özelliğe sahip bu standartlara uyulması gerekmektedir. Genel kabul görmüş denetim ilkeleri ve denetim standartları, denetim çalışmasının yürütülmesi, bulguların elde edilmesi ile ilgili genel kabul görmüş standartlardan oluşmaktadır. Buna göre üç ana grupta bu standartlar toplanabilmektedir[25]:

1. *Genel standartlar*: Bu standartlar denetçi ile onun çalışmasın kalitesi ile ilgili standartlardan oluşmaktadır. Mesleki eğitim ve yetkinlik standardı, bağımsız davranabilme standardı ve mesleğin gerektirdiği özenin gösterilmesi standardından oluşmaktadır.
2. *Çalışma sahası standartları*: Çalışma sahası standartları ise dış denetçi tarafından denetim çalışmalarında izlenecek yöntemleri gösterir. Denetimin ne şekilde, hangi önceliklerde ve hangi yöntemlerle yapılacağı çalışma sahası standartları ile

[25] Duman, age, 44

belirlenir. Bu standartlar planlama ve gözetim, iç kontrol sisteminin incelenmesi ve kanıt toplamaya ilişkin standartlardan oluşur.

3. *Raporlama standartları*: Raporlama standartları denetim sonucunda varılan görüşün açıklandığı raporların kapsam ve düzenlemeleriyle ilgili standartlardır. Genel kabul görmüş denetim on denetim standardından dördü denetim raporunun konusunu içermektedir. Bunlar, genel kabul görmüş muhasebe ilkelerine uygunluk standardı, genel kabul görmüş muhasebe ilkelerine değişmezlik standardı, mali tablolardaki açıklamaların yeterliliği standardı ve görüş bildirime standardıdır. Görüldüğü gibi görüşün alınması gerektiği konuların raporda yer alması ve görüşün nasıl belirtileceği ile ilgili tüm maddeler raporlama standartlarına göre belirlenmiş durumdadır.

Bilgi teknolojileri ile ilgili denetim standartları söz konusu olduğunda AICPA, IIA ("İç Denetim Derneği") ve ISACA ("Bilgi Sistemleri Denetimi ve Kontrolü Derneği") adlı üç kuruluşun çalışmaları göze çarpmaktadır.

Amerika Birleşik Devletleri sınırlarında resmi bir meslek kuruluşu olarak yaptırım gücüne sahip olan AICPA, denetim faaliyetlerinin yürütülmesinde belirleyici rol oynamaktadır. Kuruluş oluşturduğu denetim standartları, denetim yorumları ve denetim el kitapları ile denetim mesleğinin icrasında rehberlik teme görevini üstlenmiştir. Bilgi sistemlerinin denetimi ve ilgili faaliyetleri kapsamında AICPA bünyesinde "*Bilgisayar Denetimi Alt Komitesi*" kurulmuştur[26].

Planlama ve denetim stratejilerinin belirlenmesi, denetimin yürütülmesi ve tamamlanması ve denetim sonuçlarının ve raporların iletimi ile ilgili olarak bilgi sistemleri denetimine dolaylı veya dolaysız yoldan yol gösterecek standartlar oluşturulmuştur.

AICPA gibi resmi kurumların yanında İç Denetim Derneği gibi bir sivil toplum kuruluşu bilgi teknolojileri faaliyetlerini de kapsamına alacak standartlar geliştirmiştir. Bu kapsamda oluşturulan denetim standartlarının bazıları şöyledir[27]:

1. 310 Bilginin Güvenilirliği ve Bütünlüğü

2. 320 Politikalar, Planlar, Kanunlar ve Düzenlemelere Uyumluluk

[26] Saka, age, 78

[27] AICPA, **Audit Standards**, www.aicpa.org

3. 330 Varlıkların Korunması

4. 340 Kaynakların Ekonomik ve Etkin Kullanılması

5. Faaliyet veya Programlar için Belirlenmiş Amaç ve Hedeflerin Gerçekleştirilmesi

Son olarak sivil toplum kuruluşlarından biri olan Bilgi Sistemleri Denetimi ve Kontrolü Derneği ("ISACA") de bilgi sistemleri denetiminin standartlarına yönelik çalışmalar oluşturmuş ve birçok araştırma gerçekleştirmiştir. Bu kapsamda bilgi sistemleri denetimine yönelik olarak 16 standart ve 40 adet bilgi sistemleri denetim prensipleri belirlemiştir. Belirlenen bilgi sistemleri standartları, şu şekilde sıralanıp açıklanabilmektedir[28]:

1. *Denetim Tüzüğü*:Bilgi sistemleri denetim fonksiyonunun amacını, sorumluluğunu, otoritesini ve yerini tanımlayan standarttır.
2. *Bağımsızlık*: Bilgi sistemleri denetçilerinin profesyonel anlamda ve organizasyon içindeki bağımsızlıklarını tanımlayan standarttır.
3. *Profesyonel Etik ve Standartlar*: Bilgi sistemleri denetçisinin görevlerini yerine getirirken uymaları gereken profesyonel etik kuralları belirleyen standarttır.
4. *Profesyonel Yeterlilik*: Bilgi teknolojileri denetçisinin profesyonel anlamada görevlerini yerine getirmek için sahip olması ve sürdürmesi gereken yetkinliği açıklayan standarttır.
5. *Planlama*: Risk odaklı bilgi sistemleri denetiminin nasıl planlanması ve yürütülmesi gerektiğini açıklayan standarttır.
6. *Denetim Çalışmasının Gerçekleştirilmesi*: Bilgi sistemleri denetiminin yürütülmesi, kanıt toplanması ve çalışma kağıtlarının hazırlanması ile ilgili açıklayan standarttır.
7. *Raporlama*: Bilgi sistemleri denetim sonuçlarının raporlanması ile ilgili açıklamayı yapan standarttır.
8. *Takip Çalışmaları*: Bilgi sistemleri denetim sonucunun raporlanması sonrası bulguların ve tavsiyelerin gerekli aksiyon planlarına göre takibinin yapılmasını açıklayan standarttır.
9. *Uyumsuzluklar ve Yasal Olmayan Durumlar*: Denetim riski kapsamında bilgi

[28] ISACA, **IT Audit Standards**,

sistemleri denetiminde olası uyumsuzlukların ve yasal olmayan durumların değerlendirilmesi ile ilgili olan standarttır.

10. *Bilgi Teknolojileri Yönetişimi:* Organizasyon hedefleri ile uyumlu bir bilgi teknolojileri yönetiminin tesisi ile ilgili açıklamada bulunan standarttır.

11. *Denetim Planında Risk Değerlendirmesinin Kullanımı*: Bilgi sistemleri denetim faaliyetlerinin planlanması öncesinde risk değerlendirmesinin kapsamını açıklayan standarttır.

12. *Denetimde Önemlilik*: Bilgi sistemleri denetiminde önemlilik kavramının değerlendirilmesi ve denetim riskinin belirlenmesi ile ilgili açıklamaları yapan standarttır.

13. *Başkalarının Denetim Çalışmalarını Kullanma*: Bilgi sistemleri denetimi sırasında başkalarının (örneğin iç denetim çalışmaları) çalışmalarının değerlendirilmesi ve kullanılması ile ilgili açıklama yapan standarttır.

14. *Denetim Kanıtları*: Bilgi sistemleri denetimi sonucunun güvenilir olarak verilmesi için yeterli ve güvenilir kanıt toplama ile ilgili açıklamaların yapıldığı standarttır.

15. *Bilgi Teknolojileri Kontrolleri*: İç kontrol sisteminin bir parçası olarak bilgi teknolojileri kontrollerinin incelenmesi ve değerlendirilmesi ile ilgili açıklamaları yapan denetim standardıdır.

16. *Elektronik Ticaret*: Son olarak elektronik ticaret ile ilgili olarak uygun kontrollerin belirlenmesi ve incelenmesi ile ilgili açıklama yapan denetim standardıdır.

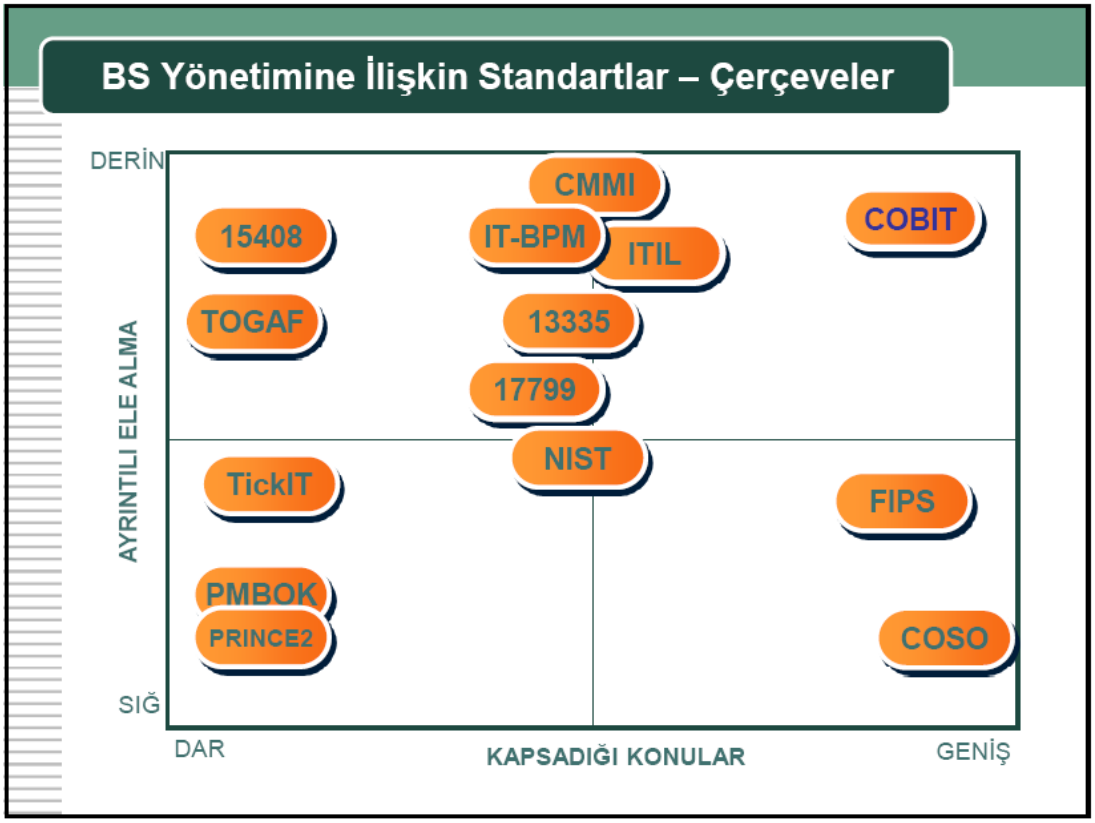
Son olarak ise bilgi teknolojisi süreçlerinin zorunlu kıldığı denetim tekniklerini kullanması gerekmektedir. Bu noktada yukarıda bahsetmiş olduğumuz denetim standartlarının yanında incelenen bilgi sistemlerine göre özel olarak hazırlanmış denetim tekniklerinin bulunduğu denetim programları mevcuttur. Örneğin SAP kurumsal kaynak planlaması sistemi inceleniyorsa, bilgi teknolojileri genel kontrol ortamının denetimi için hazırlanmış özel denetim programları da kullanılabilmektedir.

Bilişim teknolojileri yönetişimini sağlayabilmek için bilinen, dünyaca kabul görmüş yaklaşımlar, standartlar ve modeller bu bölümde anlatılıyor olacaktır. Bu araç ve yöntemleri uygulamaya geçmeden önce bunların hangi amaçla, nerede ve nasıl

kullanılacağına karar verebilmek önemlidir.

Bu çalışmada ise ele alınmış olan tüm bu çalışmaların, temelde, bilişim teknolojileri yönetişimine hizmet edebilecek alanlar olduğu vurgulanacak; aşağıdaki bilgiler doğrultusunda, adı geçen araç ve yöntemleri kullanarak daha güçlü bir bilişim teknolojileri yönetişiminin nasıl sağlanabileceğine dair bilgiler verilecektir.

Şekil 4: Bilgi Sistemleri Denetimine İlişkin Standartlar



Şekil 5: Standartların Çerçevesi

2.1. ÇERÇEVE DOKÜMANLAR VE STANDARTLAR

2.1.1. COBIT

Bilişim teknolojileri süreçlerinin yönetiminde kullanılan modellerden biri olan ve iş yöneticileri için geliştirilen COBIT (**Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri** - Control Objectives for Information and related Technology), esas itibariyle bilişim teknolojileri süreçleriyle ilgili kontrol hedeflerinden ve denetim çerçevesinden oluşmaktadır[29].

COBIT (Bilgi ve İlgili Teknoloji için Kontrol Amaçları), Bilgi Sistemleri Denetim ve Kontrol Birliği tarafından bir denetim aracı olarak tasarlanmıştır ama bilgi işlem ve iş yönetiminde de kullanılan bir araçtır. COBIT, bilgi ve ilgili teknoloji için kontrol amaçları yaklaşımıdır ve ulaşılmak istenen kontrol amaçları ve bu amaçlara ulaşmak için gerekli yollar tarafından tasarlanan kontroller olarak tanımlanan iç kontrol odaklı bir yaklaşımdır. İşletmenin iş hedefleri doğrultusunda

[29] Türkiye Bilişim Derneği-Bilişim Teknolojilerinde Yönetişim, 1. Çalışma Grubu sf. 21

hizmet vermesini sağlamak amacıyla bilgi işlem kaynaklarını kullanmasını amaçlar ve verilen hizmetlerin, istenilen kalite, güvenlik ve hukuksal ihtiyaçlara cevap vermesini sağlar. COBIT süreç değil kontrol esaslıdır.

COBIT yöneticinin, kontrol gereksinimleri, teknik konular ve iş riskleri arasındaki boşluklar arasında köprü kurmasına yardımcı olan yönetişim çatısı ve destekleyici araçlardır. COBIT, organizasyon genelinde bilgi teknolojisi kontrolü için saydam politika geliştirilmesine ve başarıyla uygulanmasına imkan vermektedir. Bilgi teknolojisinin işletmenin gereksinimlerini yerine getirmek konusunda başarılı olabilmesi için, yönetim iç kontrol modeli oluşturmaktadır. COBIT kontrol çerçevesi bu ihtiyaca cevap verir. İşletmenin gereksinimleri ile bağlantı kurar. Bilgi teknolojisi faaliyetlerini genel kabul görmüş bir süreç modeli şeklinde örgütler. Ana bilgi teknolojisi kaynaklarını tanımlar. İşletme kontrol hedeflerini açıklar.

İşletme yönelimli COBIT; işletmeninamaçlarının bilgi teknolojisi amaçlarına odaklanması, başarıyı değerlendirmek için vade modellerinin oluşturulması, işletme ve bilgi teknolojisi süreç sahiplerinin birleşik sorumluluklarının teşhis edilmesi faaliyetlerinden oluşur.

COBIT, iş süreç sahiplerinin bilgi sistem kontrol sorumluluklarını etkin ve verimli bir şekilde yerine getirmelerini sağlayan bir çerçevedir. SAC, iç denetçilere bilgi sistem ve teknolojisinin kontrol ve denetiminde yardım sağlar. SAS55 ve SAS78 dış denetçilere organizasyonun finansal tablolarının denetiminin planlanması ve gerçekleştirilmesi ile ilgili iç kontrol alanında rehberlik sağlar.

COBIT kaynak dokümanlarını COSO ve SAC ’dan sağlar. COBIT kontrolün tanımını COSO ’dan ve bilgi teknolojisi kontrol amaçlarının tanımını SAC ’dan alır. COBIT kontrol iş hedeflerinin gerçekleştirilmesi ve beklenmeyen olayların önlenmesi, düzeltilmesi için makul güvence sağlamak amacıyla tasarlanan kurallar, usuller, uygulamalar ve organizasyon yapıları olarak tanımlanmıştır.

İç kontrol, ulaşılmak istenen kontrol amaçları ve bu amaçlara ulaşmak için gerekli yollar tarafından tasarlanan kontrollerdir. COBIT anahtar iç kontrol gereksinimleri olan sistemleştirme, belgelendirme, standartlar ve tanımlanan beklentiler, değerlendirmeler, uygun risk değerlendirmeleri, tanımlanmış operasyonel hedefler ve kontrol hedefleri, uygun kontroller, yetkili ve güvenilir insanlar, kontrol etme ve değerlendirmeyi birleştirir.

COBİT ‘in misyonu; işletme yöneticileri ve denetçiler tarafından günlük kullanılan, yeterli, geçerli, modern, uluslararası genel kabul görmüş bilgi teknolojisi kontrol amaçlarını araştırmak, geliştirmek, tanıtmak ve ilerletmektir.

COBİT ‘in amacı, kar maksimizasyonu, fırsat optimizasyonu, rekabetçi avantaj sağlamak için iş riski, kontrol gerekleri ve teknik konular arasındaki boşluklar arasında köprü kurmak için bir çatı oluşturmaktır.

2.1.1.1. COBIT ‘in Unsurları

COBIT beş unsurdan oluşan bir modeldir. Bunlar; yönetici özeti, çerçeve, kontrol amaçları, denetim ilkeleri ve yönetim ilkeleridir.

Yönetici özeti, COBIT ’in amaçlarını ve süreçlerini özetler.

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

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

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

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

1)Fayda maliyetten fazla mı?

2)İyi bir performansın göstergeleri nelerdir?

3)Kritik başarı faktörleri nelerdir?

4) Amaçları gerçekleştirememenin riskleri nelerdir?

5) Diğerleri ne yapıyor?

6) Nasıl karşılaştırma ve değerlendirme yapabiliriz?

2.1.1.2. COBİT Çerçevesi

COBIT unsurlarından çerçeve, bir iş süreç akım şemasıdır. Organizasyonun elindeki kaynaklardan elde ettiği mevcut bilgilerden iş süreçleri sonucunda ihtiyaç duyulan bilgilerin elde edilmesini sağlayan bir yapıdır. COBIT çerçevesi; işletme odaklı, süreç yönelimli, kontrol esaslı ve ölçmeye dayalı olarak düzenlenmiştir. COBIT çerçevesi, işletmenin hedeflerini gerçekleştirmesi için gerekli bilgiyi sağlamak, kuruluşların gerekli bilgi hizmetlerini sunması için yapısal süreçlerde kullanılan bilgi

teknolojisi kaynaklarını yönetmek ve kontrol etmek esaslıdır.

COBIT çerçevesi üç unsurdan oluşur. Bunlar bilgi için işletme gereksinimleri, bilgi teknolojisi kaynakları ve bilgi teknolojisi süreçleridir.

İşletmenin hedeflerini gerçekleştirmesi için bilginin COBIT 'in kullandığı kontrol kriterlerine uyumlu olması gerekir. Bilgi kriterleri etkililik, verimlilik, gizlilik, bütünlük, kullanırlık, uyum ve güvenirliktir.

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

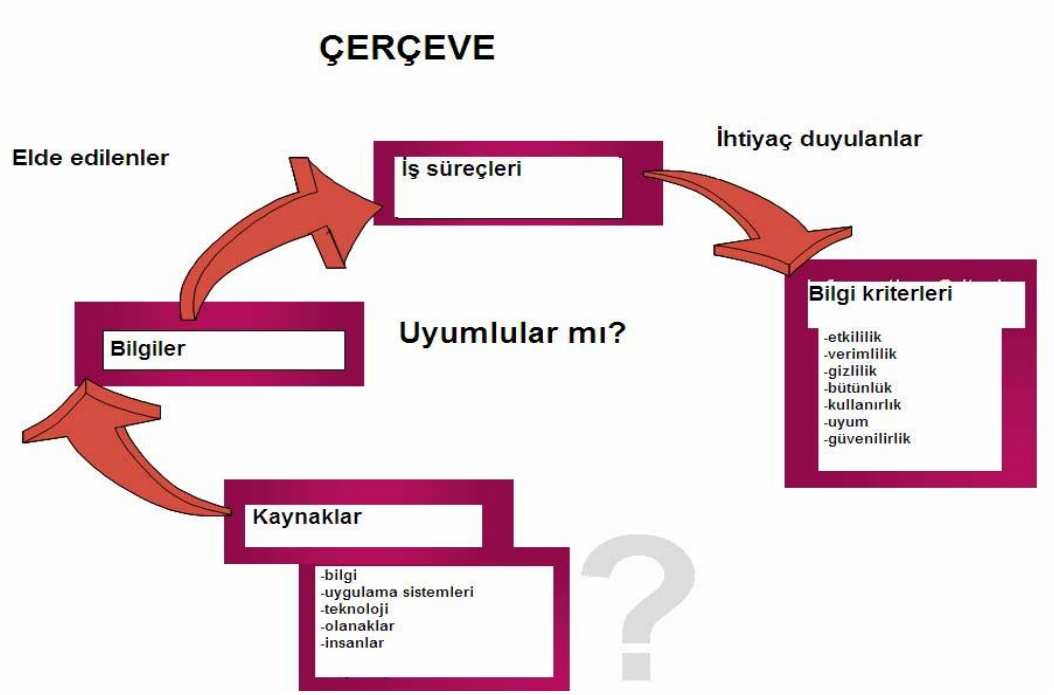
Planlama ve organizasyon süreci strateji ve taktikleri içerir, bilgi teknolojisinin iş hedeflerini gerçekleştirmesi adına en iyi katkıyı sağlamasının yollarını belirtir. Planlama ve organizasyon süreci; bilgi teknolojisi için stratejiler ve taktiksel planlar oluşturma, bilgi teknolojisinin iş hedeflerini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

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

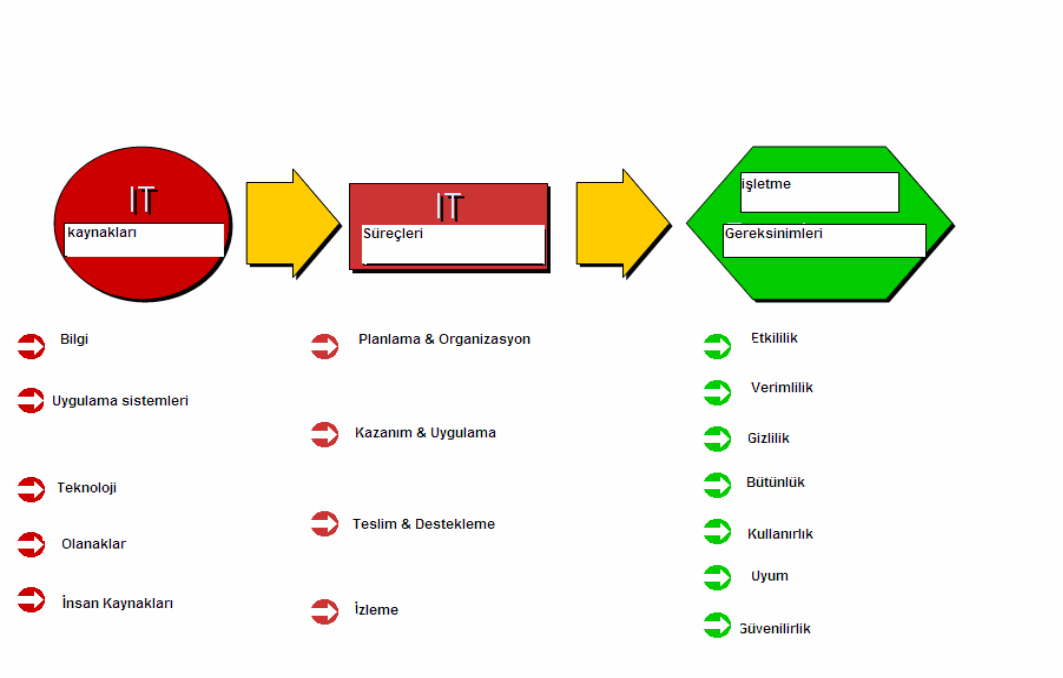
Teslim ve destekleme süreci; gerekli hizmetlerin yerine getirilmesi, hizmetlerin güvenliğinin ve devamlılığının sağlanması, eğitim ve stajı içeren destekleme sürecinin oluşturulması, uygulama kontrollerini içeren bilgi süreci faaliyetlerden oluşmaktadır.

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

COBIT çerçeve içerisinde 34 kontrol amacı ve 318 ayrıntılı kontrol amacı yer almaktadır.



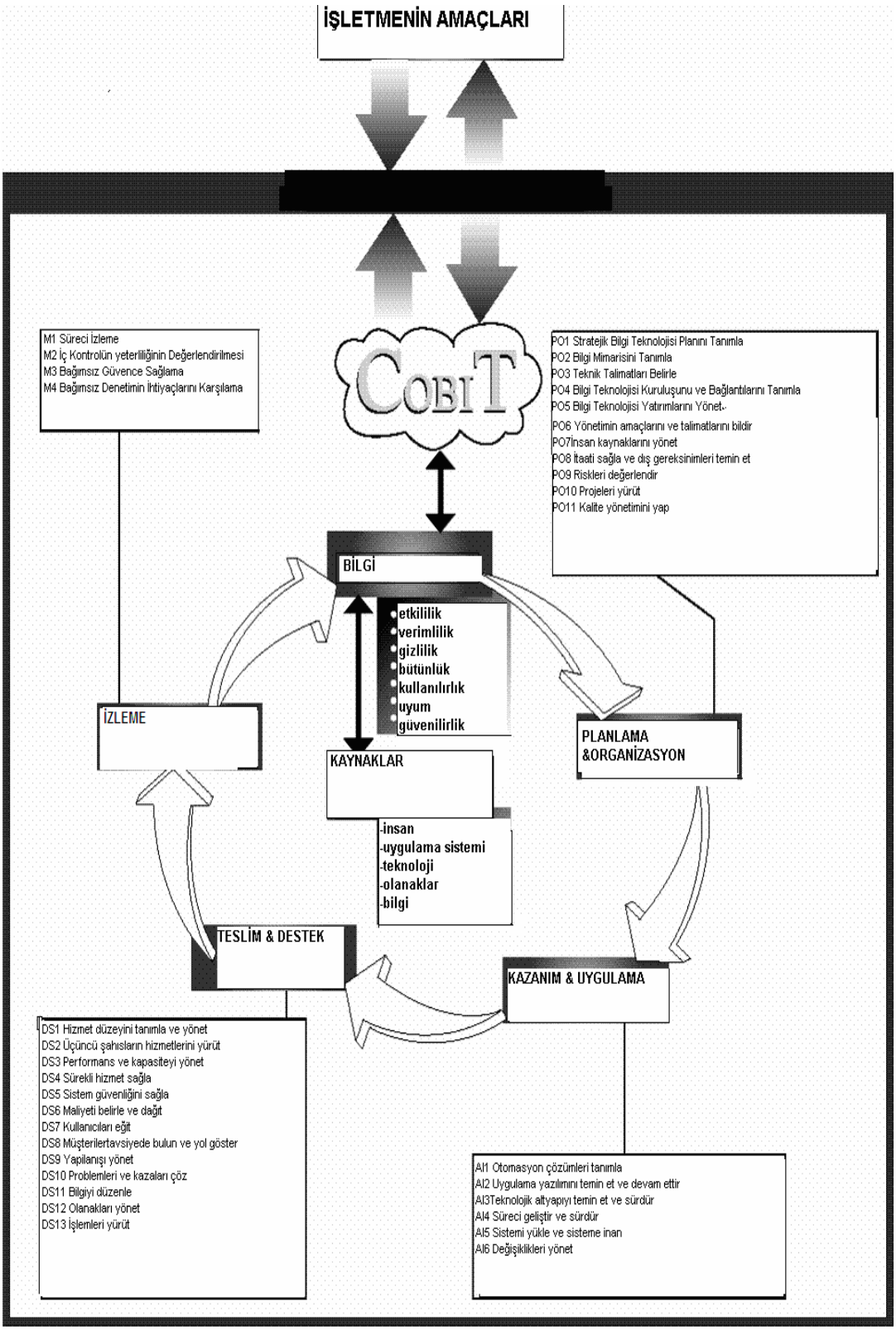
Şekil 6: Cobit Çerçevesi



Şekil 7: Bilgi teknolojisi süreçleri

2.1.1.3.COBIT Mimarisi

Bu süreçlerin altında, 318 adet kontrol hedefi veya alt aktivite tanımlanmıştır. Cobit, bilgi işlem güvenliği için kapsamlı ve en iyi uygulama niteliğinde bir yaklaşım ortaya koymaktadır. IT Governance Institute, CobiT'in oluşturulmasında tüm en iyi uygulamalar ve standartları (COSO, ISO 9000, Spice, CMM, ITIL, BSI7799 vb.) referans olarak ele almış, dünya çapında akademisyen, uzman, danışman ve analistler ile ortak bir çalışma yürütmüştür. 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 8: Cobit Mimarisi

Koyu renkli olan kontrol amaçları güvenlikle ilgili kontrol amaçlarıdır.

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.

2.1.1.4. COBIT Bilgi Güvenliği

Bilgi güvenliği, Bilgi teknolojisi yönetişiminin en önemli unsurudur ve bütün bilgi kullanıcıları için bunu anlamak ve uygulamak önemlidir. Bilgisayar sistemleri işten eve kadar hayatın her alanında yaygınlaştıkça, güvenlik riskleri de artmaktadır. İnternet, portatif bilgisayar gereçleri, mobil teknolojinin yaygın kullanımı artık tüm bilgilere daha çabuk ulaşmamızı sağlamaktadır. Ancak diğer taraftan bilgi teknolojisindeki bu gelişmeler, bilgi hırsızlığı, virüslerle kasıtlı saldırı, bilgisayar korsanlığı gibi bilgi teknolojisi ile ilgili problemlerin ortaya çıkmasına sebep olmaktadır. Bu riskler, dikkatsiz hatalar, ciddi finansal zararlara sebep olur. 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 Güvenlik Dayanağı, COBIT'e dayandırılmaktadır. COBIT, bilgi kuruluşlarının bilgi teknolojisi yönetişimine ve kontrol çerçevelerine uyum sağlamaları için gerekli olan kapsamlı kaynakları içeren bir modeldir. COBIT, bilgi teknolojisi kullanımından doğan riskleri tespit eder. Bu model, bilgi teknolojisi güvenliğindeki önemli risklere karşı ana kullanıcıların, küçük ve orta ölçekli işletmelerin, idarecilerin ve büyük kuruluşların yönetim kurulu üyelerinin kolaylıkla uygulayıp, takip edilebilecekleri işlemlerin üzerinde yoğunlaşır.

2.1.1.4.1. COBIT Bilgi Güvenliği Unsurları

COBIT Bilgi Güvenliği; arka planın başarıyla okunması, COBIT esaslı güvenlik dayanağı, teknolojik güvenlik risklerinin özetini içeren ek olmak üzere üç unsurdan oluşmaktadır.

Yüzde yüz güvenlik diye bir şey yoktur ama modeldeki tavsiyeleri takip ederek, güvenlikle ilgili riskler hakkında bilinci arttırarak çok etkili seviyede güvenlik sağlanabilir.

Bilgi teknolojisi ortamı değişmeye devam etmektedir ve dolayısıyla yeni güvenlik riskleri ortaya çıkmaktadır. İyi bir güvenlik sağlamak büyük miktarlarda zaman ve para harcamakla gerçekleştirilmez. 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 etkinliği arttırır.

2.1.1.4.2 Bilgi Güvenliğinin Tanımı

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.

İnternetin etkisi, internet üzerinden ekonominin büyümesi elektronik işlemlere güvenme ihtiyacını doğurmuştur.

2.1.1.4.3 Bilgi Güvenliği Neden Önemlidir

Bilgi teknolojisi günlük yaşamın ve iş hayatının ayrılmaz bir parçasıdır ve bilgi teknolojisine bağımlılık giderek artmaktadır. Yeni teknolojiler işlevselliği arttırırken, yeni riskler kontrol edilmesi güç sonuçlar doğurur. İnternet ağının yaygın kullanılması, bireylerin kişisel bilgileri ve şirketlerin gizli bilgilerinin güvenliği hakkında daha fazla endişelenmelerine neden olmaktadır.

2.1.1.5. COBIT Güvenlik Dayanağı: Güvenlik İçin 39 Adım

Bilgi güvenliği teknik önlemlerden ziyade davranışlarla ilgilidir. Kurumların güvenlik alanında gerekli adımları atmasına yardımcı olmak için COBIT bir güvenlik dayanağı tasarlanmıştır. Bu dayanak, güvenlikle ilgili en önemli hedefleri COBIT ’den almaktadır. Dayanak, 34 kontrol sürecinin planlama-organizasyon, kazanım-

uygulama, teslim-destek, izleme olmak üzere dört gruba ayrıldığı COBIT çerçeve kontrol modelini kullanılır. Kilit kontrol amaçlarını, gerekli minimum kontrol adımlarını, COBIT sürecini ve detaylı COBIT kontrol amaçlarını içerir. Daha güvenli kontrol için 39 adım içerir. Dayanakta, ISO17799'daki kontrol amaçları da kullanılır. COBIT, ISO 17799'dan daha üst düzeydedir.

Bu model, COBIT 'in güvenlikle ilgili kontrol amaçlarının her biri için oluşabilecek riskleri ve güvenliği sağlamak için gerekli önlemleri belirtilir. Model, kontrol amaçlarının her biriyle ilgili güvenliğin sağlanması amacıyla 39 adımdan oluşur:

1) Bilgi, hizmet ve işlemlerin doğruluğunun ve uygunluğunun tespiti, güvenlik gereksinimlerinin göz önünde bulundurulması,
2) Güvenlik yönetimi için spesifik sorumlulukların tanımlanması,
3) Sürekli iletişim halinde bulunulması, güvenlik gereksinimlerinin yerine getirilmesi için gerekli kuralların düzenli olarak görüşülmesi,
4) Personeli işe alırken referans bilgilerin doğruluğunun kontrol edilmesi,
5) Kuruluşların güvenlik gereksinimlerini yerine getirmek için gerekli kalifiye elemanların işe alınması ve yetiştirilmesi,
6) Ana güvenlik hizmetlerinin tek bir kaynağa bağlı olmamasının garanti edilmesi,
7) Gizliliğe, fikir haklarına, diğer yasal, düzenleyici sözleşmeye dayalı ve sigorta gereksinimlerine uyulması için gerekli güvenlik yükümlülüklerine ilişkin yapılmasına ihtiyaç duyulan şeylerin belirlenmesi,
8) İşletmenin başarısı için gerekli bilgi, hizmet ve işlemlerin güvenliğinin sağlanması, en önemli riskleri belirten risk yönetimi faaliyet planının hazırlanması,
9) Tanımlanmış güvenlik risklerinin yönetimi için gerekli maliyet-etkin araçlara olan ihtiyacın, tüm personel tarafından anlaşılmasının sağlanması,
10) Otomasyon çözümlerin etkinliğinin, fonksiyonelliğinin değerlendirilmesi,
11) Teknolojik altyapının otomasyon güvenlik uygulamalarını desteklemesinin sağlaması,
12) Teknolojik altyapıyı korumak için gerekli ilave güvenlik gereksinimlerinin göz önünde bulundurulması,
13) Kaynakların güncelliğinin korunması için tanımlanması ve kontrol edilmesi,
14) Güvenliği bütünleştirmek için uygulanması gereken günlük prosedürün tüm

çalışanlar tarafından bilinmesinin sağlanması,

15) Fonksiyonel ve operasyonel güvenlik gereksinimlerine karşı sistemin test edilmesi,

16) İşletmenin amaçları ve güvenlik gereksinimlerine karşı test sonuçlarının değerlendirilmesi ve güvenlik onayının verilmesi,

17) Tüm değişikliklerin değerlendirilmesi,

18) Tüm değişikliklerin kaydedilmesi,

19) İşletmenin güvenlik gereksinimlerini yerine getirmesinin sağlanması,

20) Üçüncü kişilerin profesyonel kapasitelerinin değerlendirilmesi ve işletmenin güvenlik gereksinimleri için gerekli temasın sağlanması,

21) Güvenlik gereksinimleri için işletme dışı tedarikçilere olan bağımlılığın dikkate alınması,

22) Kritik işletme fonksiyonlarının, bilgilerin ve kaynakların tanımlanması, hizmetlerin sürekliliğinin sağlanması için kaynakların kullanılırlığının arttırılması,

23) Bilgi teknolojisi hizmetlerinin korunması ve yeniden yapılandırılması için gerekli temel ilkelerin belirlenmesi,

24) İşletmenin gelişimini desteklemek için yedek kaynakların ayrılması, düzenli aralıklarla kontrol edilmesi, tamamlanması,

25) Müşterilerin, hizmet sunanların, tedarikçilerin bilgilere erişiminin gerçekleştirilmesi,

26) Bütün kullanıcı hesaplarının ve güvenlik işaretlerinin yönetimi için sorumlulukların dağıtılması,

27) Önemli güvenlik ihlallerinin günlük izlenmesi ve ortaya çıkarılması,

28) Karşı tarafın güvenilir olduğunun ve elektronik ortamda yapılan işlemlerin güvenilir olduğunun temin edilmesi,

29) İşletmenin altyapısında virüs koruma yazılımlarının kullanılmasının sağlanması,

30) Kuruluşa hangi bilgilerin gelebileceği ve kuruluştan hangi bilgilerin çıkabileceği hakkında politikaların tanımlanması, ağ güvenlik sistemlerinin yapılandırılması,

31) Bilgi teknolojisi donanım ve yazılım yapılanışında düzenli olarak güncellenmiş, eksiksiz envanter sağlanması,

32) Tesis edilmiş yazılımın ruhsatlı ve yetkili olup olmadığının düzenli olarak gözden geçirilmesi,

33) Bilginin doğruluğunun, eksiksizliğinin, geçerliliğinin, bütünlüğünün çeşitli kontrollere tabi tutulması,

34) Önemli bilgilerin sadece yetkili kişilere dağıtılması,

35) Girdi ve çıktı dokümanları, bilgi, yazılım için saklama süresinin, belgelere dayalı gereksinimlerin, depolama dönemlerinin tanımlanması,

36) Bilgi teknolojisi olanaklarının, varlıkların özellikle güvenlik tehdidi riskine karşı korunması,

37) Bilgisayar ağ sistemlerinin ve depolama teçhizatlarının çalınmaya, hasara, kaybolmaya karşı korunması,

38) Çalışanların düzenli aralıklarla güvenlik kontrollerinin yeterliliğini değerlendirmesi, güvenlik istisnalarını gözlemlemesi, güvenlik mekanizmalarının işlerliğini değerlendirmesi, önemli kontrollere uyumu sağlaması,

39) Bilgi güvenliği kontrol mekanizmalarının gözden geçirilmesi; bilgi güvenliği ile ilgili yasalara, düzenlemelere, sözleşme yükümlülüklerine uyumunun sağlanması için yetkili dış kaynakların sağlanması.

Bu 39 adımda bilgi teknolojisi güvenliğinin sağlanması amaçlanmaktadır.[30]

Çerçeve doküman, ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği - Information Systems Audit and Control Association) tarafından 1996 yılında yayınlanmıştır. Çıkış noktası bilişim teknolojileri denetimidir. Bugün gelinen noktada denetim, kontrol, yönetim ve nihayetinde yönetişim kavramlarını kapsamaktadır (Tablo – 1) :

Yıl	**İşlev**
1996	Denetim
1998	Denetim ve Kontrol
2000	Denetim, Kontrol ve Yönetim
2005-…	Denetim, Kontrol, Yönetim ve Yönetişim

Tablo 1: COBIT'in Tarihsel gelişimi, ITGI,

[30] COBİT, Vildan UZUNAY İç Kontrol Merkezi Uyumlaştırma Dairesi, 2007

COBIT denetim çerçevesinin hedef kitlesi üst yöneticiler olup, muhtemel bilişim teknolojileri risklerini,

Örneğin,

- *başarısızlıkla sonuçlanabilecek projeleri,*
- *yatırım yanlışlarını,*
- *güvenlik zafiyetlerini,*
- *kullanıcı ihtiyaçlarıyla uyumlu olmayan çözümleri,*
- *muhtemel sistem kayıplarını*

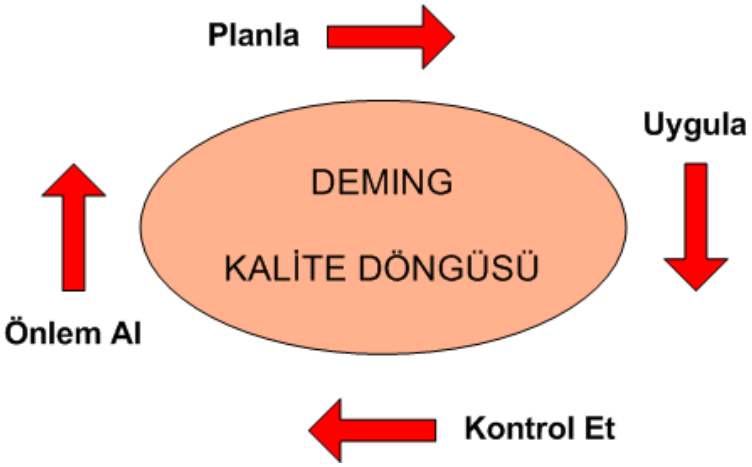
Üst yönetime görünür kılmayı amaçlamakta ve aşağıdaki sorulara cevap vermektedir:

- *Ne kadar daha ileri gidebiliriz?*
- *Harcanacak çaba ile elde edilecek fayda örtüşüyor mu?*
- *İyi bir performansın göstergeleri nelerdir?*
- *Kritik başarı faktörleri nelerdir?*
- *Kontrol hedeflerini yerine getirmemenin riskleri nelerdir?*
- *Başkaları ne yapıyor?*
- *Kendimizi nasıl ölçeriz ve başkalarıyla mukayese ederiz?*

COBIT bu yönleriyle organizasyonlarda bilişim teknolojileri yönetişim (IT Governance) modelinin oluşturulmasına yardımcı olmakta ve risk odaklı bir denetim çerçevesi sunmaktadır.

COBIT çerçevesinde bulunan süreç alanları, bilişim teknolojileri süreçlerinde uygulanması gereken kontrolleri içermektedir.

Kontroller, “Deming Kalite yaşam Döngüsü” olarak bilinen ve ISO 9001 Kalite Yönetim Sistemi temelinde de uygulanan : “Plan - Do – Check - Act / Planla – Uygula – Kontrol Et – Önlem Al” yaşam döngüsünü kullanmaktadır.



Şekil 9: Deming Kalite Döngüsü

COBIT bu çerçevede olmak üzere, organizasyonlarda bilişim Teknolojilerine yönelik bir kalite yönetim sürecinin tanımlanmasında da yönlendirici rol oynamaktadır.[31]

COBIT'deki temel **süreç alanları** aşağıdaki gibidir:

1. PO: Planla ve Organize Et (Plan & Organize)

PO : Planla ve Organize Et

PO1: Stratejik BT Planının Tanımlanması

PO2: Bilgi Mimarisinin Tanımlanması

PO3: Teknolojik Yönün Belirlenmesi

PO4: BT Organizasyon ve ilişkilerinin Tanımlanması

PO5: BT Yatırımlarının Yönetimi

PO6: Yönetimin Amaçlarının ve Talimatlarının İletilmesi

PO7: İnsan Kaynakları Yönetimi

PO8: Kalite Yönetimi

PO9: Risk Değerlendirme

PO10: Proje Yönetimi

[31] Bilişim Teknolojilerinde Kalite Yönetimi, Ahmet Pekel, Türkiye Cumhuriyet Merkez Bankası Lira Dergisi, Ocak 2007 tarihli, 41. sayı.

2. AI: Tedarik ve Uygulama (Acquire & Implement)

AI1: Otomasyon Çözümlerinin Belirlenmesi

AI2: Uygulama Yazılımı Tedarik Edilmesi ve Bakımı

AI3: Teknoloji Altyapısının Tedarik Edilmesi ve Bakımı

AI4: İŞ ve Kullanımın Etkin Kılınması

AI5. BT Kaynaklarının Sağlanması

AI6: değişiklik Yönetimi

AI7: Çözüm ve değişikliklerin Kurulması ve Kabul Edilmesi

3. DS: Teslimat ve Destek (Deliver & Support)

DS1: Hizmet Düzeyi Belirleme ve Yönetimi

DS2: Üçüncü Parti Hizmet Yönetimi

DS3: Performans ve Kapasite Yönetimi

DS4: Sürekli Hizmetin Sağlanması

DS5: Sistem Güvenliğinin Sağlanması

DS6: Harcamaların Belirlenmesi ve Bütçelenmesi

DS7: Kullanıcı Eğitimi

DS8: Kullanıcılara Yardım ve danışmanlık

DS9: Konfigürasyon Yönetimi

DS10: Problem ve Olay Yönetimi

DS11: Veri Yönetimi

DS12: Fiziksel Çevre Yönetimi

DS13: Operasyon Yönetimi

4. ME: İzle ve Değerlendir (Monitor & Evaluate)

ME1: Süreç İzleme

ME2: İç Kontrol Değerlendirme Yeterliliği

ME3: Bağımsız Güvence Elde Edilmesi

ME4: Bağımsız Denetimin Sağlanması

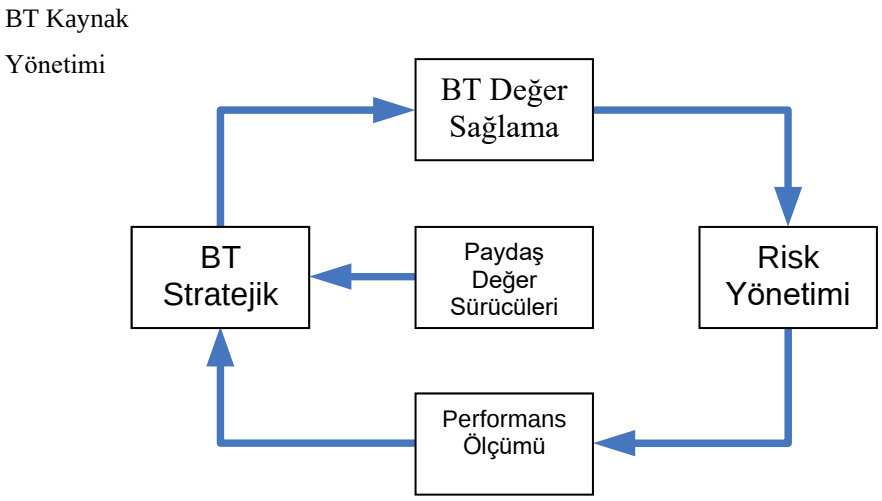
COBIT'de, İş Süreçleri ile BT Kaynakları (Veriler, Uygulamalar, Teknoloji, Hizmetler, İnsanlar) arasındaki iletişimde aranan bilgi kriterleri şunlardır :

- **Etkililik,**
- **Gizlilik,**
- **Bütünlük,**

- **Erişebilirlik,**
- **Uyumluluk,**
- **Güvenilirlik.**

BT yönetişim Enstitüsü (ITGI), yakın zamanda COBIT'i tamamlayan ve genişleten kurumsal değer çerçevesi'ni (Val IT – Value IT) yayınlamıştır. Anılan çerçeveden, genel hatlarıyla aşağıda bahsedilmektedir:

1. ***Stratejik Uyum*** - Strategic Alignment (kurumun stratejik hedefleriyle bilişim teknolojileri hedeflerinin uyumlandırılması üzerine odaklanma)
2. ***Değer Sağlama*** - Value Delivery (harcamaların optimize edilmesi ve bilişim teknolojileri değerinin kanıtlanması üzerine yoğunlaşma)
3. ***Performans Ölçümü*** - Performance Measurement (proje başarısının izlenmesi ve bilişim teknolojileri hizmetlerinin izlenmesi)
4. ***Kaynak yönetimi*** - Resource Management (bilgi ve altyapının optimize edilmesi)
5. ***Risk Yönetimi*** -Risk Management (bilişim teknolojileri varlıklarının korunması ve felaketten kurtarmanın adreslenmesi)



Şekil 10: Bilişim Teknolojileri Yönetişimi Odak Alanları

COBIT yürütme konusuna odaklanırken (Yapılanlar doğru bir yol izlenerek mi yapılıyor? İyi mi yapılıyor?), Val IT, Bilişim Teknolojileri Yatırımlarının yönetişimi üzerine kurgulanmıştır (Doğru mu yapıyoruz? Fayda sağlıyor muyuz?). Val IT yaşam döngüsü üç ana başlık altında açıklanmaktadır:

1. ***Değer Yönetişimi*** - **Value Governance** (VG, organizasyonun bilişim teknolojileri odaklı yatırımlarının değerini optimize etmek)

2. ***Portföy Yönetimi*** - **Portfolio Management** (PM, organizasyonun bilişim teknolojileri odaklı yatırımlarının tamamının organizasyonun stratejik amaçlarına optimal değer katmayla uyumlu olmasını sağlamak)

3. ***Yatırım Yönetimi*** - **Investment Management** (IM, organizasyonun tek tek Bilişim teknolojileri odaklı yatırım programlarının makul maliyetlerde bilinen ve kabul edilebilir risk seviyesinde optimal değer sağlamasını temin etmek)

Val IT'deki temel **Değer Alanları** ise aşağıdaki gibidir :

1. VG: Değer yönetişimi (Value Governance)

VG1: bilgilendirilmiş ve onaylanmış Liderliği Sağla

VG2: Süreçleri Tanımla ve geliştir

VG3: Rol ve Sorumlulukları Tanımla

VG4: Uygun ve Kabul Edilebilir Mali Sorumluluğu Sağla

VG5: Bilişim Gereksinimlerini Tanımla

VG6:Raporlama Gereksinimlerini Sapta VG7: Örgütsel Yapıları Sapta

VG8: Stratejik Yönü Belirle

VG9: Yatırım Kategorilerini Tanımla

VG10: Hedef Portföy karışımını Sapta

VG11: Kategori Bazında Değerlendirme Kriterini Tanımla

2. PM : Portföy Yönetimi (Portfolio Management)

PM1: İnsan Kaynağı Envanterinin Bakımını Yap

PM2: Kaynak Gereksinimlerini Belirle

PM3: Gap (boşluk/Aralık) Analizi Yap

PM4: Kaynak Sağlama Planını geliştir

PM5: Kaynak Gereksinimlerini ve Kullanımını İzle

PM6: Bir Yatırım eşiği Sapta

PM7: Başlangıç Programını Değerle

PM8: Program İŞ Durumunu Değerle ve Göreli Skor Ata

PM9: Tam Bir Portföy Görünümü oluştur

PM10: Yatırım Kararı Al ve iletişimi Sağla

PM11: Seçilmiş Programları Yürüt ve Fonu Yönet

PM12: Portföy Performansını Optimize Et

PM13: Portföyü Tekrar Önceliklendir

PM14: Portföy Performansını İzle ve Raporla

3. IM: Yatırım Yönetimi (Investment Management)

IM1: Yatırım Fırsatlarının Üst Düzey Tanımını geliştir

IM2: İş Durumu İçin başlangıç Programını geliştir

IM3: Aday Programların anlaşılır Halini geliştir

IM4: Alternatif Analizleri Hazırla

IM5: Program Planı geliştir

IM6: Fayda gerçekleştirim Planı geliştir

IM7: Tam Bir yaşam Döngüsü Maliyet Fayda Tanımı Yap

IM8: Ayrıntılı Program İŞ Durumu geliştir

IM9: Net Mali Sorumluluk ve Sahiplikleri Ata

IM10: Program Planla ve başlat

IM11: Program Yürüt

IM12: Yararları Yönet/İzle

IM13: İş Durumunu Güncelle

IM14: Program Performansını Monitör Et ve Raporla

IM15: Program Uygulamadan Kaldırma

Val IT'de, yöntemin gücü, bilişim teknolojileri projelerinde, bilişim teknolojileri yatırımları yapmada kullanılan bütünleşik yaklaşımda yatmaktadır. Bunun yanı sıra kapsam, projelerle sınırlıdır. Bu başlangıç sürümünde, uygulama bakım maliyetleri ve altyapı gibi yinelenen maliyetler için deneyimler ("*practice"*) eksiktir[32].

2.1.2. ITIL ve ISO 20000

1980'lerin sonunda, İngiliz Hükümeti'nin Merkezi Bilgisayar ve Telekomünikasyon Dairesi'nce, bilişim teknolojileri çalışanlarının üretkenliğinin artırılması, insandan kaynaklanabilecek hataların azaltılması ve bilişim teknolojileri

[32] Enterprise Value: Governance of IT Investments, The Val IT Framework, http://itgovernance.pbwiki.com/ValIT, 23.12.2007.

hizmetlerinden yararlanan kullanıcıların memnuniyetinin artırılması için ITIL (Bilgi Teknolojisi Altyapı Kütüphanesi - Information Technology Infrastructure Library) adı verilen ve en iyi uygulamaları içeren bir doküman kütüphanesi oluşturulmuştur. ITIL, yüksek düzeyde bilişim teknolojileri hizmeti verilmesinde yararlanılabilecek kaynak dokümanlardan oluşmaktadır. Bunlar iki ana başlıkta ele alınmaktadır:
Birinci kısımda yer alan **Hizmet Desteği** (Service Support) başlığı altında,

- *Değişiklik Yönetimi (Change Management),*
- *Sürüm Yönetimi (Release Management),*
- *Problem Yönetimi (Problem Management),*
- *Olay Yönetimi (Incident Management),*
- *Konfigürasyon Yönetimi (Configuration Management) ve*
- *Yardım Masası (Service Desk)*

süreçleri yer almaktadır.

İkinci kısımda yer alan **Hizmet Sunumu** (Service Delivery) başlığı altında ise,

- *Finans Yönetimi (Financial Management),*
- *Bilişim Teknolojileri Hizmet Sürekliliği Yönetimi(IT Service Continuity Management)*
- *Kapasite Yönetimi (Capacity Management)*
- *Kesintisiz Çalışma Yönetimi (Availability Management)*
- *Hizmet Düzeyi Yönetimi (Service Level Management)*

süreçleri yer almaktadır.

ITIL, bilişim teknolojileri hizmetlerinin planlanmasının ve uygulanmasının nasıl yapılacağını kapsamaktadır. ITIL baz alınarak 2002'de yayınlanan eski adıyla BS 15000 ve 2005'de yayınlanan yeni adıyla ISO 20000 standardı kapsamında hizmet yönetim sertifikası alınabilmektedir[33]**.**

ITIL uygulanarak,

- *işletim maliyetleri düşürülebilmekte,*
- *kaynak kullanımı iyileştirilebilmekte,*

[33] Bilişim Teknolojilerinde Kalite Yönetimi, Ahmet Pekel, Türkiye Cumhuriyet Merkez Bankası Lira Dergisi, Ocak 2007 tarihli, 41. sayı.

- bilişim teknolojileri hizmetlerinin erişilebilirliği ve bilişim teknolojileri ekiplerinin memnuniyeti artırılmakta,

- bilişim teknolojileri, önceki deneyimlerinden ders çıkarabilmekte,

- son kullanıcılara hizmet garantisi verilebilmekte,

- bilişim teknolojileri ile son kullanıcı iletişiminde iyileşme sağlanmakta,

Beklentiler yönetilebilmektedir.

1999 yılında ITIL'i uygulamaya başlayan Procter & Gamble, bilişim teknolojileri işletim maliyetlerinde %6-8, insan gücünde %15-20 oranında tasarruf sağlamıştır. Aynı kapsamda, çağrı merkezlerinin aranma oranında ise %10 azalma olmuştur[34].

Uygulanması halinde COBIT çerçevesindeki aşağıda verilen alanlara karşılık gelen hedeflere ulaşılabileceği değerlendirilmektedir (Tablo – 2,3).

IT IL(Hiz met Dest eği: Serv i ce Su p p o rt	**COBIT**
Değişiklik Yönetimi	Değişiklikleri Yönet (AI6)
Konfigürasyon + Sürüm Yönetimi	Konfigürasyonu Yönet (DS9)
Problem + Olay Yönetimi	Problemleri Yönet (DS10)
Yardım Masası	Operasyonları Yönet (DS13)

Tablo 2: ITIL Hizmet Desteği ve COBIT

ITIL (Hizmet Sunumu:Service Delivery)	**COBIT**
Finans Yönetimi	BT Yatırımlarını Yönet (PO5)
Süreklilik Yön.+ Kesintisiz çalışma	Hizmette Sürekliliği Sağla (DS4)
Kapasite Yönetimi	Performans ve Kap. Yönet (DS3)
Hizmet Düzey Yönetimi	Hizmet Düzeyi Belirleme ve Yönetimi (DS1)

Tablo 3: ITIL Hizmet Sunumu ve COBIT

2.1.3. CMMI

Bilgisayar yazılımlarında, geliştirme, test ve uygulamaya alma aşamaları önemli zaman ve maliyet gerektiren süreçlerdir. Zamanında bitirilemeyen, çok hata içeren,

[34] Gülten KIYICI, Bilişim Teknolojileri, 2006

yüksek maliyetli yazılım geliştirme projeleri, 1980'lerde ABD Savunma Bakanlığı'nın yeni bir çalışmayı başlatmasına neden olmuştur. Söz konusu proje, bakanlığın talebiyle, Carnegie Mellon Üniversitesi'nde, SEI - Software Engineering Institute (Yazılım Mühendisliği Enstitüsü) tarafından gerçekleştirilmiştir.

Yazılım geliştirme süreçlerinin iyileştirme çalışmalarında kullanılmak üzere geliştirilen CMM (Capability Maturity Model), yazılım ve sistem mühendisliği konularının bütünleştirilmesiyle 2001'de güncellenmiş ve CMMI (Capability Maturity Model Integration – bütünleşik Yetenek Olgunluk Modeli) adını almıştır. CMMI genel bir ifadeyle, süreç iyileştirme için kullanılan modellerin, değerlendirme yöntemlerinin ve eğitimlerin bütünü olarak tanımlanabilir. Başlangıçta yazılım geliştirme sahası için düşünülen CMMI'nın, süreç odaklı yaklaşıma dayalı bir model olması nedeniyle farklı alanlara da uyarlanması söz konusu olmuş ve çalışanların üretkenliğinin artırılmasını amaçlayan insan kaynakları yönetimine yönelik bir modeli de "People CMMI" ismiyle yayınlanmıştır. Diğer taraftan, SEI bünyesinde, hizmet süreçlerinin iyileştirilmesine yönelik olarak da "CMMI for Services" 2007 yılında yayınlanmıştır.

Model aşağıdaki süreç alanlarını içermektedir. Bunlar :

- Sebep Analizi ve Çözümlemesi
- Konfigürasyon Yönetimi
- Karar Analizi ve Çözümlemesi
- Bütünleşik Proje Yönetimi
- Ölçme ve Çözümleme
- Kurumsal Yaratıcılık ve yaygınlaştırma
- Kurumsal Süreç Tanımı
- Kurumsal Süreç Odaklanması
- Kurumsal Süreç başarımı
- Kurumsal Eğitim
- Proje İzleme ve Takip
- Proje Planlama
- Süreç ve Ürün Kalite Güvence
- Sayısal Proje Yönetimi

- Gereksinim Yönetimi
- Risk Yönetimi
- Teknik Çözüm
- Ürün bütünleştirme
- Doğrulama
- Geçerleme
- Gereksinim geliştirme
- Tedarikçi Yönetimi

CMMI kullanımında amaç,

- zamanında,

- bütçeye uygun,

- arzu edilen işlevsellikte ve

- kabul edilebilir kalite seviyesinde

ürünler geliştirerek kullanıcı beklentilerini karşılamaktır.

CMMI, mevcut süreçlerin yetenek seviyelerine göre iyileştirilmesi için gerekli model ve metotları sunmaktadır. Süreç yetenek seviyelerinin belirlenmesinde (derecelendirmesinde) ise SCAMPI (Süreç iyileştirme için Standart CMMI Değerlendirme Metodu - Standard CMMI Appraisal Method for Process Improvement) adı verilen değerlendirme yöntemi kullanılmaktadır.

CMMI'da kurumsal düzeyde yapılacak değerlendirmeler kapsamında,

1: başlangıç,
2: yönetilen,
3: tanımlı,
4: nicel yönetilen,
5: iyileşen
Olarak ifade edilen olgunluk düzeyleri kullanılmaktadır.

Seviye 1, başlangıç düzeyidir. Bu seviyede :

- Risk yönetimi yapılmamaktadır.
- Dış kaynak kontrolü yoktur.
- Değişiklikler yönetilmez.
- Gereksinimler kontrol edilemez.
- Zayıf proje yönetimi vardır.
- Projeler izlenmez.
- Kalite güvence yoktur.

- Çıkan ürün kontrolsüzdür.
- Başarı tesadüflere bağlıdır.
- Kahramanlara ihtiyaç vardır.

Seviye 2'nin Seviye 1'den farkı, yönetiliyor olmasıdır. Bu seviyede:

- Dış kaynak kontrolü vardır.
- Değişiklikler yönetilmektedir.
- Gereksinimler kontrol edilmektedir.
- Proje yönetimi uygulanmaktadır.
- Çıktılar tekrarlanabilmektedir.

Seviye 3'ün Seviye 2'den farkı, süreç standardizasyonunun olmasıdır:

- Risk yönetimi vardır.
- Süreçler tanımlıdır.
- Süreçler yönetilmektedir.

Seviye 4'ün Seviye 3'den farkı nicel yönetilebilir olmasıdır:

- İstatistiksel ve sayısal teknikler kullanılmakta; süreçler, verilere dayalı olarak yönetilmektedir.

Seviye 5'de, süreçlerin sürekli iyileştirilmesi söz konusudur.

- Toplam kalite hedeflenmektedir.
- Problemler ortaya çıkmadan önlenmektedir[35]**.**

Boeing Firması'nda Şef Mühendis olarak çalışan John D.Vu'nun değerlendirmelerine göre; Bilgi Servisleri Bölümü'nde, uçuş yazılımı geliştirmede CMMI Seviye 1'den Seviye 2'ye 34 ayda geçen Firma;

- hataları %12,
- zamanı %10,
- maliyeti %8

Oranında azaltmıştır.

Seviye 2'den Seviye 3'e 25 ayda geçen Firma,

- hataları %40,
- zamanı %38,
- maliyeti %35

Oranında azaltmayı başarabilmiştir.

Firma, Seviye 3'den Seviye 4'e 30 ayda geçerek,

[35] Bilgi Grubu, E.Demirörs, CMMI : Temel Kavramlar Kurs Notları, www.bg.com.tr, 2/5/2006

- hataları %85,
- zamanı %63,
- maliyeti ise %75

Oranında azaltmıştır.

Bu modelde, süreçlerin olması gerektiği gibi, diğer bir deyişle önceden tanımlanmış Şekliyle işliyor olması hedeflenmektedir. Ürünün (yazılımın) nihai kalitesinin garanti edilmesi söz konusu değildir.

Çünkü CMMI nihai yazılım kodunun değil, yazılım geliştirme süreçlerinin değerlendirilmesini sağlamaktadır.

CMMI, sürece uygun hareket edildiğinde kaliteli yazılım geliştirilebileceği anlayışına dayalıdır[36].

Uygulanması halinde COBIT çerçevesindeki belli alanlara karşılık gelen hedeflere de ulaşılabildiği değerlendirilmektedir (Tablo – 4).

CMMI	**COBIT**
Gereksinim Yönetimi	Uygulama Yazılımı Tedarik ve Bakım (AI2)
Proje Yönetimi	Projeleri Yönet (PO10)
Tedarikçi Yönetimi	Üçüncü Parti Hizmetleri Yönet(DS2)
Konfigürasyon Yönetimi	Konfigürasyonu Yönet (DS9)
Kalite Yönetimi	Kalite Yönetimi (PO8)
Risk Yönetimi	BT Risklerini Değerlendir ve Yönet (PO9)
İnsan Kaynakları Yön.	İnsan Kaynaklarını Yönet (PO7)

Tablo 4: CMMI ve COBIT

Aşağıda, konuyla ilgili iki standartlaşma çalışmasından daha bahsedilecektir. Bunlardan biri, yazılım süreçlerinin değerlendirilmesine yönelik bir diğer model olan SPICE'dir. Anılan model, uluslararası bir çalışma grubu tarafından geliştirilmiştir. Son hali ISO 15504 standardı olarak yayınlanmıştır. ISO 15504, temel olarak bir Yazılım geliştirme ve Yetenek Belirleme Standardı'dır ve CMMI'nın her süreç alanı için bir yetenek seviyesi belirlemeyi sağlayan modeli ile uyumludur.

[36] Bilişim Teknolojilerinde Kalite Yönetimi, Ahmet Pekel, Türkiye Cumhuriyet Merkez Bankası Lira Dergisi, Ocak 2007 tarihli, 41. sayı.

Yazılım mühendisliğinde doğrudan yazılım kalitesine yönelik olarak bilinen bir başka Standart ise ISO 9126'dır.

ISO 9126, yazılım kalitesinin değerlendirilmesi için geliştirilmiş uluslararası bir standarttır. Square, ISO 25000:2005 projesi tarafından, benzer genel görüşlerin yerine geçirilmiştir[37].

Standart;

- Kalite modeli,
- Dış metrikler,
- İç metrikler,
- Kullanılmakta olan kalite metrikleri

olarak dört temel bölüme ayrılmıştır.

Standardın ilk bölümünde yer alan ISO-9126-1 kalite modeli, yazılım kalitesini aşağıda listelenen özellik ve alt özellikler kümesi olarak listelemektedir :

İşlevsellik – Fonksiyonlar kümesinin ve onların belirli özelliklerinin varlığına dayalı özellikler kümesidir.

- Uygunluk,
- Birlikte çalışabilirlik,
- İtaat,
- Güvenlik.

Güvenilirlik – Belli bir zaman periyodu ve belli durumlar altında, yazılımın performans seviyesini sürdürme yeteneğine dayalı özellikler kümesidir.

- Olgunluk,
- Kurtarılabilirlik,
- Aksaklığa dayanıklılık.

Kullanılırlık – Belli durum ve kullanıcı kümesi altında kullanım için gerekli olan çaba üzerine dayalı özellikler kümesidir.

- Öğrenilebilirlik,
- Anlaşılabilirlik,
- İş görürlük.

Etkinlik – Belli durumlar altında yazılımın performans seviyesi ile ihtiyaç duyulan

[37] ISO 9126, http://en.wikipedia.org/wiki/ISO_9126, 4.4.2011

kaynak miktarı arasındaki ilişkiye dayalı özellikler kümesidir.

- Zaman davranışı,
- Kaynak davranışı.

Dayanıklılık – Gerekli değişiklikleri yapabilmek için gerekli olan çabaya dayalı özellikler kümesidir.

- İstikrar,
- Analiz edilebilirlik,
- Değiştirilebilirlik,
- Test edilebilirlik.

Taşınırlık – Yazılımın bir ortamdan diğerine taşınabilmesi üzerine dayalı özellikler kümesidir.

- Yüklenebilirlik,
- Yer değiştirilebilirlik,
- Şartlara ve çevreye uyma yeteneği.

ISO 9126'da, her bir kalite alt özelliği, daha alt niteliklere bölünmüştür. Bir nitelik, yazılım ürününde doğrulanan ve ölçülebilen bir varlıktır. Yazılım projelerinde değişkenlik gösterdiğinden, bu nitelikler standartta anlatılmamıştır.

Bu standart, organizasyonların bir yazılım ürününe ait kalite modeli tanımlaması için çatı sağlamakta, her bir organizasyonun kendi modelini tanımlama görevini organizasyona bırakmaktadır.

ISO 9126 “kusur” ve “uygunsuzluk” kavramlarını ayırmıştır. Kusur; niyetlenilen kullanıcı gereksinimlerini karşılayamamak olarak nitelendirilirken, uygunsuzluk, belirlenen gereksinimlerin karşılanmaması olarak tanımlanır. Benzer bir ayrım *Doğrulama* ve *Geçerleme* kavramları arasında da yapılır. Bu durum test aşamasında “V&V” (Validation and Verification) olarak isimlendirilmiştir.

Konuya, yazılımla ilgili kalite yükümlülükleri açısından bakıldığında, Kamu'ya proje hazırlık aşamasında rehber olması amacıyla hazırlanan, DPT'nin Temmuz 2007 tarihli Kamu Bilgi ve iletişim Teknolojisi Projeleri Hazırlama Kılavuzu'nda, “2007 yılından itibaren Yatırım Programı‟nda yer alan tüm BT projeleri kapsamındaki uygulama yazılımı geliştirme bileşenleri için belirlenecek kriterler çerçevesinde SPICE veya CMMI kalite olgunluk seviyelerine uyumun zorunlu hale

getirileceği" ifade edilmektedir.

Bu çerçevede, 2008-2010 Döneminde, yeni proje olarak Yatırım Programı'nda yer alacak veya henüz ihalesi yapılmamış olan ve uygulama yazılımı geliştirme bileşeni içeren BT projelerinde, tahmini proje tutarı 5.000.000 YTL ve üzeri olanlar için CMMI Seviye 2 veya eşdeğer yazılım kalite sertifikasyonları (SPICE 3"üncü seviyesi, AQAP[1]) aranmasının zorunlu olduğu belirtilmektedir. Ayrıca, "Proje tutarı 5.000.000 YTL"nin altında olan ve uygulama yazılımı geliştirme bileşeni içeren BT projelerinde, ISO 12207 Yazılım yaşam Döngüsü Standardının uygulanması gerekmektedir" denilmektedir.

Anılan düzenlemelerin, Kamu'da, ilerleyen zaman içinde, satın alınacak hizmet ve ürünler bakımından standardizasyon arayışının daha fazla önem kazanacağını ortaya koyan çalışmalar olduğu değerlendirilmektedir**.**

2.1.4. COSO

Kurumsal Risk Yönetim Modeli olan COSO (Tahrif edilmiş Mali Raporlama Komisyonu İçin Sponsor Kuruluşlar Komitesi - The Committee of Sponsoring Organizations of the treadway commission), iç kontrolü, "bir kurumun yönetim kurulu, yönetimi ve ilgili diğer personeli tarafından uygulanan ve aşağıdaki kategorilerde hedeflere ulaşma seviyesi konusunda makul güvence vermeyi amaçlayan bir süreç" olarak tanımlamaktadır :

- Operasyonların etkinliği ve verimliliği,
- Mali raporlamanın güvenilirliği,
- İlgili kanunlara ve mevzuata uyum.

COSO, risk analizinde kullanılan bir yöntem olarak bilinmekle birlikte aslında 1985 yılında ABD'de kurulan gönüllü bir özel sektör kuruluşudur. İç denetimin etkinliğini artırmayı amaçlamaktadır. Süreç odaklıdır. 1992 yılında İç Denetim – tümleşik Çerçeve'sini yayınlamıştır[38].

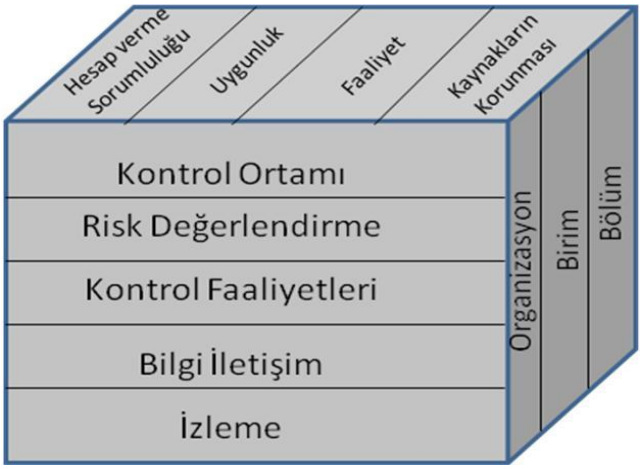
[38] PWC Çözüm Ortaklığı Platformu, şirketlerde İç Kontrol ve İç Denetim Fonksiyonu, PWC, http://www.pwc.com, 22.12.2007,

COSO raporu dört bölümden (cilt) oluşmaktadır :

- İç denetim çerçevesine üst düzey bakış sağlayan **Yönetimsel Özet**,
- İç denetim sisteminin değerlendirilme kriterlerini içeren **Çerçeve**,
- Rehber niteliğindeki **Raporlama**,
- İç denetim sisteminin değerlendirilmesi için yararlı olacak materyalleri içeren değerleme araçları.

Rehberlik raporları iç denetimi oluşturan beş bileşenden oluşmaktadır (bkz. Şekil 4) :

- ***Kontrol Ortamı***
- ***Risk Değerlendirme***
- ***Kontrol Faaliyetleri (Politikalar ve prosedürler)***
- ***Bilgi ve İletişim***
- ***İzleme***



Şekil 11 : COSO Kübü

2.1.5. ISO 9001 Kalite Yönetim Sistemi, Toplam Kalite Yönetimi, Six Sigma Kalite

1940'lı yıllarda endüstrilerinin tahrip olması sonrası, kalifiye iş gücü eksikliği nedeniyle ucuz ve kalitesiz üretim yapan Japonlar yeni bir arayışa yönelmişlerdir. Bu arayış çerçevesinde, kalite guruları olarak kabul edilen Joseph M. Juran, W. Edwards Deming ve Armand V.Feigenbaum'un fikirlerinden yararlanan Japonlar, 1950'lerin başlarında fabrikalarında ilk "kalite yönetim" pratiklerini gerçekleştirmişlerdir. Kalite kontrolü ve kalite yönetimi zamanla bir Japon Yönetim Felsefesi haline gelmiştir. Bunun sonucunda, 1960'ların sonu ile 1970'lerin başlarında, daha ucuz ve kaliteli ürünler sunmayı başaran Japonlar'ın, ABD ve Avrupa ülkelerine ihracatı hızla artmaya başlamıştır.

1960'da, "Kalite Kontrolü" konusundaki ilk uluslararası konferans, Japonların ev sahipliğinde Tokyo'da yapılmış ve "Toplam Kalite" terimi Feigenbaum tarafından ilk defa burada kullanılmıştır. Toplam kalite anlayışı Japon Şirketlerinde, 1970'lerin sonlarından başlayarak giderek daha fazla benimsenmeye başlanmıştır.

Esas itibariyle, Toplam Kalite Yönetimi, müşteri (bilişim teknolojilerinde kullanıcı) odaklıdır. Bir grup etkinliğidir. Bireysel olarak gerçekleştirilemez. Hataları önlemek ve kaliteye ulaşmak, üst yönetimden, çalışanlara, tedarikçilerden üretim sürecinde görev alan tüm çalışanlara kadar herkesin sorumluluğudur.

Japonların, uygulamaya başladıkları kalite yönetimi anlayışıyla ürettikleri ürünler sayesinde dünya pazarında pay sahibi olmaya başlamaları batı dünyasını da harekete geçirmiş; bu doğrultuda İngiltere'de, 1979'da, kalite sistemleri için BS (British Standard) 5750 dokümanı yayınlanmıştır. Aynı kapsamda, 1983'de, dünya piyasalarındaki rekabet ortamında, endüstri dünyasının dikkatini kalitenin önemine çekebilmek amacıyla Ulusal Kalite Kampanyası başlatılmıştır. O tarihten sonra belgelendirmeye (sertifikasyona) yönelik olarak, BS 5750 dokümanı temel alınarak geliştirilen ISO (International Organization for Standardization) 9000 tüm dünyaca kabul gören kalite sistemleri standardı haline gelmiştir. Anılan belge, ISO tarafından 2000 yılında tekrar gözden geçirilmiş ve ISO 9001:2000 adıyla yayınlanmıştır[39]. ISO 9001:2000 süreç modelli olup, sekiz temel yönetim esası üzerine kurulmuştur.

[39] Bilişim Teknolojilerinde Kalite Yönetimi, Ahmet Pekel, Türkiye Cumhuriyet Merkez Bankası Lira Dergisi, Ocak 2007 tarihli, 41. sayı.

Bunlar[40] :

1. **Müşteri odaklılık:** Bir kuruluşun varlığı müşterilerine bağlıdır. Dolayısıyla halen mevcut ve gelecekteki müşteri ihtiyaçlarını anlamaya, müşteri isteklerini karşılamaya ve müşteriye beklentisinin üzerinde hizmet sunmaya çalışmalıdır.

2. **Liderlik:** Liderler kuruluştaki amaç ve hedef birliğini sağlarlar. Çalışanların, kuruluşun hedeflerine ulaşmaya yönlendirileceği bir ortamı oluşturmak ve sürekliliğini sağlamak liderin sorumluluğundadır.

3. **Çalışanların katılımı:** Bir kuruluş, tüm seviyedeki çalışanlardan oluşmaktadır ve çalışanların katılımı, onların yeteneklerinin kuruluşun yararına kullanılabilmesini sağlar.

4. **Proses (Süreç) yaklaşımı:** İlgili kaynaklar ve eylemler bir süreç (proses) olarak yönetilirse planlanan bir sonuca çok daha etkin bir Şekilde ulaşılabilir.

5. **Yönetimde sistem yaklaşımı:** ilişkili süreçleri (prosesleri) bir sistem olarak tanımlamak, anlamak ve yönetmek kuruluşun hedeflerine ulaşma konusundaki etkinliğine katkıda bulunur.

6. **Sürekli gelişme:** kuruluşun toplam performansının sürekli geliştirilmesi, kuruluş için kalıcı bir hedef olmalıdır.

7. **Karar verme sürecinde olgulara dayalı yaklaşım:** Etkili kararlar veri ve bilgilerin analizine dayanırlar.

8. **Tedarikçilerle karşılıklı faydaya dayalı ilişkiler:** Bir kuruluş ve onun tedarikçileri karşılıklı olarak birbirlerine bağlıdırlar. Karşılıklı faydaya dayalı bir ilişki her iki tarafın da değer üretme yetisini geliştirir.

ISO 9001 Kalite Yönetim Sistemi'nin, bilişim Teknolojileri Süreçlerinin Kalite Güvencesi'nin sağlanması bağlamında COBIT'in Kalite Yönetimi (PO8), İzle ve Değerlendir (ME1: Süreç İzleme, ME2: İç Kontrol Değerlendirme Yeterliliği) olarak bilinen kontrol hedeflerine ulaşılmasına yardımcı olacağı değerlendirilmektedir.

Kalite Yönetim Sistemi bağlamında son olarak, Six Sigma'dan bilgi amaçlı bahsedilecektir.

1980'lerin ortalarında Motorola firması, zamanla kalite geliştirme yöntemlerinden biri olarak kabul edilecek Six Sigma'yı kullanmaya başlamıştır. Anılan belge, resmi olarak 1995 yılında yayınlanmıştır. Six Sigma DMAIC ve DMADV olarak iki temel

[40] (1) KAS Certification International, http://www.kascert.com, 2011,
(2) TSE, http://www.tse.org.tr, 23.12.2011.

metodolojiden oluşmaktadır.

DMAIC olarak ifade edilen metodolojinin safhaları aşağıdaki gibidir :

1. Tanımla / **D**efine,
2. Ölç / **M**easure,
3. Analiz Et / **A**nalyze,
4. Geliştir / **I**mprove,
5. Kontrol Et / **C**ontrol.

DMADV olarak ifade edilen metodoloji ise aşağıdaki adımlardan oluşmaktadır :

1. Tanımla / **D**efine,
2. Ölç / **M**easure,
3. Analiz Et / **A**nalyze,
4. Tasarla / **D**esign,
5. Doğrula / **V**erify.

Six Sigma'da, hatasız üretim, sayılarla ifade edilmektedir. Buna göre; %30.9 hatasız üretim "1", %69.1 hatasız üretim "2", %93.3 hatasız üretim "3", %99.4 hatasız üretim "4", %99.98 hatasız üretim "5", %99.99 hatasız üretim ise "6" sayısı ile ifade edilmektedir. Six Sigma, üretim performansını, işleyiş hatalarını tespit ederek ve düzelterek iyileştirmeyi amaçlamaktadır.

Bu kapsamda; Six Sigma'nın da ISO 9001 gibi süreç bazlı bir kalite yönetim sistemi olduğu ve COBIT'deki Kalite Yönetimi, İzleme ve Değerlendirme kontrol hedefleriyle uyumluluk sağladığı değerlendirilmektedir.

2.1.6. BS 7799, ISO 17799, ISO 27001

Bilgi güvenliği sahası, bilişim teknolojileri yönetişimde öncelikli olarak ele alınması gereken temel kalite unsurlarından biri olarak değerlendirilmektedir. Bu bölümde bilgi güvenliğine yönelik olarak dünya genelinde bugüne kadar yapılan standartlaştırma çalışmaları, tarihi gelişimi içinde ele alınacaktır. Bilişim teknolojileri süreçlerinin yönetimine yönelik olarak kullanılan belgelerden, 2000 yılında yayınlanan ISO 17799'un temeli 1995'de yayınlanan İngiliz Bilgi Güvenliği Standardı BS 7799'a dayanmaktadır. ISO 17799, Bilgi Güvenliği Yönetim Sistemi'ni

kurmayı hedefleyen bir standarttır. ISO 17799 dan, bilgi varlıklarına yönelik tehditler karşısında uygun koruma önlemlerinin alınmasını sağlayacak kurumsal bilgi güvenliği yönetimi altyapısının kurulmasında yararlanılmaktadır. ISO 17799'un son hali, 2007 yılında ISO 27002 olarak yeniden yayınlanmıştır. Denetime yönelik olan standart ise 2005'in sonunda yeniden düzenlenerek yayınlanan ISO 27001'dir. ISO 27001'de, Bilgi Güvenliği Olay Yönetimi başlığı dokümana ilave edilmiştir.

ISO 27001'in temelinde bilginin aşağıdaki niteliklerinin korunması yatmaktadır:

Gizlilik: Bilginin sadece erişim izni olanlar için erişilebilir olmasının sağlanması.

Bütünlük: Bilginin ve bilgi işleme yöntemlerinin tamlığının ve doğruluğunun sağlanması.

Erişebilirlik: Yetkisi olan kullanıcıların gerekli olduğunda bilgiye ve ilişkili varlıklara erişiminin sağlanması.

Bilgi varlıkları kurumsal düzeyde; gizlilik derecelerine göre çok gizli, gizli, hizmete özel, kişiye özel ve tasnif dışı olarak sınıflandırılmalı, bilgi üzerindeki tehditler belirlenmeli ve bu tehditlere uygun koruma tedbirleri alınmalıdır.

Bilgi güvenliği yönetim sisteminin uygulanmasında süreç yönetimi yaklaşımı benimsenmiştir.

"Planla-Uygula-Kontrol Et-Önlem Al" olarak bilinen kalite döngüsü, Bilgi Güvenliği Yönetim Sistemi'nin de uygulanma esaslarından birisidir. Bu anlamda, bilgi güvenliği başlı başına bir kalite hedefi olarak ön plana çıkmaktadır.

Anılan standart, farklı yapı ve sektördeki birçok kuruluş için aşağıdaki hedefleri içermektedir[41];

- Güvenlik gerekliliklerini ve amaçları belirlemek,
- Güvenlik risklerinin ekonomik olarak yönetildiğinden emin olmak,
- Yasal gerekliliklere uygunluktan emin olmak ,
- Bilgi güvenliği altyapısının içerdiği uygulamaların ve kontrollerin, kuruluşun amaçladığı güvenlik seviyesi ile uyumlu olduğunu göstermek ,
- Mevcut bilgi güvenliği yönetim süreçlerini belirlemek ve açıklamak,
- Yönetim tarafından, bilgi güvenliği yönetimi faaliyetlerinin durumunu belirlemek,
- İç ve dış tetkikçiler tarafından, kuruluşun, politikalara, prosedürlere ve

[41] (1) Evrim Numanoğlu, BSI Eurasia, http://www.kalder.org, 23.12.2007, (2) BSI Türkiye, http://www.bsi-turkey.com, 23.12.2007

standartlara uygunluğunu değerlendirmek,

- Ticari ortaklara, bilgi güvenliği politikaları, prosedürler ve standartlar hakkında bilgi sağlamak ,
- Müşterilere, kuruluşun bilgi güvenliği hakkında bilgi sağlamak.

27001'in uygulanması halinde COBIT çerçevesindeki aşağıdaki kontrol hedeflerine de ulaşılmaktadır:

PO4: BT Organizasyon ve ilişkilerinin Tanımlanması

- Risk, Güvenlik ve Uyumluluk Yükümlülükleri,
- Veri ve Sistem Sahipliği

PO6: Yönetimin Amaçlarının ve Talimatlarının İletilmesi

- Kurumsal BT Risk ve Kontrol Çerçevesi

PO8: Kalite Yönetimi

- Geliştirme ve Edinme

PO9: Risk Değerlendirme

- BT ve İŞ Riski Yönetimini uyumlaştırma,
- Risk Şartlarının oluşturulması,
- Olay Tanımlama,
- Risk Değerlendirme

AI2: Uygulama Yazılımı Tedarik Edilmesi ve Bakımı

- Uygulama Kontrol ve Denetim,
- Uygulama Güvenliği ve Mevcudiyeti/Kullanılırlığı

DS4: Sürekli Hizmetin Sağlanması

- BT Süreklilik Çerçevesi,
- BT Süreklilik Planının Bakımı,
- Planın Testi,
- Eğitimi,
- Dağıtımı

DS5: Sistem Güvenliğinin Sağlanması

- BT Güvenlik Yönetimi,
- BT Güvenlik Planı,
- Kimlik Yönetimi,
- Kullanıcı Hesap Yönetimi,

- Güvenlik Testi,
- Gözleme ve İzleme,
- Güvenlik Olay Tanımlama,
- Kriptolu Anahtar Yönetimi,
- Şüpheli Yazılım Önleme,
- Tespit ve Düzeltme,
- İletişim Ağı Güvenliği,
- Hassas Veri alış verişi

DS7: Kullanıcı Eğitimi

- Eğitim İhtiyaçlarının Belirlenmesi

DS11: Veri Yönetimi

- Veri Saklama Düzenlemeleri,
- Medya Kütüphanesi Sistemi,
- İmha, Yedekleme ve Geri Yükleme,
- Veri Yönetimi İçin Güvenlik Gereklilikleri.

DS12: Fiziksel Çevre Yönetimi

- Fiziki yerleşim Planı,
- Fiziki Güvenlik Ölçümü,
- Fiziki erişim,
- Çevre Şartlarına karşı Koruma.

ME3: Bağımsız Güvence Elde Edilmesi

- Kanun ve Düzenlemelerin BT Üzerindeki Etkisinin Belirlenmesi

Genel BT kontrollerine ek olarak,

AC: Yetki Kontrolü

- AC7: Doğruluk, Tamlık ve Yetki kontrolleri,
- AC8: Veri giriş Hata Önleme Şekli,
- AC9: Veri işlem Bütünlüğü,
- AC10: Veri işlem Gerçekleme ve Düzeltme,
- AC11: Veri işlem Hata Önleme Şekli,
- AC14: Çıktı Dengeleme ve Yeniden Konsolide Etme,
- AC16: Çıktı Raporları için Güvenlik koşulu,
- AC17: Aslına Uygunluk ve Bütünlük,

- AC18: Hassas Verinin İletilmesi Sırasında Korunması.

Halihazırda dünya genelinde alınmış olunan ISO 27001 BGYS sertifikası sayısı Tablo–5'de verilmektedir. Tablo 5'de, Türkiye'den alınan sertifika sayısının toplam 14 olduğu, en çok sertifikanın ise Japonya' dan alındığı görülmektedir[42].

Japonya	2354	İspanya	12	Sri Lanka	3
Hindistan	387	İsviçre	12	Vietnam	3
İngiltere	374	Birleşik Arap Em.	12	Belçika	2
Tayvan	165	Suudi Arabistan	10	Bulgaristan	2
Çin	101	Fransa	8	Danimarka	2
Almanya	93	İzlanda	8	Litvanya	2
Macaristan	60	İsveç	8	Umman	2
Kore	59	Yunanistan	7	Peru	2
ABD	59	Pakistan	7	Portekiz	2
Avustralya	53	Kuveyt	6	Katar	2
İtalya	45	Rusya Federasyonu	6	Ermenistan	1
Hollanda	32	Slovenya	6	Mısır	1
Hong Kong	30	Tayland	6	Gibraltar	1
Çek Cum.	28	Slovakya	5	Lübnan	1
Singapur	28	Arjantin	4	Lüksemburg	1
Malezya	22	Bahreyn	4	Makedonya	1
Avusturya	21	Kanada	4	Moldova	1
Polonya	21	Romanya	4	Fas	1
Brezilya	18	İili	3	Yeni Zelanda	1
İrlanda	18	Kolombiya	3	Ukrayna	1
Finlandiya	14	Hırvatistan	3	Uruguay	1
Norveç	14	Endonezya	3	Yugoslavya	1
Türkiye	14	Isle of Man	3		
Meksika	12	Makau	3		
Filipinler	12	Güney Afrika	3	**Toplam**	**4209**

Tablo 5: Ülkelere Göre ISO 27001 Sertifika Sayısı

[42] ISO 27001, http://www.iso27001certificates.com,

2.1.6.1. Bilgi Güvenliği Yönetim Sistemi (BGYS)

Bilgi Güvenliği Yönetim Sistemi BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar.

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

Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, dokümante edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir.

Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005* ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın belgelendirmesi

* Standartların sonunda yer alan :2005 yayınlandığı tarihi gösterir.

* Bu standardın orijinali Temmuz 2007 tarihinden itibaren ISO/IEC 27002:2005 adını almıştır. Bu makalenin yazıldığı tarih itibariyle TSE ilgili standartta bir isim değişikliği yapmamıştır.

2.1.6.1.1. Bilgi Güvenliği Yönetim Sistemi Kurulumu

TÜBİTAK–UEKAE konusunda TSE tarafından TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu standardı yayınlanmıştır.

ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart da doğrudan bilgi güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir.

BGYS standartları kapsamında BGYS'in kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için PUKÖ (Planla – Uygula – Kontrol et – Önlem al) modeli kullanılmaktadır.

ÜÇÜNCÜ BÖLÜM

3. ISACA-BT DENETİM VE GÜVENCE STANDARTLARI

3.1. ISACA

Kısaca Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Derneği) ISACA 1967 yılında küçük bir grubun bir araya gelmesi ile kuruldu. Bugün ISACA'ın 160'tan fazla ülkede 89,000 civarında çeşitli sektör ve seviyelerde çalışan BT profesyoneli üyesi var. Bu kadar farklı sektör ve seviyeden üyeye sahip olmak, ISACA üyelerin birçok konuda birbirlerinin deneyimlerinden faydalanmasını, görüş alışverişinde bulunmasını sağlamaktadır. ISACA'nın en önemli özelliklerinden bir tanesi de 70 ülkede kurulu olan 175 şubesidir. Bu şubeler üyelerine, eğitim, kaynak paylaşımı, profesyonel bağlantılar oluşturma konularında yardımcı olmaktadır.

ISACA kuruluşundan beri yönetişim, güvenlik ve denetim elemanları için dünyanın önde gelen kurumlarından biri olmuştur. Kurumun sertifikasyonunu yaptığı CISA (Certified Information Systems Auditor – Sertifikalı Bilgi Sistemleri Denetçisi) programı dünya çapında tanınmaktadır ve oluşumundan bu yana sertifikalı denetçi sayısı 60,000'e ulaşmıştır. Özellikle Bilgi Güvenliği alanının hedefleyen CISM (Certified Information Security Manager – Sertifikalı Bilgi Güvenliği Yöneticisi) sertifikasına sahip 10,000'in üzerinde bilgi güvenliği yöneticisi mevcuttur. Kurumsal BT Yönetişimi alanında ise CGEIT, (Certified in the Governance of Enterprise IT – Sertifikalı Kurumsal BT Yönetişim Uzmanı) sertifikası vermektedir. Kurum ISACA Journal adında BT kontrollerine yönelik bir dergi çıkarmakta, düzenlediği uluslararası konferanslar ile Bilgi Sistemleri Denetim ve Kontrolleri, Güvenlik ve BT Yönetişimi alanlarında hizmet vermektedir.

Bilgi Teknolojileri'nin Denetimi ve Kurumsal Yönetimi ile ilgili faaliyet gösterecek olan dernek, uzun yıllardır devam eden çalışmaların sonucunda 10 Mart 2009 tarihinde resmi olarak kuruluşunu tamamlamıştır. Derneğin öncelikli amacı organizasyonların yapısı içerisinde gittikçe daha önemli bir hale gelmeye başlayan bilişim teknolojilerinin denetlenmesine yönelik merkezi bir bilgi kaynağı ve kılavuz oluşturmaktır.

ISACA ve ITGI çatısı altındaki üye grubu tarafından "Komiteler" oluşturulmuştur. Bu "Komiteler" mesleki standartların belirlenmesinde, konferans ve seminerlerin düzenlenmesinde, uluslararası yayınların adaptasyonunda ve bunları destekleyen akademik çalışmalarda önderlik edeceklerdir.
COBIT'in yaygınlaşması ve kullanımı ile ilgili birçok eğitim, bilinçlendirme ve uygulama çalışmasına rehberlik etmek yönünde faaliyetler başlamıştır[43].

ISACA(Bilgi Sistemleri Denetim ve Kontrol Derneği) tarafından 01.01.2005 tarihinde bütün bilgi sistemlerine yönelik Bilgi Teknolojileri ve Bilgi Sistemleri Denetimi standartları yayınlanmıştır.

BT Denetim ve Güvence Standartları İndeksi	**Yürürlük Tarihi**
S1 Denetim Yönetmeliği	1 Ocak 2005
S2 Bağımsızlık	1 Ocak 2005
S3 Mesleki Etik ve Standartları	1 Ocak 2005
S4 Yeterlilik	1 Ocak 2005
S5 Planlama	1 Ocak 2005
S6 Denetim Görevinin Yürütülmesi	1 Ocak 2005
S7 Raporlama	1 Ocak 2005
S8 Denetim Sonrası İzleme Faaliyetleri	1 Ocak 2005
S9 Aykırılıklar ve Yasadışı Davranışlar	1 Eylül 2005
S10 BT Yönetişimi	1 Eylül 2005
S11 Denetim Planında Risk Değerlendirmesinin Kullanılması	1 Kasım 2005
S12 Denetimin Önemliliği	1 Temmuz 2006
S13 Diğer Uzman Çalışmalarının Kullanımı	1 Temmuz 2006
S14 Denetim Kanıtı	1 Temmuz 2006
S15 BT Kontrolleri	1 Şubat 2008
S16 E-ticaret	1 Şubat 2008

[43] www.isaca-istanbul.org

3.1.1. BT Denetim ve Güvence Standartları[44]

S1 Denetim Yönetmeliği

Bu BS Denetim Standardının amacı, denetim süresince kullanılan Denetim Yönetmeliği ile ilgili olarak bir rehber oluşturmak ve sağlamaktır.

Standart

Bilgi sistemi denetim işlevi ya da bilişim sistemi denetim görevlerinin amacı, sorumluluğu, yetkisi ve hesap verebilirliği denetim Yönetmeliğinde ya da hizmet sözleşmesinde uygun biçimde belgelenmelidir.

Denetim Yönetmeliği ya da hizmet sözleşmesi üstünde kurum(lar) içinde uygun seviyede anlaşmaya varılmalı ve onaylanmalıdır.

Açıklama

Kurum içi bilgi sistemleri denetim işlevinin, bir Denetim Yönetmeliği sürekli faaliyetleri kapsayacak biçimde hazırlanmalıdır. Denetim Yönetmeliği, yıllık olarak yada sorumlulukların çeşitlenmesi ya da değişmesi durumunda daha sıklıkla gözden geçirilmelidir. Bir hizmet sözleşmesi, Kurum içi BS denetçisinin denetime özel yada denetim dışı görevlerin kapsamını yeterince netleştirmek yada onaylamak için kullanılabilir. . Dışarıdan bir BS denetçisi için hizmet sözleşmesi her denetim veya denetim dışı görev için normal olarak hazırlanmalıdır.

Denetim Yönetmeliği ya da hizmet sözleşmesi, denetim işlevi ya da görevinin amaç, sorumluluk ve kısıtlamaları arasında yeterli ilişkiyi kuracak kadar ayrıntılandırılmalıdır.

Denetim Yönetmeliği ya da hizmet sözleşmesi, yazılı hale getirilen amaç ve sorumluluğu sağladığından emin olmak için belirli aralıklarla gözden geçirilmelidir.

Denetim Yönetmeliği ya da hizmet sözleşmesi hazırlarken daha fazla bilgi için aşağıdaki rehberlere ilgi gösterilmelidir:

- BS Denetim Rehberi G5 Denetim Yönetmeliği
- COBIT *Çerçevesi,* Kontrol Hedefi M4

[44] **ISACA-**Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri Klavuzu-Çevirmen Ömer YURDAGÜL

S2 Bağımsızlık

Bu BS Denetim Standardının amacı, denetim süresince bağımsızlık konusunda bir yol gösterici oluşturmak ve sağlamaktır.

Standart

Mesleki Bağımsızlık; Denetimle ilgili bütün konularda, BS denetçisi hem tavır hem de görünüş olarak denetlenen kurumdan bağımsız olmalıdır.

Kurumsal Bağımsızlık; BS Denetim işlevi, denetim faaliyetlerinin amaçlarının tarafsız bir biçimde tamamlanmasına olanak vermek için, denetim alanı veya faaliyetlerden bağımsız olmalıdır.

Açıklama

Denetim Yönetmeliği ya da hizmet sözleşmesi, denetim işlevinin bağımsızlık ve hesap verebilirliğini içermelidir.

BS Denetçisi, tutum ve davranışlarında daima bağımsız olmalı ve bağımsız görünmelidir.

Gerçekte ya da görünüşte bağımsızlık zarar görürse, zararın ayrıntıları ilgili taraflara açıklanmalıdır.

BS denetçisi, kurumsal olarak denetim alanından bağımsız olmalıdır.

Bağımsızlık, BS denetçisi, yönetim ve eğer var ise denetim komitesi tarafından düzenli olarak değerlendirilmelidir.

Düzenleyici kurumlar veya diğer mesleki standartlarca yasaklanmadıkça, BS denetçisinin, BS faaliyetlerindeki rolünün niteliği denetim dışı olduğu durumlarda bağımsız olmasına veya bağımsız gibi görünmesine gerek yoktur.

Mesleki ve Kurumsal Bağımsızlık hakkında daha fazla bilgi için aşağıdaki rehberlere başvurulabilir:

- BS Denetim Rehberi G17, BS Denetçisinin Bağımsızlığında Denetim Dışı Rolünün Etkisi.
- BS Denetim Rehberi G12, Kurumsal İlişkiler ve Bağımsızlık
- *COBIT* Çerçevesi, Kontrol Hedefi M4.

S3 Mesleki Etik ve Standartlar

Bu BS Denetim Standardının amacı, BS denetçisinin ISACA'nın Mesleki Etik Kurallarına bağlı kalmasına ve denetim görevinde beklenen mesleki özeni uygulamasında standart oluşturmak ve rehber sağlamaktır.

Standart

BS denetçisi, denetim yaparken ISACA Meslek Etik Kurallarına bağlı kalmalıdır.

BS denetçisi, denetim görevini yaparken, yürürlükteki mesleki denetim standartlarını gözeterek gereken mesleki özeni göstermelidir.

Açıklama

ISACA tarafından yayımlanan ISACA Mesleki Etik Kuralları, denetim mesleğinin ortaya çıkan yönelim ve gereksinimlerine uygun olarak zaman içinde değişecektir. ISACA üyeleri ve BS denetçileri, bir denetçi olarak görevlerini yerine getirirlerken en son ISACA Meslek Etik Kurallarına uygun davranmalıdırlar.

ISACA Meslek Etik Kuralları, sürekli gelişme için düzenli olarak gözden geçirilmekte ve denetim mesleğindeki zorluklara uyum Sağlaması gereğini karşılamak amacıyla gerektiğinde değiştirilmektedir. ISACA üyeleri ve BS denetçileri, denetim görevlerini yerine getirirlerken en son yürürlükteki BS denetim standartlarının farkında olmalı ve beklenen mesleki özeni göstermelidirler.

ISACA'nın Mesleki Etiği İlkelerine ve/veya BS denetim standartlarına uyumda başarısızlık, ISACA üyesinin ya da CISA sahibinin disiplin soruşturmasına uğraması ya da tamamen ihracıyla sonuçlanabilir.

ISACA üyeleri ve BS denetçileri, denetim görevlerini yerine getirirken kendi takım üyeleriyle iletişim kurmak ve takımın Mesleki Etik İlkelerine ve uygulanabilir BS Denetim Standartlarına uymalarını sağlamak durumundadırlar.

BS denetçileri, denetim görevlerini yerine getirirlerken karşılaştıkları her durumda Meslek Etiği uygulamaları veya BS Denetim Standartlarına uygun olarak işlem yapmalıdırlar. Meslek Etik ve BS denetim standartları zarar görmüş ya da zarar görüyor gibi Görünüyorsa, BS denetçisi sözleşmeden çekilmeyi düşünmelidir.

BS denetçisi, en yüksek seviyede dürüstlüğü ve ahlakı korumalı ve yasadışı, etik veya mesleki uygulamalarına uygun olmayan Yöntemleri kullanılmamalıdır.

Meslek Etiği ve Standartları hakkında daha fazla bilgi için aşağıdaki rehberlere başvurulabilir:

- BS Denetim Rehberi G19, Aykırılıklar ve yasadışılıklar
- BS Denetim Rehberi G7 Beklenen Mesleki Özen
- BS Denetim Rehberi G12, Kurumsal ilişkiler ve Bağımsızlık
- COBIT Çerçevesi, Kontrol Hedefleri M4.

S4 Mesleki Yeterlilik

Bu BS Denetim Standardının amacı, BS Denetçisinin mesleki yeterliğe ulaşıp bu yeterliğini muhafaza etmesi için ona rehberlik etmektir.

Standart

BS Denetçisi, denetim yapabilmesi için gerekli bilgi ve beceriye sahip ve mesleki açıdan yeterli olmalıdır.

BS Denetçisi, sürekli mesleki eğitim almak suretiyle mesleki yeterliğini devam ettirmek durumundadır.

Açıklama

BS Denetçisi, işe başlamadan önce, mesleki yeterliliğinin (planlanan işle ilgili becerisi, bilgisi, ve tecrübesinin) bulunduğu konusunda makul güvence sağlamalıdır. Şayet bunlar yoksa, BS Denetçisi görevi red etmeli yada geri çekilmelidir.

Eğer zorunlu ise, BS Denetçisi, CISA'nın sürekli mesleki eğitimi ya da geliştirme gereksinimlerini ve denetimle ilgili diğer mesleki atama şartlarını karşılamalıdır. CISA'ya ya da denetimle ilgili diğer atama şartlarına sahip olmayan ve bilgi sistemleri denetiminde yer alan ISACA üyeleri, yeterli resmi eğitim, hizmet içi eğitim ve iş deneyimine sahip olmalıdır.

BS Denetçisi, denetim görevini yürüten bir takımı yönetiyor ise, bütün üyelerin, yaptıkları işe uygun mesleki yeterlilik seviyesine sahip olduklarına makul güvence sağlamalıdır.

Mesleki Yeterlilik hakkında daha fazla bilgi için aşağıdaki rehberlere başvurulabilir:

- CISA sertifikasyon ve eğitim materyali
- CISA sürekli sertifikasyon ve eğitim gereksinimleri
- COBIT çerçevesi, kontrol hedefleri M2, M3 ve M4.

S5 Planlama

Bu BS denetim standardının amacı, denetimin planlaması konusunda standartları oluşturmak ve kılavuz sağlamaktır.

Standart

BS denetçisi, denetiminin hedeflerini karşılayacak bilgi sistemleri denetim kapsamını ve yürürlükteki kanun ve mesleki denetim standartlarıyla uyumlu planlamalıdır.

BS denetçisi, risk tabanlı bir denetim yaklaşımı geliştirmeli ve belgelendirmelidir.

BS denetçisi, denetimin doğasını ve hedefleri, zamanlaması ve kapsam ve hedeflerini ve gerekli kaynakların ayrıntılarını listeleyen denetim planını geliştirmeli ve belgelendirmelidir.

BS denetçisi, denetimini gerçekleştirmek için gerekli ayrıntılı şekilde denetim sürecinin doğasını, zamanlaması ve sınırlarını içeren bir denetim programı ve/veya planı geliştirmeli ve belgelendirmelidir.

Açıklama

Bir iç denetim birimi, sürekli faaliyetler için en azından yıllık olarak bir plan geliştirilmeli ve güncelleştirilmelidir. Bu plan denetim faaliyetlerinin çerçevesi olmalı ve denetim yönetmeliğiyle oluşturulan sorumlulukları yerine getirmeyi sağlamalıdır. Yeni /güncellenmiş plan, eğer var ise denetim komitesince onaylanmış olmalıdır.

Bir dış BS denetiminde, normalde her bir denetim veya denetim dışı görev için bir plan hazırlanmış olmalıdır. Bu plan denetimin hedeflerini kapsamalıdır.

BS denetçisi, denetim faaliyetleri anlamalıdır. Gerekli bilginin kapsamını kurumun doğası, çevresi ve riskleri ve denetimin hedefleri belirlenmelidir.

BS denetçisi, denetim sırasında bütün önemli konuların yeterli bir şekilde kapsayacağı konusunda makul güvence sağlamak için risk değerlendirmesi yapmak durumundadır. Denetim stratejileri, önemlilik seviyeleri ve kaynaklar sonra geliştirilebilir.

Denetim programı ve/veya planının, denetimin yürütülmesinde ortaya çıkan durumlara göre (yeni riskler, yanlış varsayımlar veya hâlihazırda gerçekleştirilmiş işlemlerden elde edilen bulgular gibi) denetim yönünün değiştirilmesine ihtiyaç duyulabilir.

Bir denetim yönetmeliği veya hizmet sözleşmesi hazırlanması konusunda daha fazla bilgi için aşağıdaki rehberlere başvurulabilir:

-BS denetim rehberi g6, bilgi sistemlerin denetimi için gereklilik kavramları

-BS denetim rehberi g15, planlama

-BS denetim rehberi g13 denetim planlamasında risk değerlendirmesinin kullanımı
-BS denetim rehberi g16 bir organizasyonunun bt kontrollerinde üçüncü tarafların etkileri
-COBIT çerçevesi, kontrol hedefleri

S6 Denetim işinin Yürütülmesi

Bu BS Denetim Standartlarının amacı, denetim işinin yürütülmesi ile ilgili rehber ve standartlar oluşturmak ve sağlamaktır.

Standart

Denetim ve Gözetim-BS Denetim Kadrosu, denetim hedeflerinin başarıldığının ve yürürlükteki mesleki denetim standartlarının karşılandığının makul güvencesini sağlamak amacıyla denetimin işinin yürütülmesi esnasında gözden geçirilmelidir.

Kanıt-Denetim süreci boyunca BS Denetçisi, denetim hedeflerini başarmak için gereken yeterli, güvenilir ve ilişkili bulgu sağlamalıdır. Denetim bulguları ve çıkarılan sonuçlar, bu kanıtların uygun analizi ve yorumuyla desteklenmelidir.

Dosyalama-Denetim süreci, yapılan denetimi ve BS Denetçisinin bulgu ve sonuçlarını destekleyen denetim kanıtını gösterir bir biçimde dosyalanmak zorundadır.

Açıklama

BS Denetim takımının rol ve sorumlulukları, asgari karar verme, uygulama ve gözden geçirme rollerini belirleyecek biçimde, denetimin başlangıcında oluşturulmalıdır.

Sözleşme kapsamında gerçekleştirilmekte olan iş, önceden belirlenmiş usuller takip edilerek sınıflandırılmalı ve dosyalanmalıdır. Bu dosyada, iş kapsam ve hedefleri, denetim programı, yürütülecek denetim aşamaları, toplanan kanıtlar, bulgular, sonuçlar ve öneriler gibi şeyler bulunmalıdır.

Denetim dosyası, bağımsız bir tarafın denetim sırasında gerçekleştirilen bütün görevleri yeniden gerçekleştirdiğinde aynı sonucu elde etmesine fırsat tanıyacak biçimde düzenlenmelidir.

Denetim dosyası, her denetim görevini kimin gerçekleştirdiğini ve rolünün ne olduğunu ayrıntılı biçimde içermelidir. Genel bir kural olarak, takımın bir üyesi veya bir üyeler grubu tarafından yapılan denetimle ilgili her görev, karar ve adım veya

ortaya çıkan sonuç, ilgili konunun önemine uygun olarak görevlendirilen aynı takımın diğer bir üyesi tarafından gözden geçirilmelidir.

BS Denetçisi, denetim kanıtının elde edilmesi için gerekli zaman, çaba ve denetim hedefinin önemiyle tutarlı ulaşılabilir en iyi denetim kanıtını kullanmayı planlamalıdır.

Denetim kanıtı, BS Denetçisinin bulgu ve sonuçlarını desteklemek ve görüşlerini Şekillendirmek için yeterli, güvenilir, ilgili ve faydalı olmalıdır. BS Denetçisi, denetim kanıtının bu kıstasları karşılamadığına karar verir ise daha fazla denetim kanıtı elde etmelidir.

Denetim işinin yürütülmesi hakkında daha fazla bilgi için aşağıdaki rehberlere başvurulabilir:

- COBIT *Çerçevesi,* Kontrol Hedefleri

S7 Raporlama

Bu BS Denetim Standardının amacı, BS denetçisinin raporlama sorumluluğunu yerine getirirken kullanacağı standardı oluşturmak ve yol göstericilik sağlamaktır.

Standart

BS Denetçisi, denetim tamamlanması sonucunda uygun biçimde bir rapor hazırlamalıdır. Rapor, kurumu, hedeflenen alıcıları ve dağıtım sınırlamalarını tanımlamalıdır.

Denetim raporu, yürütülen denetim işinin kapsamını, hedeflerini, denetim dönemini ve zamanlamasını, doğasını ve sınırlarını ortaya koymalıdır.

Rapor, BS Denetçisinin denetimle ilgili olarak bulgularını, sonuçlarını ve önerilerini, sahip olduğu çekincelerini, niteliklerini veya sınırlandırmalarını belirtmelidir.

BS Denetçisi, raporlanan sonuçları destekleyecek uygun ve yeterli denetim kanıtlarına sahip olmalıdır.

BS Denetçisi, raporunu bitirdiği zaman raporunu imzalamalı, tarih atmalı ve denetim yönetmeliği veya hizmet sözleşmesine göre dağıtmalıdır.

Açıklama

Raporun Şekli ve içeriği, hizmet türü ve anlaşma açısından çeşitlilik gösterir. Bir BS Denetçisi aşağıdaki maddelerden herhangi birisini uygulayabilir:

- Denetim (doğrudan veya onaylı)
- Gözden geçirme (doğrudan veya onaylı)

- Üzerinde anlaşılmış usuller

BS Denetçisi, anlaşma maddeleri uyarınca kontrol ortamı üzerinde fikir beyan etmesi gerektiğinde ve önemli veya kayda değer bir zayıflığın denetim kanıtı bulunması durumu, BS Denetçisinin iç kontrollerin etkili olduğu yönünde sonuca varmasını imkansız hale getirir. BS Denetçisinin raporu, önemli ve kayda değer zayıflıkları ve bunların kontrol kıstaslarının hedeflerinin başarılmasına etkilerini tanımlamalıdır.

BS Denetçisi taslak raporun içeriğini söz konusu alanda sonlandırılmadan ve yayınlanmadan önce yönetimle tartışmalı, nihai raporunda, yönetimin yorumlarına uygun yerlerde vermelidir.

BS Denetçisinin, kontrol ortamında önemli hatalar bulduğu durumlarda, bu hataları denetim komitesine veya sorumlu yetkililere bildirmelidir ve önemli hatalara dair bildirimin yapıldığını raporunda açıklamalıdır.

BS Denetçisi, ayrı raporlar hazırladığı durumlarda nihai raporunda tüm ayrı raporlara gönderme yapmalıdır.

BS Denetçisi, büyük hatalardan daha az önemli olan küçük boyutta iç kontrol yetersizliklerini yönetime bildirip bildirmeme konusunu kendisi düşünüp değerlendirmelidir. Bildirmesi durumunda, BS Denetçisi denetim komitesine veya sorumlu yetkililere bu iç kontrol yetersizliklerinin yönetime iletildiğini bildirmelidir.

BS Denetçisi, uygun ve zamanında önlemlerin alınıp alınmadığını belirlemek için önceki rapor bulgu, sonuç ve önerileriyle ilgili bilgileri istemeli ve değerlendirmelidir.

Rapor hazırlama hakkında daha fazla bilgi için aşağıdaki rehberlere başvurulabilir:

- BS Denetim Rehberi G20 Raporlama
- COBIT *Çerçevesi,* Kontrol Hedefleri M4.7 ve M4.8

S8 Denetim Sonrası İzleme Faaliyetleri

Bu BS Denetim Standardının amacı, BS Denetim sürecinde kullanılmak üzere denetim sonrası izleme faaliyetleri standardını oluşturmak ve yol göstericilik sağlamaktır.

Standart

Bulguların ve önerilerin raporlanmasından sonra, BS Denetçisi yönetim tarafından zamanında ve uygun bir şekilde harekete geçilip geçilmediğini belirlemek için ilgili bilgileri istemeli ve değerlendirmelidir.

Açıklama

Eğer yönetim, rapordaki uygulama önerilerine dair eylem planını BS Denetçisiyle tartışmış yada ona bildirmiş ise, bu eylemler nihai raporda yönetimin verdiği yanıt olarak kaydedilmelidir.

Denetim sonrası izleme faaliyetlerinin, doğası, zamanlaması ve kapsamı, raporlanan bulguların önemini ve düzeltici faaliyetlerin gerçekleştirilmemesinin etkisini dikkate almalıdır. Asıl raporla ilgili olarak, BS Denetim sonrası faaliyetlerin zamanlamasını bağlantılı risklerin doğası yada büyüklüğü ve kuruma maliyeti gibi çok sayıda varsayıma bağlı olarak ortaya çıkan mesleki yargısıyla belirlemelidir.

İç denetim BS birimi, yönetimin eylemleri etkili biçimde uygulamasını sağlamak ve izlemek için denetim sonrası izleme süreci oluşturmalıdır, aksi takdirde üst yönetim harekete geçmemenin riskini kabul eder. Denetim sonrası izleme faaliyetleri sorumluluğu, iç denetim birimi yönetmeliğinde tanımlanabilir.

Görevin alanı ve Şartlarına bağlı olarak dış BS Denetçileri, kendilerinin üzerinde anlaştıkları önerileri izlemek için bir iç BS Denetim birimine güvenebilirler.

Önerileri uygulamak için yapılan etkinliklerle ilgili olarak yönetimin bilgi sağladığı ve BS Denetçisinin de sağlanan bu bilgilerle ilgili şüphelerinin oluştuğu durumlarda, denetim sonrası izleme faaliyetleriyle ilgili sonuca varmadan önce gerçek durumun belirlenmesi amacıyla uygun test yada diğer usullerin kullanılması gereklidir.

Üzerinde anlaşmaya varılmış ama uygulanmamış önerileri de içeren, denetim sonrası izleme faaliyetlerinin durumuyla ilgili bir rapor eğer var ise denetim komitesine sunulabilir veya aynı rapor diğer bir seçenek olarak uygun seviyedeki kurum yönetimine sunulabilir.

Denetim sonrası izleme faaliyetlerinin bir parçası olarak BS Denetçisi eğer uygulanmadıysa bulguların hala geçerli olup olmadığını değerlendirmek durumundadır.

S9 Aykırılıklar ve YasadıŞı Hareketler

Bu ISACA Standardının amacı, denetim sürecinde BS denetçisinin göz önünde bulundurması gereken aykırılıklar ve yasadışı hareketlerle ilgili standardı oluşturmak ve yol göstericilik sağlamaktır.

Standart

BS Denetçisi, denetim riskini düşük bir seviyeye indirmek için denetimi planlanmasında ve yürütülmesinde aykırılıklar ve yasadışı hareketler riskini göz önünde bulundurmalıdır.

BS Denetçisi denetim süresince; aykırılıklar ve yasadışı hareketlerden dolayı önemli yanıltıcı ifadelerin olabileceği ihtimalini dikkate alarak, aykırılıklar ve yasadışı hareketler riski ilgili kendi değerlendirmelerine bakmaksızın mesleki Şüphecilik tutumunu sürdürmelidir.

BS Denetçisi, iç kontroller dahil kurumun kendisine ve çevresine hakim olmalıdır.

BS Denetçisi, . Yönetimin veya kurum içindeki diğer kişilerin mevcut, Şüpheli veya iddia edilen herhangi bir düzensizlik ve yasadışı hareketle ilgili bilgilerinin olup olmadığını belirlemek için yeterli ve uygun denetim kanıtı elde etmelidir.

BS Denetçisi, kurumun kendisi ve çevresine hakim olmak için denetim sürecini yürütürken aykırılıklar ve yasadışı hareketlerin riskini gösterebilecek sıra dışı veya beklenmedik ilişkileri göz önünde bulundurmalıdır.

BS Denetçisi, iç kontrollerin uygunluğunu ve yönetimin bu kontrolleri ihlâl etme riskini test etmek için süreçleri tasarlamalı ve gerçekleştirmelidir.

BS Denetçisi, yanıltıcı bir ifade belirlediğinde bu yanıltıcı ifadenin bir aykırılık ve yasadışı hareket göstergesi olup olmadığını değerlendirmelidir. BS Denetçisi, böyle bir gösterge var ise, denetimin diğer yanları ile özellikle de yönetimin temsilcileriyle ilişkilerinin çıkarımlarını da dikkate almalıdır.

BS Denetçisi yönetimden, en azından yılda bir kez veya denetim görevine bağlı olarak daha sık, yazılı açıklama istemelidir. Bu açıklama aşağıdakileri içermelidir:

- Aykırılık veya yasadışı hareketleri önleyici ve tespit edici iç kontrollerin tasarlanması ve uygulanması için

Sorumluluğunu kabul ettiğini göstermelidir.

- Bir aykırılık veya yasadışı hareket sonucu olarak önemli yanıltıcı bir ifadenin var olabileceğinin risk değerlendirmesinin sonuçlarını BS Denetçisine bildirmelidir.
- BS Denetçisine, kurumu etkileyen aykırılık ve yasadışı hareketlere dair aşağıdakilerle ilgili bilgilerini bildirmelidir.

Yönetim ve İç Kontrolde önemli rolü olan çalışanlar

-BS Denetçisine, çalışanlardan, önceki çalışanlardan veya düzenleyiciler tarafından bildirilmiş, kurumu etkileyen aykırılık veya yasadışı hareket iddialarını ya da aykırılık ve yasadışı hareket Şüphelerini bildirmelidir.

Eğer BS Denetçisi, somut bir aykırılık veya yasadışılık belirlemişse veya somut bir aykırılık ya da yasadışılık olması ihtimali bilgisini edinmişse, bu meseleleri yönetimin uygun kademesine zamanında bildirmelidir.

Eğer BS Denetçisi, yönetimle ilgili veya iç kontrolde önemli rolü olan çalışanlarla ilgili bir somut aykırılık veya yasadışı bir hareket belirlenmişse, bu meseleleri yetkili mercilere zaman geçirmeden iletmelidir.

BS Denetçisi, denetim esnasında dikkatini çeken düzensiz ve yasadışı hareketleri önleyici ve tespit edici kontrollerin tasarımında ve işleyişinden sorumlu uygun yönetim seviyesini ve yetkili mercileri önemli zayıflıklardan haberdar etmelidir.

BS Denetçisi, denetimi devam ettirmede kendisini etkileyen ve yasadışı bir hareketten veya yanıltıcı bir ifadeden kaynaklanan istisnai bir durumla karşılaşırsa, böyle durumlarla ilgili yürürlükteki yasal ve mesleki sorumlulukları dikkate almalı, sözleşme taraflarına veya bazı durumlarda yetkili yönetime veya düzenleyici kurumlara rapor etmeyi veya sözleşmeden çekilmeyi düşünmelidir.

BS Denetçisi, yönetime, yetkili mercilere, düzenleyicilere ve diğerlerine rapor edilmiş bir önemli aykırılık veya yasadışı bir hareketle ilgili bütün iletişimi, planlamayı, sonuçları, değerlendirmeleri ve yorumları dosyalamalıdır.

Açıklama

BS Denetçisi, bir aykırılık veya yasadışı hareket ne demektir tanımlamak için BS Denetim Rehberi G19, Aykırılıklar ve yasadışı Hareketler Bölümüne başvurmalıdırlar.

BS Denetçisi, aykırılıklar ve yasadışı hareketlerden kaynaklanan önemli yanıltıcı ifadeler olmamasına makul güvence sağlamalıdır. BS Denetçisi, bir görüşün kullanılması, test kapsamı ve iç kontrollerin kalıtsal sınırları gibi etmenlerden dolayı mutlak güvence sağlayamaz. Bir denetim sırasında BS Denetçisinin elde edebildiği denetim kanıtı, kesin delil olmaktan ziyade ikna edici olmalıdır.

Bir yasadışı hareketten kaynaklanan somut yanıltıcı bir ifadenin tespit edilememesi riski, bir aykırılık veya hatadan kaynaklanan somut yanıltıcı ifadenin tespit

edilememesi riskinden daha yüksektir, çünkü yasadışı hareketler, olayları saklamayı veya BS Denetçisine verilen kasıtlı yalan beyanda bulunmaya uygun tasarlanmış karmaşık planları içerebilirler.

BS Denetçisinin kuruma dair önceki deneyimi ve bilgisi denetim sırasında BS Denetçisine yardımcı olmalıdır. Sorgulamalar yaparken ve denetim usullerini yürütürken BS Denetçisinin geçmiş deneyimi tamamen göz ardı etmesi beklenmemeli. Ancak belli seviyede mesleki bir Şüphecilik içinde bulunması beklenmelidir. BS Denetçisi, ikna edici denetim kanıtı yerine yönetimin ve yetkili mercilerin doğru ve dürüst olduğu inancına dayanan düşük seviyede bir denetim kanıtından tatmin olmamalıdır. İkna edici denetim kanıtı hariç, BS Denetçisi ve denetim takımı, planlama ve tüm denetim boyunca kurumun aykırılıklar ve yasadışı hareket şüphe edilebilirliğini tartışmalıdır.

S9 Aykırılıklar ve Yasadışı Hareketler

Somut aykırılılar ve yasadışı hareketlerin varlığı riskini değerlendirmek için BS Denetçisi aşağıdakileri kullanmayı düşünmelidir:

- Kurumla ilgili önceki bilgi ve deneyimi (yönetim ve yetkili mercilerin doğruluğu ve dürüstlüğü ile ilgili bilgisi dahil)
- Yönetimin yaptığı soruşturmalardan elde edilen bilgi
- Yönetim açıklamaları ve iç kontrol beyanları
- Denetim sırasında elde edilen diğer güvenilir bilgi
- Yönetimin aykırılık ve yasadışı hareketlerle ilgili risk değerlendirmesi ve bu riskleri tanımlama ve risklere müdahale süreci

Aykırılıklar ve yasadışı hareketlerle ilgili daha fazla bilgi için aşağıdaki rehberlere başvurmalıdır:

- BS Denetim Rehberi G5, Denetim Yönetmeliği
- COBIT Çerçevesi, Kontrol Hedefleri DS3, DS5, DS9, DS11 VE PO6
- Sarbanes -Oxley Yasası, 2002
- Yabancı Uygulamalar Yasası 1977

S10 BT Yönetişimi

Bu BS Denetim Standartlarının amacı, denetim sürecinde BT yönetişimi alanlarında BS denetçinin ihtiyaç duyacağı standardı oluşturmak ve rehberlik sağlamaktır.

Standart

BS Denetçisi, BS işlevlerinin kurumun misyonu, vizyonu, değerleri, hedef ve stratejileriyle uyumlu olup olmadığını gözden geçirmeli ve değerlendirmelidir.

BS Denetçisi, BS biriminin iş (etkililik ve etkinlik) tarafından beklenen hizmeti ve başarısının değerlendirilmesi hakkında açık bir bildirime sahip olup olmadığını gözden geçirmelidir.

BS Denetçisi, BS kaynaklarının ve performans yönetim sürecinin etkililiğini denetlenmeli ve değerlendirmelidir.

BS Denetçisi, yasal, çevresel ve bilgi niteliği ve güvenlik ve emniyet gereksinimlerine uygunluğunu denetlenmeli ve değerlendirmelidir.

BS Denetçisi, risk temelli bir yaklaşım kullanarak BS birimini değerlendirmelidir.

BS Denetçisi, kurumun kontrol ortamını gözden geçirmeli ve değerlendirmelidir.

BS Denetçisi, BS ortamını olumsuz yönde etkileyebilecek riskleri gözden geçirmeli ve değerlendirmelidir.

Açıklama

BS Denetçisi BS Denetim Rehberi G18, BT Yönetişimine işaret etmelidir.

BS Denetçisi, iş sürecini destekleyen BS iş ortamı risklerini gözden geçirmeli ve değerlendirmelidir. BS Denetim etkinliği, risk yönetimi ve kontrol sistemleri gelişimine katkı sunarak ve maruz kalınan önemli riskleri tanımlayıp değerlendirerek kuruma destek sunmalıdır.

BT yönetişimi, kendi kendine ya da gözden geçirilen her BS işlevi bağlamında gözden geçirilebilir.

BS Denetçisi, BT yönetişimi hakkında daha fazla bilgi için aşağıdaki rehberlere başvurabilir:

BS Denetim Rehberleri:

- G5 Denetim Yönetmeliği
- G6 Bilgi Sistemleri Denetimi İçin Önemlilik Kavramları
- G12 Kurumsal ilişki ve Bağımsızlık
- G13 Denetim Planlamasında Risk Değerlendirmesi Kullanımı

- G15 Planlama
- G16 Kurum BT kontrollerine Üçüncü Tarafların Etkisi
- G17 BS Denetçisinin Bağımsızlığında Denetim dışı Rolünün Etkisi
- COBIT *Yönetim Rehberleri*
- COBIT *Çerçevesi, Kontrol Hedefleri;* bu standart bütün COBIT alanları kontrol hedefleriyle ilişkilidir
- *BT Yönetişimi Kurul Bilgilendirmesi 2. Basım*; BT yönetişim Enstitüsü
- *Sarbanes – Oxley için BT kontrol Hedefleri*, BT yönetişim Enstitüsü
- US Sarbanes – Oxley Yasası 2002 ve diğer özel yönetmelikler ayrıca uygulanabilir.

S11 Denetim Planlanmasında Risk Değerlendirmesinin Kullanımı

Bu BS Denetim Standartlarının amacı, denetim sürecinde risk değerlendirmesinin kullanımı için bir standart oluşturmak ve yol göstericilik sağlamaktır.

Standart

BS Denetçisi, BS Denetim planının tamamını geliştirmede ve BS Denetim kaynaklarının etkili dağıtımı için önceliklerin belirlenmesinde kullanılabilecek uygun bir risk değerlendirme tekniği veya yaklaşımı kullanmalıdır.

BS Denetçisi, kişisel denetim planlamasında, denetlenen alanla ilgili riskleri tanımlamalı ve değerlendirmelidir.

Açıklama

Risk değerlendirmesi, BS Denetim evrenindeki denetlenebilir birimleri kontrol etmek, gözden geçirmek ve en yüksek risklere sahip alanları, BS yıllık planına dahil etmek için seçmede kullanılan bir tekniktir.

Denetlenebilir bir birim, her kurumun ve onun sistemlerinin ayrı bir parçası olarak tanımlanmıştır.

BS Denetim evreninin belirlenmesi, kurumun BT stratejik planı işleyişine ve ilgili yönetim birimleriyle yapılan görüşmelerinin bilgisine dayanmalıdır

BS Denetim planını geliştirmeyi kolaylaştırmak için risk değerlendirmesi uygulaması, en azından yılda bir kez yapılmalı ve dosyalanmalıdır. Kurumsal stratejik planlar, amaçlar ve kurumsal risk yönetim çerçevesi uygulamaları risk değerlendirmesinin bir parçası olarak değerlendirilmelidir.

BS Denetçisine, denetim projelerinin seçiminde risk değerlendirmesinin kullanımı, BS Denetim planını veya belirli bir gözden geçirmeyi tamamlamak için gereken BS Denetim kaynaklarının miktarını belirlemek ve gerekçelendirmek için olanak tanır.

Ayrıca, BS Denetçisi, risk algılamalarına dayanarak ve risk yönetim çerçevesinin raporlamasına katkı sağlamak için gözden geçirmelerin zamanlamasını da önceliklendirebilir.

Bir BS Denetçisi, gözden geçirilen alanla ilgili risklerin bir ön değerlendirmesini gerçekleştirmelidir. Her bir özellikli gözden geçirme için, BS Denetim görev amaçları böyle bir risk değerlendirmesinin sonuçlarını yansıtmalıdır.

BS Denetçisi, gözden geçirmenin tamamlanmasından sonra, gözden geçirme bulgu ve önerileri ile denetim sonrası faaliyetleri yansıtması için, eğer böyle bir kayıt varsa kurumun Kurumsal risk yönetiminin çerçevesinin veya risk kütüğünün güncellenmesini sağlamalıdır.

BS Denetçisi, BS Denetim Rehberi G13 Denetim Planlanmasında Risk Değerlendirmesinin Kullanımı bölümüne ve BS Denetim usulü P1 BS Risk Değerlendirmesi Ölçümü bölümüne başvurmalıdır.

S12 Denetimin Önemliliği

Bu BS Denetim Standardının amacı, denetim önemliliği kavramını ve bu kavramın denetim riski ile ilişkisine dair standart oluşturmak ve yol göstericilik sağlamaktır.

Standart

BS Denetçisi, denetim usullerinin sınırı, doğası ve zamanlaması belirlenirken denetimin önemliliği ve bunun denetim riskiyle ilişkisini göz önünde bulundurmalıdır.

BS Denetçisi, kontrollerin olmaması veya zayıf olması ihtimalini veya kontrollerin olmamasının veya zayıflığının bilgi sistemlerinde önemli hatalara veya ciddi zayıflıklara yol açıp açmadığını dikkate almalıdır.

BS Denetçisi, küçük kontrol hataların ve kontrollerin olmaması veya zayıf olmasının toplam etkisinin bilgi sistemlerinde önemli hata veya ciddi zayıflıklara dönüşüp dönüşmediğini dikkate almalıdır.

BS Denetçisinin raporu, yetersiz kontrollerin olması veya kontrollerin olmaması ve kontrol hatalarının önemini ve bu zayıflıklardan kontrol hatalarının ve ciddi zayıflıkların kaynaklanma olasılığını açıklamalıdır.

Ek Rehberlik

Denetim riski, BS Denetçisinin denetim bulgularına dayanarak yanlış sonuçlara ulaşması riskidir. BS Denetçisi, denetim risklerinin üç bileşeninin de farkında olmalıdır: Kalıtsal risk, kontrol riski ve belirleme riski. Risklerle ilgili daha ayrıntılı açıklamalar

Ve bilgi için, G13, Denetim Planlamasında Risk Değerlendirmesinin Kullanımı bölümüne başvurunuz.

BS Denetçisi, denetimi planlarken ve yürütürken denetim riskini kabul edilebilir bir seviyeye indirmeye ve denetim hedeflerini gerçekleştirmeye çalışmalıdır. Bu, BS ve ilgili kontrollerin uygun biçimde değerlendirmesiyle başarılır.

Kontrollerdeki zayıflıklar, eğer kontrollerin olmaması kontrol hedeflerinin gerçekleştirilmesinde makul bir güvence sağlamada başarısızlıkla sonuçlanıyorsa önemli kabul edilir.

Önemli olarak sınıflandırılan bir zayıflık şu anlama gelir:

- Kontroller yerinde değildir ve/veya kontroller kullanımda değildir ve/veya kontroller yetersizdir.
- Hataların artmasına sebep olur

Önemli zayıflık, önlenemeyen ve tespit edilemeyen istenmeyen olay(lar)ın düşük olma olasılığını artıran önemli hata veya önemli hataların bileşkesidir.

Önemlilik ve BS Denetçisi tarafından kabul edilebilir denetim riski seviyesi arasında tersine bir ilişki vardır; örneğin önemlilik seviyesi ne kadar yüksekse denetim riskinin kabul edilebilirliği o kadar düşük olur veya tam tersi söz konusudur. Bu, BS Denetçisine denetim usullerinin doğasını, zamanlamasını ve sınırlarını belirlemesini sağlar. Örneğin, BS Denetçisi özellikli bir denetim usulünü planlarken önemliliği düşük belirler ve bu sebeple denetim riski artar. BS Denetçisi, bu durumu ya kontrollerin testlerini artırarak (kontrol riskinin değerlendirmesini azaltarak) ya da maddi doğruluk test usullerini genişleterek gidermek ister

(tespit etme riskinin değerlendirmesini azaltarak).

BS Denetçisi, bir kontrol hataları bileşkesinin veya tek bir kontrol hatasının önemli bir hata mı ya da önemli bir zayıflık mı olduğunu belirlemede azaltıcı kontrollerin etkisini ve bu tür azaltıcı kontrollerin etkin olup olmadığını değerlendirmelidir.

BS Denetçisinin önemlilik ve denetim riski değerlendirmesi, Şartlara ve değişen çevreye bağlı olarak zaman zaman değişebilir.

BS Denetçisi, BS Denetim Rehberi G6 Bilgi Sistemleri Denetimi için Önemlilik Kavramları Rehberine başvurmalıdır.

Denetim önemliliği konusunda daha fazla ilgi için aşağıdaki rehberlere başvurulmalıdır:

- BS Denetim Rehberi:
- *G2 Denetim Kanıtı Gereksinimi*
- *G5 Denetim Yönetmeliği*
- *G8 Denetim Dosyalaması*
- *G9 Aykırılıklar için Denetim Varsayımları*
- *G13 Denetim Planlamasında Risk Değerlendirmesinin Kullanımı*
- COBIT 4.0, IT yönetişim Enstitüsü, 2005
- *Sarbanes-Oxley için IT Kontrol Hedefleri*, IT yönetişim Enstitüsü, 2004

S13 Diğer Uzmanların Çalışmalarının Kullanımı

Bu BS Denetim Standardının amacı, denetimde diğer uzmanların çalışmalarını kullanan BS Denetçileri için bir standart oluşturmak ve yol göstericilik sağlamaktır.

Standartlar

BS Denetçisi, uygun olan yerlerde denetim için diğer uzmanların çalışmalarını kullanmayı düşünmelidir.

BS Denetçisi, denetim görevinden önce diğer uzmanların bağımsızlık ve kalite kontrol süreçleri, ilgili deneyim, kaynaklar, uzmanlıklar, mesleki nitelikler gibi konuları değerlendirmeli ve tatmin olmalıdır.

BS Denetçisi, denetimin bir parçası olarak diğer uzmanların çalışmalarını gözden geçirmeli, değerlendirmeli ve ne derece kullanılacaklarına ve ne kadar güvenileceklerine karar vermelidir.

BS Denetçisi, diğer uzmanların çalışmalarının, BS Denetçisine güncel denetim hedefleri hakkında sonuca varmaya sağlamada yeterli ve tam olup olmadığını saptamalı ve sonuçlandırmalıdır. Varılan sonuç açık bir biçimde belirtilmelidir.

BS Denetçisi, diğer uzmanların yeterli ve uygun denetim kanıtı sağlamadığı yer ve durumlarda yeterli ve uygun denetim kanıtı elde etmek amacıyla ek test usulleri uygulamalıdır.

BS Denetçisi, ek test usulleri kullanılarak gereken kanıtın elde edilemediği durumlarda uygun denetim görüşü sağlamalı ve kapsamını sınırlandırmalıdır.

Ek Rehberlik

BS Denetçisi, gerçekleştirilecek denetim işini veya denetimin kalitesindeki olabilir kazanımları zayıflatabilecek kısıtlamaların olduğu durumlarda diğer uzmanların çalışmalarını kullanmayı düşünmelidir. Bunlara örnek olarak, gerçekleştirilecek işin teknik doğası tarafından gerek duyulan bilgi, denetim kaynağı kıtlığı ve zaman kısıtlamaları verilebilir.

Bir uzman, BS Denetim takımı ya da üst yönetim tarafından, dış muhasebe firmasından, bir yönetim danışmanlığı firmasından, bir BT uzmanı ya da denetim alanındaki bir uzman atanarak bilgi sistemi denetçisi olabilir.

Bir uzman, kurum içinden de, kurum dışından da olabilir. Eğer bir uzman kurumun diğer bir bölümüyle de ilgiliyse, uzmanın raporuna güven duyulabilir. Bazı durumlarda bu, BS Denetçisinin destekleyici belgeleme ve çalışma belgelerine erişimi olmasa bile BS Denetim kapsamının duyduğu gereksinimi azaltabilir. BS Denetçisi, böyle durumlarda görüş belirtirken dikkatli olmalıdır.

BS Denetçisi, diğer uzmanların bütün çalışma belgelerine, destekleyici belgelere ve raporlarına -yasal açıdan sakınca olmadığı sürece erişim hakkına sahip olmalıdır. Yasal açıdan sakınca bulunan ve bu yüzden erişimin olmadığı durumlarda BS Denetçisi diğer uzmanın çalışmalarına güven ve kullanım sınırları uygun biçimde belirlemeli ve karar vermelidir.

BS Denetçisinin, diğer uzman raporunun kullanımı hakkındaki görüş, ilişkililik ve yorumları BS Denetçisinin raporunun bir parçasını oluşturmalıdır.

BS Denetçisi, denetim hedeflerine ulaşmak için BS Denetçisinin yeterli, güvenilir, ilgili ve faydalı kanıtlar elde etmesi gerektiğini anlatan BS Denetim Standardı S6 Denetim İşinin Yürütülmesi bölümüne başvurmalıdır.

BS Denetçisi, denetimi yapmak için gereken yeteneklere veya diğer uzmanlıklara sahip değilse diğer uzmanlardan yardım almalıdır; bununla birlikte, BS Denetçisi

yürütülen işle ilgili bilgi sahibi olmalıdır fakat kendisinden bir uzmanınkine denk bilgi sahibi olması beklenmemelidir.

BS Denetçisi, BS Denetim Rehberi G1 Diğer Denetçilerin ve Uzmanların Çalışmalarının Kullanımı bölümüne başvurmalıdır.

Diğer denetçilerin ve uzmanların çalışmalarının kullanımı konusunda detaylı bilgi için aşağıdaki rehberlere başvurulmalıdır:

- BS Denetim Rehberleri
- *G5 Denetim Yönetmeliği*
- *G8 Denetim Belgelendirmesi*
- *G2 Denetim Kanıt Gerekliliği*
- *G10 Denetim Örneklemesi*
- *G13 Denetim Planlamasında Risk Değerlendirmesinin Kullanımı*
- *COBIT 4.0, IT Yönetişim Enstitüsü, 2005*
- *Sarbanes-Oxley için IT Kontrol Hedefi*, IT YönetiŞim Enstitüsü, 2004

S14 Denetim Kanıtı

Bu BS Denetim Standartlarının amacı, BS Denetçisi tarafından elde edilecek denetim kanıtını nelerin oluşturduğu ve bu kanıtın nicelik ve niteliği ile ilgili standart oluşturmak ve yol göstericilik sağlamaktır.

Standart

BS Denetçisi, denetim sonuçlarının dayandığı makul çıkarımlara temel olacak yeterli ve uygun denetim kanıtı sağlamalıdır.

BS Denetçisi, denetim sırasında elde edilen denetim kanıtının yeterliliğini değerlendirmelidir**.**

Açıklama

a) Uygun Kanıt

Denetim kanıtı:

- Denetçi tarafından kullanılan usulleri içerir
- BS Denetçisi tarafından kullanılan usullerin sonuçlarını içerir
- Denetimi desteklemek için kullanılan kaynak belgeleri (elektronik veya basılı olarak), kayıtları, güçlendirici bilgileri içerir
- Denetim işinin bulgu ve sonuçlarını içerir

- İşin yapıldığını ve yürürlükteki yasalara, düzenlemelere ve politikalara uygunluğunu gösterir

BS Denetçisi, kontrol testlerinden denetim kanıtı elde ederken değerlendirilen kontrol riski seviyesini desteklemek amacıyla denetim kanıtının tamlığını, dikkate almalıdır.

Denetim kanıtı uygun bir Şekilde tanımlanmış, çapraz ilişkilendirilmiş ve kataloglanmış olmalıdır

Denetim kanıtının kaynağı, doğası (yazılı, sözlü, görsel, elektronik, gibi) ve asıllık (dijital ve el imzaları, mühürler, vb.) gibi özellikler güvenilirlik değerlendirmesi sırasında göz önünde bulundurulmalıdır.

b) Güvenilir Kanıt

Genel olarak, denetim kanıtı güvenilirliği aşağıdaki durumlarda daha büyüktür**:**

-Sözlü ifadelerden ziyade yazılı biçimde olması

-Bağımsız kaynaklardan elde edilmesi

-Denetlenen kurumca sağlanmasındansa BS Denetçisi tarafından elde edilmiş olması

-Bağımsız biri tarafından onaylı olması

-Bağımsız biri tarafından saklanmış olması

BS Denetçisi, denetim hedeflerini ve denetim risklerini karşılayacak gerekli kanıtları elde ederken maliyeti en uygun olan araçları düşünmelidir. Fakat gerekli bir işlemi atlamak için maliyet veya zorluk geçerli bir özür değildir.

Denetim kanıtı elde etme usulleri, denetim konusuna bağlı olarak değişir (denetimin doğası, zamanlaması, mesleki yargılar vb.).

BS Denetçisi, denetim hedefleri için en uygun usulü seçmelidir.

BS Denetçisi, denetim kanıtını aşağıdaki biçimlerde elde edebilir:

- Soruşturma
- Gözlem
- Araştırma ve doğrulama
- Yeniden gerçekleştirme
- Yeniden ölçüm yapma
- Hesaplama
- Analitik usuller
- Genel kabul görmüş diğer yöntemler

BS Denetçisi, güvenilirliği ve daha fazla doğrulanabilirliği değerlendirmek için bilginin elde edildiği kaynağı ve özelliklerini dikkate almalıdır.

c) Yeterli Kanıt

Kanıt denetim hedefi ve kapsamında bütün önemli soruları destekliyorsa yeterli olarak düşünülebilir.

Denetim kanıtı, bağımsız ve yetkin bir tarafın testleri yeniden gerçekleştirdiğinde aynı sonuçları elde etmesini sağlayacak derecede nesnel ve yeterli olmalıdır. Kanıt, konunun ve ilişkili olduğu risklerin önemine uygun olmalıdır.

Yeterlilik, denetim kanıtı miktarının ölçüsüyken uygunluk, denetim kanıtının niteliğinin ölçüsüdür ve bu ikisi birbiriyle karşılıklı ilişki içindedir. Bu bağlamda, kurumdan elde edilen bilgi BS Denetçisi tarafından denetim süreçlerini gerçekleştirmek için kullanıldığı zaman BS Denetçisi bilginin doğruluğu ve bütünlüğüne gereken vurguyu yapmalıdır.

BS Denetçisi, yeterli denetim kanıtının elde edilemediğine inandığı durum ve yerlerde, bu gerçeği denetim sonuçlarıyla tutarlı bir Şekilde açıklamalıdır.

S14 Denetim Kanıtı (Devamı)

Delillerin Korunması ve Saklanması

Denetim kanıtı, yetkisiz erişimlere ve değiştirmelere karşı güvenlik altına alınmalıdır.

Denetim kanıtı, denetim işi tamamlandıktan sonra, yürürlükteki yasaların, düzenlemelerin ve politikaların öngördüğü sürede ve biçimde korunmalıdır.

Referans

Denetim kanıtı konusunda detaylı bilgi için aşağıdaki rehberlere başvurulmalıdır:

- BS Denetim Standardı S6, Denetim İşinin Yürütülmesi
- BS Denetim Rehberi G2, Denetim Kanıtı Gerekliliği
- BS Denetim Rehberi G8 Denetim Belgelendirmesi
- COBIT Kontrol Hedefi ME2 İç Kontrolün İzlenmesi ve Değerlendirilmesi ve ME3 Düzenlemelere Uygunluğun Sağlanması

S15 BT Kontrolleri

Bu ISACA Standardının amacı, BT kontrolleri ile ilgili standart oluşturmak ve yol göstericilik sağlamaktır.

Standart

BS Denetçisi, kurumun iç kontrol ortamının bütünleşik bir parçası olan BT kontrollerini izlemeli ve değerlendirmelidir.

BS Denetçisi, BT kontrollerinin tasarımı, uygulanması, işletimi ve geliştirilmesi ile ilgili öneriler sağlayarak yönetime yardımcı olmalıdır.

Açıklama

Yönetim, bir kurumun, BT kontrollerini de içeren iç kontrol ortamından sorumludur. Bir iç kontrol çevresi, iç kontrol sisteminin temel hedeflerinin başarılması için disiplin, çerçeve ve yapı sağlar.

COBIT, istenmeyen olayların tespit edilmesi, önlenmesi, düzeltilmesi ve iş hedeflerinin başarılmasına makul güvence sağlamak için tasarlanmış politikalar, usuller, uygulamalar ve kurumsal yapılar gibi kontrolleri tanımlar. Ayrıca, COBIT, kontrol hedefi ifadesini -*Belirli bir süreçte, kontrol usullerini kullanarak başarılması arzu edilen sonuç veya amaç* - olarak tanımlar.

BT kontrolleri, BT sisteminin edinilmesi, uygulanması, sunumu, desteklenmesi ve hizmetleri üzerindeki kontrolleri gösteren yaygın BT kontrolleri, ayrıntılı BT kontrolleri ve uygulama kontrollerini kapsayan genel kontrollerden oluşur.

Genel BT kontrolleri, kurumun BT sisteminin ve altyapısının tüm işleyişiyle ve otomatik çözümler (uygulamalar) kümesi ile ilgili riskleri en aza indiren kontrollerdir.

Uygulama kontrolleri, uygulamalar içerisinde gömülü kontroller kümesidir.

Yaygın BT kontrolleri, BT çevresini izlemek ve yönetmek için tasarlanmış ve bu sebeple BT ile ilgili bütün faaliyetleri etkileyen genel BT kontrolleridir. Bu kontroller, BT izlemesine ve yönetimine odaklanmış genel kontrollerin alt kontrol kümesidir.

Ayrıntılı BT kontrolleri, uygulama kontrollerine ilaveten yaygın BT kontrollerinde kapsanmayan genel BT kontrollerinden oluşur.

BS Denetçisi, BT kontrol süreçlerinin durumuyla ilgili güvence sağlamak amacıyla, BS Denetim kaynaklarının etkili dağılımı için öncelikleri belirlemede ve tüm denetim planının geliştirilmesinde uygun bir risk değerlendirme tekniği ya da yaklaşımı kullanmalıdır. Kontrol süreçleri, risklerin, risk yönetimi süreciyle

oluşturulmuş risk toleransları içerisinde bulunmasını sağlamak amacıyla tasarlanmış kontrol çevresinin bir parçası olan politikalar, usuller ve etkinliklerden oluşur.

BS Denetçisi, BT kontrollerini bilgisayar aracılığıyla gözden geçirirken seçici denetim kanıtlarını toplama ve sürekli olarak BS Denetçisine sistem güvenilirliğini izleme olanağı sunan sürekli güvencenin kullanımında veri analiz tekniklerinin kullanımını düşünmelidir.

Kurumlar üçüncü tarafları kullandıklarında bu taraflar kurumun kontrollerinde ve ilgili kontrol hedeflerinin başarılmasında temel unsur haline gelebilir. BS Denetçisi, BT çevresi, ilgili kontroller ve BT kontrol hedefleriyle ilişkili olarak üçüncü tarafların yürüttüğü rolü değerlendirmelidir.

Aşağıdaki ISACA ve BT Yönetişim Enstitüsü (ITGI) Rehberlerine, IT kontrolleriyle ilgili ayrıntılı bilgi için başvurulmalıdır:

- Rehber G3 Bilgisayar Destekli Denetim Tekniklerinin (BDDT) Kullanımı
- Rehber G11 Yaygın BS kontrollerinin Etkisi
- Rehber G13 Denetim Planlamasında Risk Değerlendirmesinin Kullanımı
- Rehber G15 Planlama
- Rehber G16 Kurumsal BT kontrollerinde Üçüncü Tarafların Etkisi
- Rehber G20 Raporlama
- Rehber G36 Biyometrik Kontroller
- Rehber G38 Erişim Kontrolleri
- COBIT çerçevesi ve kontrol hedefleri

DÖRDÜNCÜ BÖLÜM

4. DÜNYADA KAMUSAL BİLGİ SİSTEMLERİ DENETİMİ

ÜLKELER	Kullanılan Yaklaşımlar
FİNLANDİYA	"İç Kontrol ve Risk Yönetimi" İle İlgili Geliştirdikleri Kendi Standartları
NORVEÇ	COBIT Baz Alınmıştır
MACARİSTAN	COBIT Baz Alınmıştır
ÇEK CUMHURİYETİ	IT Yönetişimi ve Operasyonel Risk Kapsamında Sınırlı Düzenlemeler
MAKEDONYA	ISO 17799 Baz Alınmıştır
SLOVAKYA	Her Yıl Bilgi Sistemleri Güvenliğini Kapsayacak Bir Denetim Raporu
DANİMARKA	Finansal Denetimin Yanında Sistem, Operasyon, Veri ve İş Devamlılığı Denetimi
PORTEKİZ	Üç Yılda Bir BS Denetimi Yapılmasını Zorunlu Kılan Kanun Tasarısı
İSRAİL	ISO 17799 Baz Alınmıştır
HOLLANDA	Sınırlı Anlamda BS Denetimi'ne de Referansta Bulunan Standardlar
İTALYA	Sınırlı Anlamda BS Kontrolleri İçeren Düzenlemeler
SLOVENYA	ISO 17799 Baz Alınmıştır
YUNANISTAN	BS Denetimi'ne de Değinen Bankacılık İle İlgili İki Kanun
ALMANYA	Almanya Denetim Kuruluşu (IDW) Tarafından Geliştirilen PS 330 Standardı

Tablo 5: Ülkelere Göre Bilgi Sistemleri Denetimi Yaklaşımları

Tablodan da anlaşılacağı üzere Bilgi Sistemleri Denetimi hususunda bazı ülkelerin Cobit yaklaşımının, bazı ülkelerin ISO 17799(ISO 27001) ve bazı ülkelerinde kendi mevzuatlarını oluşturmak suretiyle denetimleri baz aldıkları görülmektedir.

Ülkemizde kamusal anlamda Bilgi Sistemleri Denetimine ilişkin Bankacılık Düzenleme ve Denetleme Kurumu tarafından 13.01.2010 tarihinde "*Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik"* ve 13.01.201 tarihinde *"Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Tebliğ"* yayınlanmış olup bu düzenlemeler ile bankacılık bilgi sistemleri denetiminin nasıl ve ne şekilde yapılacağı belirlenmiştir. BDDK tarafından denetimde COBİT çerçevesi baz alınmış, kriter ve kontroller bu çerçevede belirlenmiştir.

Tapu ve Kadastro Genel Müdürlüğünce yürütülen bilgi sistemlerinin denetimine ilişkin açıklanan standartlara uygun şekilde bir yönetmelik hazırlanarak bilgi sistemlerinin kontrolünün sağlanması hedeflenmelidir.

BEŞİNCİ BÖLÜM

5. E-TEFTİŞ

Teftiş, teftişe tabi birimin gerek asli ve mali işlemlerinin, gerekse teşkilat yapısı ile insan ve maddi kaynaklarının, yerindelik, amaca uygunluk, hukuka uygunluk ve performans bakımından risk analizleri çerçevesinde değerlendirildiği, sorunların çözümü ve iyi yönetişimin başarılması konusunda idareye yardımcı olmayı ve rehberliği amaç edinen, insan ve sistem odaklı bir faaliyettir.

"e-Teftiş" ise, teftişin anılan fonksiyonlarından bazılarını mümkün olan en yüksek seviyede elektronik ortamda gerçekleştiren, bilişim alanındaki gelişme ve yeniliklere uyum kabiliyeti yüksek, sürekli gelişen ve dinamik bir teftiş faaliyetidir. Dolayısıyla e-teftiş, teftiş faaliyetinin, dolayısıyla da yönetimin, etkinliğini ve etkiliğini arttıracaktır. Bilişim teknolojilerindeki gelişim ve otomasyonlaşma sürecine paralel olarak zamanla "e-Teftiş"in ağırlığı artacak gözükmektedir.

e-Teftiş'in de amacı, teftiş faaliyetinde olduğu gibi; idareye yol göstermek ve rehberlik etmek yaklaşımı içinde, idareyle karşılıklı işbirliği ve koordinasyon dahilinde, otomasyon sistemi bünyesindeki birimlerin karşılaştıkları riskleri tespit etmek, değerlendirmek ve risk yönetimine katkı sağlamaktır. Bu katkı, otomasyon uygulamalarında, veri ambarlarındaki bilgilerin değerlendirilmesinde ve diğer yeni bilişim teknolojilerinin uygulamalarında gerek idareler gerek ilgililer açısından iyileştirici çözümler önerilmesi şeklinde ortaya çıkmaktadır.

Bu amaç çerçevesinde veri bankalarındaki mevcut data, önceden belirlenmiş kriterler ve risk göstergeleri doğrultusunda seçilerek alınmakta, takiben değişik bilgisayar programları yardımıyla yeniden muhtelif yöntemlerle işlenerek değerlendirilmekte ve analiz edilmektedir. e-Teftiş faaliyeti kapsamında çok büyük miktarlardaki data, çok kısa süre içinde değerlendirilerek analiz edilebilmekte ve böylece yapıcı, önleyici, caydırıcı, çözüm önerici ve otomasyon sistemlerini iyileştirici teftiş sonuçlarına ulaşılmaktadır.

e-Teftiş ile, geleneksel teftişlerde yapılabilenden çok daha fazla işlem, çok daha hızlı bir şekilde teftiş edilebilmektedir.

e-Teftişin temel özelliği,

- uzaktan,

- sürekli,
- entegre,
- risk odaklı ve
- sistemli bir şekilde

gerçekleştirilebilmesidir.[45]

Son dönemde kamu yönetimi alanında önemli reformlar gündeme gelmektedir. Bilişim teknolojileri toplumların ilişkiler ağını temelden etkilemekte, bu teknolojilerin kullanımı ile birlikte ortaya çıkan ihtiyaçlar kamu yönetiminin doğasını, örgüt yapısını, amaç ve hizmet sunumunu önemli ölçüde değiştirmektedir. Çünkü e-Devlet sadece teknoloji kullanımının öne çıktığı bir süreç değil, kamunun kurumsal kültüründe dönüşümü de içermektedir. (Parks ve Schelin, 2005:616). Günümüzde teknolojinin sosyal hayatı şekillendiren yönüne ilişkin önemli bir literatür oluşmuştur (Homburg ve Snellen, 2007:139).

Osborne ve Geaber (1993) yeniden icat edilecek kamu yönetiminde devletin takip eden değil yönlendiren, rekabete önem veren, kural odaklı değil misyon odaklı olan, girdilere göre değil sonuçlara göre fonlanan, bürokrasinin değil vatandaşların taleplerini ve ihtiyaçlarını dikkate alan, tedaviden ziyade önlemeye önem veren bir yapıda olmasını önermektedir. Bilişim teknolojileri Osborne ve Geaber tarafından önerilen yeni kamu yönetiminin inşasına önemli katkılar sunma potansiyeline sahiptir. Nitekim 1990'larda Clinton/Gore Yönetimi bilişim teknolojilerini kamu yönetiminin yeniden inşası için önemli bir araç olarak görmüşlerdir (Homburg ve Snellen, 2007:136).

Bilginin yaygınlaşması ve bilgi temelli ekonomiye doğru gidiş, vatandaşların ve iş çevrelerinin kamudan olan taleplerini ve beklentilerini artırmıştır. Bu ise kamunun bilişim teknolojilerini kullanmasını zorunlu hale getirmiş, inisiyatifler almasına neden olmuştur. (Ho:2002). Dolayısıyla e-Devlete yöneliş yukarıdan ve aşağıdan tazyiklerin etkisi ile hız kazanmıştır.

Yönetimin bir fonksiyonu olan denetim, yönetim yapılanmasından doğrudan etkilenmekte, bilişim teknolojilerinin kamu yönetimi üzerindeki etkisi denetim fonksiyonunu da dönüştürmektedir. Bu açıdan elektronik ve bilgi temelli denetim

[45] http://www.mtk.gov.tr

uygulaması ancak, elektronik devlet (e-Devlet) *(electronic government)* ve daha ileri aşamada bilgi devletinin *(information government)* varlığı ile birlikte mümkündür.

Elektronik ve bilgi devleti uygulamalarının her ikisi de çoğu kez e-Devlet olarak isimlendirilmektedir. Elektronik devlette, bilgisayar, yazılım ve network ağlarının kamu yönetiminin hizmet ve işlemlerinde yaygın bir şekilde kullanılması söz konusu iken, bilgi devletinde elektronik devlet fonksiyonlarına ilave olarak güçlü, entegre bilgi sistemleri altyapısı ile karar ve uygulamalarını bilgi temelli yürütülmesi öne çıkmaktadır.

Türkiye son yıllarda ağırlıklı olarak elektronik devlet anlamında e-Devlet alanında önemli atılımlar yapmıştır. Nüfus, vergi, gümrük, güvenlik, yargı başta olmak üzere pek çok alanda e-Devlet uygulamaları hayata geçirilmiştir. E-Devlet uygulamalarındaki gelişmeler, bu alanda e-Denetim ihtiyacını da beraberinde getirmiştir.

Bilişim teknolojilerindeki ve buna paralel olarak e-Devlet alanındaki gelişmeler denetimi çeşitli şekillerde etkilemektedir. En temel ve yaygın olan etki, klasik denetim yöntem ve tekniklerinin teknolojinin sunduğu yeni imkanlar kullanılarak yerine getirilmesidir. Burada, denetim fonksiyonunun niteliğinde önemli bir değişikliğe gidilmemekte, teknoloji denetime verimlilik, hız, güvenilirlik, tespit ve önleyicilik açılarından katkıda bulunmaktadır.

Bilişim alanındaki gelişmeler ve devlet bilgi sistemlerinin gelişmesi sonrasında denetimde bir ileri aşamaya geçilerek denetimlerin bilgi sistem altyapılarını yoğun olarak kullandığı, bilgi ve risk esaslı olarak gerçekleştirildiği, daha kapsamlı, geneli daha iyi kavrayan ve çözüm üreten yeni denetim yöntem ve teknikleri kullanılarak yapılması söz konusu olmaktadır.

Bilişim teknolojilerindeki gelişmeler, aynı zamanda yeni denetim alanlarının da ortaya çıkmasına neden olmaktadır. Bilişim sistemlerinin denetimi, bilgilerin doğruluğu, güvenliğinin sağlanması gibi hususlar özel sektöre paralel olarak kamuda da yeni denetim alanları olarak ortaya çıkmaktadır.

Böylece bilişim teknolojileri alanındaki gelişmeler denetimi kapsam ve derinlik açısından önemli ölçüde etkilemiştir. Yeni denetim alanlarının ortaya çıkması, klasik denetimlerdeki örneklem kümesinin artırılması imkanı denetimin kapsam olarak genişlemesine neden olmuştur. Aynı şekilde, daha önce uygulanması mümkün

olmayan yeni tekniklerin, çapraz kontrollerin, değişik bilgi sistemlerindeki veri tabanlarının bir arada kullanılması denetime derinlik kazandırmıştır.

İş ve işlemlerin bilişim teknolojileri kullanılarak otomasyona dayalı bir şekilde gerçekleştirilmeye başlanması, bu iş ve işlemlerin teftiş ve denetiminde de benzer şekilde değişim ve dönüşümü zorunlu kılmıştır. Böyle bir zorunluluk, bir yandan otomasyona dayalı sistemlerin bilişim teknolojileri kullanılarak teftişinin sunduğu inanılmaz fırsatları değerlendirmek, diğer yandan da bilişim teknolojilerinin yoğun kullanımının getirdiği yeni risk alanlarını tespit ederek çözüm önerileri geliştirmek ihtiyacından kaynaklanmıştır.

Yürütülen e-Devlet uygulamalarında otomasyon projelerinin birbirlerinden kopuk şekilde yapılandırılması pek çok otomasyon projesi adacıklarının (Seifert, 2007:2) oluşmasına neden olmaktadır. Türkiye'de mevcut durum birbirleriyle ilişkileri kopuk, aynı dili yeterince konuşmayan otomasyon uygulamaları şeklindedir. E-Teftiş uygulamaları ile değişik otomasyon uygulamalarının sonuçlarının bir arada değerlendirilerek bu kopukluklarının giderilmesine ön ayak olunması ve böylece devletin e-Devletten, bilgi temelli devlete doğru yol almasının önemine vurgu yapılması amacı da güdülmektedir[46].

5.1.Tapu ve Kadastro Genel Müdürlüğünce Yürütülen (TAKBİS) Tapu ve Kadastro Bilgi Sistemi Projesi

Tapu ve Kadastro Genel Müdürlüğünün tapu ve kadastro tekniği ile ilgili işlemlerini standartlaştırarak Tapu Sicil ve Kadastro Müdürlüklerinde (Şeflikler dahil) yürütülen işlemlerin mevzuata uygun bir şekilde ve bilgisayar ortamında yürütülmesini sağlayan;

· Geliştirilen uygulama yazılımlarına dahil edilen kontrol ve uyarı mekanizmaları ile memurun yaptığı işlemle ilgili riskini minimize eden veya ortadan kaldıran;

· İlgili memura ekranı üzerinden yaptığı işlemle ilgili en son mevzuat desteği sağlayan, yapılan işlemle ilgili açıklayıcı bilgi sağlayarak kendi ekranı üzerinden Bilgisayar Destekli Eğitim imkanı getiren,

[46] Arif KAPANOĞLU, Bahri SÖKMEN,Hasan AYKIN,Kayıt Dışı ekonomi ve yolsuzlukla mücadele açısından Maliye Teftiş Kurulu Elektronik Denetim Uygulaması

· Üretilen verilerin Genel Müdürlükte kurulacak sisteme akmasıyla entegre bir yapı oluşturan, mevzuat değişikliği yapılması halinde vatandaşın satış benzeri işlemleri Türkiye'nin herhangi bir yerinden yapabilmesini sağlayan;

· Müdürlüklerin ve müdürlük personelinin performansının üst hiyerarşi tarafından izlenebilmesini sağlayan,

· Memur inisiyatifini ortadan kaldırarak işlemlerin yasal mevzuata uygunluğunu, vatandaşa en kısa sürede ve doğru sonuç sağlayarak, devletle vatandaş arasında zaman içinde yıpranan güven duygusunu geliştirecek,

· Merkezde oluşan bilgileri kullanarak Bölge Müdürlükleri ve Genel Müdürlük merkez birimleri için Karar Destek fonksiyonları ve raporları üreten,

· Herhangi bir kamu kuruluşu için taşınmaz ile ilgili stratejik konularda anlık istatistiki sonuçlar üretecek,

· Milli Güvenlik açısından gereken yabancı mülkiyetindeki taşınmazlar ve yabancıların hangi yörelerde taşınmaz hareketinde bulundukları, yoğunlaştıkları hususu merkezden ve kolaylıkla izlenebilecek,

· Tarım bilgi sistemine ve Doğrudan Gelir Desteğine esas Çiftçi Kayıt Sistemine doğru ve güncel bilgi altlığı oluşturan,

· Mali suç araştırmaları ve mal varlığı sorgulamalarını tek bir merkezden yaparak, mali suçlarla ilgili sorgulamaları en kısa sürede sonuçlandırılarak, rüşvet ve yolsuzlukla mücadelede devletin etkin denetimi sağlanacak,

· ve tüm bu işlemleri Coğrafi Bilgi Sistemi/Arazi Bilgi Sistemi mantığında gerçekleştiren *entegre bir bilgi sistemi'dir.*

Türkiye genelinde Tapu ve Kadastro kayıtlarının bilgisayar ortamına aktarılarak tüm faaliyetlerin bilgisayar sistemi üzerinden yürütülmesi, böylece gerek özel, gerekse kamu taşınmaz mallarının etkin biçimde takip ve kontrolünün sağlanmasıdır.

Ülke genelinde mülkiyet bilgilerinin bilgisayar ortamına aktarılıp her türlü sorgulamanın yapılabilmesini amaçlayan en temel e-devlet projelerinden birisidir.

Tapu ve Kadastro Bilgi Sistemi ile tapu sicil ve kadastro birimlerdeki yaklaşık 650 çeşit işlem ve mevzuata uygun iş adımlarında vatandaşımıza hizmetin güvenilir, güncel ve hızlı bir şekilde hizmet sunulması mümkün olacaktır.

1990'lı yılların başında bilgisayar kullanımının yaygınlaşması ile birlikte başlatılan kurum içi otomasyon çalışmalarında geliştirilen tapu otomasyon ve kadastro

otomasyon projeleri, her ne kadar zaman içerisinde eşdeğer yazılımların ve teknolojinin gerisinde kalsa bile, bilgisayar okur-yazarlığının artırılmasında ve verilerin toplanmasında katkı sağlamışlardır.

Genel Müdürlüğümüz, bu çalışmaları takiben, mevcut verilerin hata analizlerini yaparak, gerekli düzeltici faaliyetleri başlatmak, daha gelişmiş teknoloji ve profesyonel yazılımlarla işlemleri gerçekleştirmek, ürettiği verileri diğer ilgili kurum ve kuruluşlarla paylaşmak üzere 2000 yılında TAKBİS 'i (Tapu ve Kadastro Bilgi Sistemi) projelendirmiştir.

TAKBİS üzerinden yapılan iş ve işlemlere ilişkin kayıtlar TAKBİS veri tabanında tutulmakta olup tutulan kayıtlar yardımı ile elektronik denetimin sağlanması için çalışmalar başlatılmalıdır.

5.1.1.Tapu ve Kadastro Bilgi Sistemi Üzerinden Denetim

Mevcut Tapu ve Kadastro Bilgi Sisteminde herhangi bir denetim modülü bulunmayıp, sistem üzerinden herhangi bir denetim yapılamamaktadır. Mevcut sisteme denetim modülü oluşturularak gerçekleştirilen iş ve işlemlere ilişkin verilerin kontrolü, yapılan işlemlerin mevzuat yönüyle kontrolü, personelin performans kontrolü sistem üzerinden gerçekleştirilebilecektir.

İlk olarak TAKBİS üzerinden herhangi bir denetimin yapılabilmesi için denetim kriterlerinin belirlenmesi gerekmektedir. Denetimde kullanılacak verilerin doğru, güvenilir, tutarlı, eksiksiz ve sağlıklı olması gerekmektedir. Bu anlamda sistem üzerinde bulunan verilerin tereddüte imkan vermeyecek bir şekilde oluşturulmuş olması veya tanımlanması sağlanmalıdır.

Tapu ve Kadastro Genel Müdürlüğüne bağlı Tapu ve Kadastro Müdürlüklerinin yapmış olduğu iş ve işlemlerinin denetiminin elektronik ortamda gerçekleştirilebilmesi için yapılan iş ve işlemlere ilişkin tüm bilgi ve belgelerin elektronik ortamda sağlıklı, güvenilir ve eksiksiz olarak oluşturulmuş yada tanımlanmış olması gerekmektedir. Aksi takdirde denetimin sağlıklı yapılabilmesi mümkün değildir.

e-devlet projelerinin gelişimi ve e-imza olgusunun tüm kurum ve kuruluşlarda olgunlaşması sonucunda şu anda mevcut kağıt ortamında bulunan belgelerin elektronik olarak düzenlenmesi, bu suretle belge alış verişlerinin elektronik ortamdan gerçekleştirilmesi sürecine girilecektir. Kurum ve kuruluşlar arasında paylaşım

sistemlerinin geliştirilmesi ile tüm bilgi ve belgelerin güvenli ve onaylı bir şekilde sistemde tanımlanmış olması gerçekleşecektir.

TAKBİS'in, TAKBİS verisi paylaşılmakta olan 7 adet kurum/kuruluşa ilave olarak ihtiyaç duyan tüm kurum/kuruluşların talebine cevap verebilecek bir yapıya dönüştürülmesi (web servisleri) gerekmektedir. Öncelikli olarak aşağıdaki kurum/kuruluşlar ile gerekli veri paylaşımlarının yapılması ihtiyacı bulunmaktadır.

- Bankalar
- Belediyeler
- Barolar Noterler
- Değerleme Şirketleri
- Emlak Büroları
- Tarım ve Köyişleri Bakanlığı
- LİHKAB
- YURTKUR

Diğer kurum/kuruluşların ürettiği ve TAKBİS'in ihtiyaç duyduğu "Noterlerden sahteciliği önleyebilmek amacıyla vekaletnameler", "UYAP'dan kadastroyu etkileyen mahkeme kararları" gibi verilerin de ilgili Kurum/kuruluşların sistemlerinden web servisleri aracılığıyla anlık ve güncel olarak alınmasını sağlamak üzere gerekli girişimlerde bulunulmalıdır.

Tapu ve Kadastro Müdürlüklerince doğru ve güvenilir bilgi ve belgelerin elektronik ortamda oluşturulmasından sonra TAKBİS 'de oluşturulacak denetim modülü altında yapılan iş ve işlemlere ilişkin bilgi ve belgelerin teftiş edenlerce istenilmesi halinde görülebilmesi sağlanmalıdır.

Yine gelişen teknolojilere paralel olarak bilgi sistemleri denetimlerine yönelik paket yazılımlar oluşturulmuştur. Bu yazılımlardan bazıları ACL, Excel, IDEA, Other, Access vs. dir.

Örneğin ACL yazılımı

- Veri çekme & analiz
- Yolsuzluk araştırma
- Sürekli gözetim & denetim

gibi etkin ve stratejik denetimlerde kullanılmaktadır. Paket yazılımlar aracılığı ile verilere doğrudan ulaşım, verilerin tamamına ulaşım, her tur veriye ulaşım, her formattaki veriye ulaşım, hızlı ulaşım imkanlar sağlanmaktadır.

Teftiş Kurulu Başkanlığınca Bilgi Sistemleri Denetimi ve Bilgisayar Destekli Denetim konularında hazırlıklar başlatılarak, Başkanlık bünyesinde bulunan Müfettişlere bu yönde eğitim ve sertifikaların kazandırılması sağlanmalıdır.

5.2. E-Teftiş Uygulamasının Temel Özellikleri

Teftiş; teftişe tabi birimin gerek asli ve mali işlemlerinin, gerekse teşkilat yapısı ile insan ve maddi kaynaklarının, yerindelik, amaca uygunluk, hukuka uygunluk ve performans bakımından risk analizleri çerçevesinde değerlendirildiği, sorunların çözümü ve iyi yönetişimin başarılması konusunda idareye yardımcı olmayı ve rehberliği amaç edinen, insan ve sistem odaklı bir faaliyet olarak tanımlanmaktadır.

"E-Teftiş" ise teftişin fonksiyonlarından bazılarının mümkün olan en yüksek seviyede bilişim teknolojisinin sunduğu imkanlar kullanılarak ve bilgi temelli olarak gerçekleştirildiği gelişme ve yeniliklere açık dinamik bir teftiş sürecini ifade etmektedir.

e-Teftiş uygulamaları ile birlikte teftişin temel karakteristiklerinde önemli dönüşümler meydana gelmiştir. Bunlar ana başlıkları ile aşağıdaki gibi sıralanabilir:

5.2.1. Teftişte Kapsam Genişlemesi

Klasik teftişlerde, teknolojik ve zaman kısıtları nedeniyle ilgili idarenin işlem, dosya ve/veya ilgililerin belli kısmının incelenmesi mümkün olmakta iken e-Teftiş imkanları ile önceden hazırlanan parametreler kullanılarak ilgili müdürlüğün tüm işlem, dosya ve/veya ilgilileri, konular ve sorgular itibariyle denetlenebilmesi mümkün olabilmektedir. Bu teftişin incelenen işlem açısından kapsamını maksimum düzeye çıkarması anlamına gelmektedir.

5.2.2. Teftişte Derinlik

Teftişlerde sadece dairedeki veri ve dosyalar kullanılmak yerine farklı kurum ve kuruluşlardaki bilgi sistemleri ve veriler kullanılmak suretiyle çapraz kontroller mümkün hale gelmiştir. Böylece teftişte dikkate alınan parametreler, veriler artmış ve teftişte daha fazla derinlik sağlanmıştır. Aşağıda yer alan uygulama teftişin derinliğinin artışını göstermek açısından bir örnek olarak sunulabilir:

Bilindiği üzere yeşil kart kullanımı tüm ülke çapına yayılmış önemli sosyal yardım müesseselerinden birini oluşturmaktadır. Gerçek hak sahibi olmayanların bu haktan

yararlanmasının önüne geçilmesi büyük önem taşımaktadır. Tüm kontrollere rağmen hak sahibi olmayanların sistemi kullanmasının ve usulsüzlüklerin önüne tam olarak geçilememiştir. Bu sorunla mücadele amacıyla e-Teftiş çalışmaları kapsamında iller bazında sırayla yeşil karttan yararlananların durumu tek tek çapraz kontrole tabi tutulabilmektedir. Sağlık Bakanlığı Bilgi İşlem Merkezi, Tapu, Sosyal Güvenlik Kurumu, GİB-BİM verileri bir havuzda değerlendirmeye tabi tutularak çapraz olarak karşılaştırılmakta ve kolaylıkla hak sahibi olmayan kişiler tespit edilmektedir. Yapılan tespitlerde çok sayıda evi, arabası olan, hatta şirket ortağı bulunanların haksız yere yeşil kart kullandıkları tespit edilmiştir. Bu tespitler neticesinde sosyal boyutlu bir sistemin kötüye kullanılması kamudaki değişik veriler bir arada değerlendirilmek suretiyle engellenmekte, kötüye kullanımların neden olduğu Hazine zararı ilgililerden cezası ile birlikte takip edilebilir hale gelmektedir.

Bu tür kontroller Devlet tarafından yapılan diğer benzeri sosyal ödeme ve yardımları da kapsayacak şekilde genişletilmektedir. 2010 yıl itibariyle yeşil kart kontrol yapılan il sayısı yirmiyi aşmıştır. Önümüzdeki yıllarda bu tür kontrollerin tek seferde tüm Türkiye'yi kapsayacak şekilde yapılması yoluna gidilmesi planlanmaktadır.

5.2.3. Teftişte Risk Odaklılık

Teftiş sırasında tüm işlemlerin belli parametre ve sorgular kullanılarak incelenmesi hata, kayıt dışı ve yolsuzluk riski yüksek işlemlerin belirlenmesine ve teftişte risk düzeyi yüksek bu unsurlar üzerinde yoğunlaşılmasına daha fazla imkan tanımaktadır. Bu ise e-Teftişlerin risk esaslı bir yaklaşımla *(risk based approach)* gerçekleştirilmesi anlamına gelmektedir.

5.2.4. Teftişte Objektiflik

Daha önce rassal olarak seçilen dosyalar üzerinden yapılan teftişlerde, sadece seçilen dosyalarda ortaya çıkması muhtemel hata, usulsüzlük ve yolsuzlukların incelenmesi söz konusu olduğundan çok daha riskli olan ve öncelikli olarak incelenmesi gereken işlem ve kişilere ilişkin işlem yapılamama ihtimali bulunmakta keza dosya seçme yöntemi teknik imkansızlıkların da etkisi ile bazen sübjektif unsurları bünyesinde barındırabilmekte idi. Oysa bilişim teknolojilerinin sunduğu imkanlarla e-Teftişlerde objektif kriterlere göre oluşturulan risk parametreleri esas alınarak yüksek riskli

işlem ve kişilere öncelik verilebilmekte, böylece teftişte daha yüksek oranda objektiflik sağlanmaktadır.

5.2.5. Önleyicilik Fonksiyonu

Teftiş sırasında sistematik hatalara ve yolsuzluk riski bulunan alanlara ilişkin olarak getirilen öneriler üzerine bilgi sistemlerine entegre edilen uygun kontrol modülleri sayesinde hata ve yolsuzlukların önlenmesi mümkün hale gelmektedir. Böylece hata ve yolsuzlukların gerçekleşmesinden sonra tespitinden daha öncelikli olarak bu tip hata ve yolsuzlukların gerçekleşmelerinden önce önlenmesi fonksiyonu üzerinde durulmaktadır.

5.2.6. Çözüm Odaklılık

Teftişlerin kapsamının genişlemesine paralel bir şekilde, tespit edilen hata ve yolsuzlukların yaygınlığı, nedenleri üzerinde veriye dayanan daha kapsamlı, net analizler yapılabilmekte ve hata ve yolsuzlukların önlenmesine yönelik çözümler geliştirilebilinmektedir. Teftişte tek tek hata ve yolsuzlukların tespitinden ziyade genel nitelikli sorunların ve yolsuzluk alanlarının tespiti ve bunlara ilişkin idareye çözüm önerisinde bulunma konusuna daha yüksek oranda ağırlık verilmektedir. İdareye sorunları ve sorumluları bildirmekten ziyade çözümler öneren bir teftiş yaklaşımına geçilmektedir.

5.2.7. Teftişte Mekansal Sınırın Önemini Kaybetmesi

Teftişlerde en çok zaman ve emek harcanan, teftişin maliyetini artıran unsur teftişin her durumda mahallinde yapılması gerekliliği idi. Ancak bilişim teknolojilerinin sağladığı imkanlar sayesinde kurumun her bir biriminin yaptığı işlemler on-line olarak merkezden izlenebilmekte, merkezden ilgili birimlerin işlemleri toplu olarak analize tabi tutulabilmekte ve birimler performans ve risk açısından kategorize edilebilmektedir. Mahallinde yapılacak teftişler daha çok, önemli hata ve yolsuzluk riski tespit edilen birimlerde söz konusu olmaktadır.

Bazı işlemlere ilişkin hazırlanan sorgular Türkiye'deki tüm işlemler için aynı anda uygulanmaktadır. İzleyen yıllarda belki AB mevzuatı veya diğer uluslararası anlaşmalar çerçevesinde bir çok ülke kendi vatandaşlarının bazı bilgilerini – karşılıklılık ilkesi çerçevesinde- diğer ülke kurumları ve denetim birimleri ile

paylaşacak ve onlar tarafından da sorgulanabilmesi gündeme gelecektir. TKGM tarafından başlatılacak e-Teftiş çalışmaları ileride diğer ülkelerdeki verileri de kullanacak şekilde genişleyebilecektir. Sonuç itibariyle giderek devasa bir network halini alan dünya taşınmaz bilgi sistemleri ve teftiş sistemlerinin gelecekteki yeni yapılanmalara da hazırlıklı olması gerekmektedir.

5.2.8. Bütüncüllük

E-teftiş uygulamaları ile birlikte tek tek dosyalar yerine işlemlerin tümü incelenebilmekte, işlem, dosya veya kişilerin ilgili olduğu diğer unsurlar bir bütün olarak değerlendirmeye tabi tutulabilmektedir. Böylece, işlem, dosya veya kişilerin durumları bütün şeklinde kavranmaya çalışılmaktadır.

5.2.9. İşlem Teftişinden Sistem Teftişine Geçiş

İşlem denetiminden sistem denetimine geçiş, diğer bir deyişle sistematik hatalara yöneliş e-Teftişin başlıca unsurlarından biridir. Böylece geçmişe yönelik sorgulamalardan reel zamanlı sorgulamalara geçiş amaçlanmakta, diğer taraftan basit çapraz kontrollerden çok daha büyük boyutlu, sistematik ve organize şekilde gerçekleşen unsurların tespiti ve önlenmesine yönelinmektedir. Klasik teftiş uygulamaları ile tespiti son derece güç olan ve sistematik risk içeren alanların tespitine yönelim e-Teftişin temel amaçlardan birini oluşturmaktadır.

5.2.10. Uygunluk Denetim yanında Yerindeliğe İlişkin Sonuçlara da Ulaşma

Klasik teftişlerde esas olan, yapılan iş ve işlemlerin ilgili mevzuat hükümlerine uygun olarak yapılıp yapılmadığının ortaya konulmasıdır. Bu husus son derece önemli olmakla birlikte, e-Teftiş imkanları ile birlikte yapılan analiz çalışmaları sonucu, mevzuata uygunluk yanında işlemlerin yerindeliğine yönelik de önemli bulgulara ulaşılmakta ve bu konuda birimler uyarılabilecektir.

5.2.11. Yolsuzlukların Tespiti ve Önlenmesi

E-Teftiş çalışmalarında, aynı otomasyon sistemindeki farklı verilerin birbirleriyle ve farklı otomasyon sistemlerindeki veri ve bilgilerle çapraz kontrolleri sonucunda önemli yolsuzlukların tespiti mümkün hale gelecektir. Tespit edilen yolsuzluklardan hareketle önleme stratejileri otomasyon sistemleri içine monte edilmelidir.

5.2.12. Sürekli Teftiş

Klasik teftişlerde personel kısıtları ve mekansal ulaşım imkanları nedeniyle dairelerin belli periyotlarla teftişi söz konusu olmakta hatta bazen bu periyotlar çok uzamakta ve daireler uzun yıllar hiç teftiş edilmemekte idi. E-Teftiş ile birlikte, işlemlerin sürekli olarak izlenmesi ve kontrolü mümkün hale gelecektir. Turneye dayalı, belli zamanlarda yapılan teftişten sürekli teftiş konseptine geçiş söz konusu olabilecektir.

5.3. E-Teftiş Uygulamaları İle Beklenilen Önemli Sonuçlar

- Teknolojideki gelişmeler, hayatın her alanını etkilemektedir. Kamu yönetiminin doğası, kültürü, hizmet sunma yöntem ve teknikleri teknolojik gelişmelerle yeniden şekillenmektedir.
- Denetim, yönetimin önemli bir fonksiyonudur. Ondan ayrı düşünülemez. Bu kapsamda başta bilişim teknolojileri olmak üzere teknolojik gelişmeler kamu yönetimini ve buna paralel olarak denetim fonksiyonunu temelden etkilemektedir.
- E-Teftiş uygulamaları ile birlikte denetimin kapsam ve derinliğinde artış meydana gelebilecek, daha hızlı, uzaktan, risk odaklı, objektif kriterlerle yürütülen, önleyicilik ve çözüm odaklılığı daha ön planda tutan, bütüncül, işlem teftişi yerine sistem teftişini benimseyen, yolsuzluk ve kayıt dışı ile mücadeleye önemli katkılar veren bir teftiş söz konusu olacaktır.
- E-Devlete geçişte, işlemlerin gerçekleştirilmesi ve hizmet sunulmasında yoğun teknoloji kullanımı söz konusu olmaktadır. Ancak, zamanla bir ileri aşamaya geçilerek bilgi sistemlerinin politika oluşturma ve uygulamada bilgi temelli yönetim anlayışı ile daha entegre ve etkin bir şekilde kullanılması gerekmektedir.
- E-Devlet uygulamalarının ilk aşamasında, kamuda birbirlerinden kopuk şekilde çalışan "*otomasyon adacıkları"* oluşturulmaktadır. Daha ileri aşamaya geçmek için otomasyon adacıklarının birbirleriyle bağlantılarının kurulması, entegre hale getirilmesi önem taşımaktadır. Buna paralel olarak e-Teftiş uygulamalarının da entegre yapıda sunulması önem taşımaktadır. Bu kapsamda, otomasyon projelerinde pek dikkate alınmayan denetim modüllerinin oluşturulması ve geliştirilmesinde teftiş birimlerinin birikimlerinden yararlanılması önem arz etmektedir.
- Teftiş Kurulu Başkanlığınca oluşturulacak komisyon ile TAKBİS aracılığı ile denetimin ilk adımları atılmalı, TAKBİS te bir denetim modülü oluşturularak tüm müfettişlerce bu modülün işletilmesini sağlayacak eğitimler hazırlanmalıdır.

- Teftişlerin teknolojinin sunduğu imkanlar kullanılarak yapılmasının yanında, otomasyon sistemlerindeki verilerin kendi içinde ve diğer sistemlerdeki verilerle birlikte bütüncül olarak değerlendirilmesi şeklinde bir yaklaşım benimsenmeli, böyle bir yaklaşımın kayıt dışı ekonomi ve yolsuzlukla mücadele açısından önemli sonuçlar ortaya çıkaracağı da açıktır. Bu sonuçlar aynı zamanda, Türkiye'de otomasyon sistemlerinin birbirleriyle konuşur ve birbirlerine entegre hale getirilmesinin ne kadar önem arz ettiğini göstermiştir. Çünkü, kamuda bilgi sistemlerinin birbirleriyle konuşabilir yapıda olmaması, kayıt dışı ve yolsuzluk açısından büyük risk oluşturmakta, etkin bir yönetim ve denetim fonksiyonunun gerçekleştirilmesini güçleştirmektedir.
- E-Teftiş uygulamaları sırasında, etkin bir yönetim ve denetim uygulaması açısından otomasyon sistemlerindeki verilerin doğru ve zamanında kaydedilmesi büyük önem taşıyacaktır. Uygulamada veri girişlerinde önemli hata ve eksikliklerin bulunduğu, verilerin zamanında sisteme girilmesinde gecikmelerin yaşandığı gözlemlenmektedir.
- Sahtecilik ve yolsuzluk başta olmak üzere pek çok suçla mücadele açısından kamuda etkin bir veri paylaşım sisteminin oluşturulması önem taşımaktadır.
- Önümüzdeki dönemde, teknolojideki değişim hızlanarak devam edecektir. Küreselleşme ve uluslararası rekabet şartlarında kamu yönetiminin örgütsel kapasitesi ülkenin rekabet gücünü daha fazla etkileyecektir. Bunun için hızlı bir şekilde bilgi temelli, öncü, sonuç odaklı, rekabeti teşvik eden bir yapıya kavuşmuş bir kamu yönetimine ihtiyaç bulunmaktadır. Böyle bir kamu yönetiminde denetim fonksiyonunun, bütünleşik, hızlı, yönetimin kararlarının oluşturulmasına katkı sunan bir yapıya kavuşması önem taşımaktadır.
- Önümüzdeki dönemde, veri ambarlarından daha fazla yararlanılması, veri madenciliği üzerinde önemle durulması gerekmektedir.
- Bilgi güvenliği ve kişisel verilerin korunması hususunda her türlü önlemin alınması önem taşımaktadır.
- Uluslararası alanda e-Devlet ve e-Teftiş alanındaki gelişmelerin, trendlerin yakından takip edilmesi ve iyi örneklerin sisteme adapte edilmesi önem taşımaktadır.
- E-Teftiş modelinin tüm kamu kurumlarında, çalışma alanlarıyla uyumlu şekilde uygulanabilmesi için, ilgili kurumlarla işbirliği gerekmektedir.

- E-Teftiş uygulamalarının organizasyon yapılarında, teknik ve hukuki altyapıların değişimini gerektirdiği unutulmamalıdır. İnsan kaynağının ise ömür boyu eğitim yaklaşımı ile sürekli eğitilmesi, çalışanların bireysel kapasitelerinin, analitik düşünme becerilerinin geliştirilmesine gereken önem verilmelidir.

KAYNAKÇA

Kitaplar

Bozkurt, Nejat. **Muhasebe Denetimi**. 3. Baskı (İstanbul: Alfa Basım Yayım, 2000)

Devlin, Edward S. Cole H. Emerson ve diğerleri. **Business Resumption Planning** (USA: AUERBACH, 2000)

Duman, Ömer. **SM, SMMM, ve YMM Sınavları için Muhasebe Denetimi ve Raporlama**. 2. baskı (Ankara: Siyasal Kitabevi, 2008)

Erdoğan, Melih. **Denetim Kavramsal ve Teknolojik Yapı.** 3. baskı (Ankara: Maliye ve Hukuk Yayınları, 2006)

ISACA. **IT Assurance Guide** (USA: 2007)

ISACA. **Control Objectives for Information and related Technology 4.1** (USA, 2007)

ISACA. **Control Objectives for Information and related Technology 4.0** (USA, 2005)

Johnson, Everett C. Robert D. Johnson. **CISA Review Manual 2007.** (USA: ISACA, 2007)

Kepekçi, Celal. **Bağımsız Denetim**. 5. baskı (İstanbul: AVCIOL Basım Yayın, 2007)

Porter, Brenda, Jon Simon, David Hatherly. **Principles of External Auditing** (USA: John Wiley & Sons, 1996)

Rosenblatt, Shelly Cashman. **System Analysis and Design.** 5. Edition (USA: Thomson Learning, 2002)

Saka, Tamer. **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi.** Yayın:224 (İstanbul: Türkiye Bankalar Birliği, 2001)

Sommerville, Ian. **Software Engineering**. 6. Edition (England: Pearson Educated Limited, 2001)

Bilişim Teknolojilerinde Kalite Yönetimi, Ahmet Pekel, Türkiye Cumhuriyet Merkez Bankası Lira Dergisi, Ocak 2007 tarihli, 41. sayı.

Enterprise Value: Governance of IT Investments, The Val IT Framework, http://itgovernance.pbwiki.com/ValIT, 23.12.2007.

ISACA-Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri Klavuzu-Çevirmen Ömer YURDAGÜL, 2010.

Makaleler-Tezler-Çalışmalar

Mustafa Cem Akocak, Bilgi Teknolojileri Denetiminin Esasları ve Türk Bankacılık Sektöründeki Uygulamaları (Yüksek Lisans Tezi.2009)

Bağcı, Barış. **Bilgi Teknolojileri Risk Yönetimine Genel Bakış**. (İstanbul: Deloitte Touche Tohmatsu, 2007)

Bakman, Alex. "If Compliance is so critical , Why are we still failing audits?", **Information Systems Control Journal**, volume 5 (2007): s. 37

Gallegos, Frederick. **Information Technology Control and Audit**.(USA: Auerbach Publications, 2004)

Lawton, Robert. "Transitioning IT From a Compliance to a Value-driven Enterprise Using CobiT", **Information Systems Control Journal**, volume 6 (2007): s.43

Pironti, John P. "Key Elements of an Information Risk Management Program", **Information Systems Control Journal**, volume 2 (2008): s. 43

Ross, Steven J. "Reliable Security", **Information Systems Control Journal**, volume 5 (2008): s. 9

Swaroop, Shankar. "Managing Multiple Medium and Small Scale Projects in Large IT Organization", **Information Systems Control Journal**, volume 4 (2007): s. 24

Türkiye İç Denetim Enstitüsü. **Uluslararası İç Denetim Standartları ve Mesleki Uygulama Çerçevesi.** (İstanbul: Print Center, 2008)

Arif KAPANOĞLU, Bahri SÖKMEN,Hasan AYKIN,Kayıt Dışı ekonomi ve yolsuzlukla mücadele açısından Maliye Teftiş Kurulu Elektronik Denetim Uygulaması

Diğer Yayınlar

AICPA. **Audit Standards**. www.aicpa.org [03.03.2009]

BDDK. "**Bilgi Sistemleri Denetim Yetkisi Verilen Kuruluşlar**". www.bddk.org.tr [28.03.2009]

BDDK. "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**"(Sayı 26643; Tarih 14 Eylül 2007)

BDDK. "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Sayı 26170; Tarih: 16 Mayıs 2006)

BDDK. "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğine**" (Sayı 26367; Tarih: 5 Aralık 2006)
BDDK. "**Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik**" (Sayı 26333; Tarih: 1 Kasım 2006)

ISACA. **IT Continuity Planning Audit/Assurance Program**. www.isaca.org [01.03.2009]

ISACA. **IT Audit Standards**. [03.03.2009]

KPMG. **IDEA Training Course Documents.** (İstanbul: KPMG Turkey, 2005)

KPMG. **CobiT Olgunluk Seviyesi Değerlendirme Aracı El Kitabı.** (İstanbul: KPMG Turkey, 2005)

KPMG. **KPMG's 2009 IT Internal Audit Survey**. (Turkey: KPMG, 2009)

KPMG. **KPMG IT Audit Methodology (KAM)**. www.kworld.com [23.03.2009]

Microsoft. **MSAT Tool**. http://technet.microsoft.com/tr-tr/security/cc185712(en-us).aspx[15.04.2009]

Önal, Mehmet Zeki. "**An Aggregated Information Technology Checklist for Operational Risk Management**". Yüksek Lisans Tezi. Boğaziçi Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

SPK, "**Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ"** (Seri: X, No:22)

TUBİTAK UEKAE. **Yedekleme ve İş Sürekliliği Kontrol Listesi**. (Ankara: TUBİTAK, 2007)

COBİT, Vildan UZUNAY İç Kontrol Merkezi Uyumlaştırma Dairesi, 2007
www.isaca.org,www.ITgovernance.org,www.sox-online.com, www.theiia.org/itaudit
www.kpmg.com,www.isaca.org/ COBIT Security Baseline

A.Pekel, Ü.Zaim, T.Cumurcu, D.Peker-TBD-BİB Kamu Bilişim Platformu-X, Bilişim Teknolojilerinde Yönetişim, 1. Çalışma Gurubu, Sürüm 1.3, Nisan 2008

Bilgi Grubu, E.Demirörs, CMMI : Temel Kavramlar Kurs Notları, www.bg.com.tr, 2/5/2006

ISO 9126, http://en.wikipedia.org/wiki/ISO_9126, 4.4.2011

PWC Çözüm Ortaklığı Platformu, şirketlerde İç Kontrol ve İç Denetim Fonksiyonu, PWC, http://www.pwc.com, 22.12.2007.

KAS Certification International, http://www.kascert.com, 2011

TSE, http://www.tse.org.tr, 23.12.2011.

Evrim Numanoğlu, BSI Eurasia, http://www.kalder.org, 23.12.2007,

Türkiye, http://www.bsi-turkey.com, 23.12.2007

ISO 27001, http://www.iso27001certificates.com