BDDK TEBLİĞİ ÇERÇEVESİNDE "BİLGİ SİSTEMLERİ DENETİMİ" KAVRAMININ İRDELENMESİ VE GÜNCEL GELİŞMELER

Dr. Deniz Umut ERHAN *

ÖZET

Bankacılık Düzenleme ve Denetleme Kurumu tarafından, 14.10.2007 tarihli ve 26643 sayılı Resmi Gazete'de "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" yayınlanmıştır. Yayınlanan tebliğ ile 5411 sayılı Bankacılık Kanunu'nun 93 üncü maddesi ve Bankaların İç Sistemleri Hakkındaki Yönetmeliğin 11 inci maddesinin beşinci fıkrası ile 16 ncı maddesinin üçüncü fıkrasınca tanımlanan yükümlülük yerine getirilmiştir. Tebliğ, bankacılık ve finans sektörüne özel olarak düzenlenmiş olmakla birlikte diğer sektörlerde de uygulanabilir bir nitelik taşımaktadır. Söz konusu Tebliğ'e bağlı olarak yayınlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" ile birlikte ülkemizde "Bilgi Sistemleri Denetimi" kavramı sağlam bir temele yerleştirilmiştir. Bu çalışmada öncelikle bu tebliğ ve yönetmeliğin denetime esas olan ilkeleri ele alınmıştır. Tebliğ'in bilimsel altyapısını oluşturulan, Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) ve Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından geliştirilmiş "Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (CobIT)" dokümanının 2007 tarihli son 4.1 sürümü ile Uluslararası Standartlar Örgütü (ISO) tarafından 2008 yılı içinde yayınlanan ISO/IEC 38500 "Bilgi Teknolojilerinin Kurumsal Yönetimi" standardıyla gündeme gelen güncel gelişmeler ele alınmıştır.

Anahtar Sözcükler: Bilgi Sistemleri Denetimi, Kurumsal Yönetim, CobIT, Kontrol Hedefleri

ABSTRACT

SURVEY OF "IT SYSTEMS AUDIT" CONCEPT FROM BRSA REGULATION PERSPECTIVE AND RECENT DEVELOPMENTS

"Regulation on Principles of Information Systems Management to be made in Banks" was published in the Official Gazette dated 14/10/2007 Nr. 26643 by Banking Regulation and Supervision Agency (BDDK). By release of the Regulation, BDDK fulfilled the legal provisions defined at Article 93 of Banking Law dated October 19, 2005 Nr. 5411 together with Article 11(5) and Article 16(3) of "Regulation on Banks' Internal Control and Risk Management Systems". Although particularly targeted for banking and finance sectors, Regulation's content and approach with its cognizant character towards globally accepted and widely practiced methodologies and management frameworks, exhibits a proficient baseline which could be also conveinent to others. Besides this Regulation, and after the release of "Regulation on Information Systems Audit to be made in Banks by Independent Audit Institutions", it is regarded that Information Systems Audit concepts were placed on firm foundations. In this study, initially the approach of Regulation on basis of audit principles were detailly commented. Afterwards, the recent advancements at IT systems audit area was reviewed based on the publications of International Standards Organization ISO/IEC 38500 "Corporate Governance of Infromation Systems" dated June, 2008 and version 4.1 of CobIT "Control Objectives for Information and related Technology" guideline dated 2007 which also accepted as the scientific backbone of the Regulation. Resultingly, new dimensions added to corporate governance concept which unseperably dependent on reliable information technologies and also remarks on probable difficulties that may be confronted at the practice were discussed.

Keywords: Information Technology Audit, Corporate Governance, CobIT, Control Objectives

* Başkent Üniversitesi, Ticari Bilimler Fakültesi Muhasebe ve Finansal Yönetim Bölümü e-posta : duerhan@baskent.edu.tr

1. GİRİŞ

Francis Fukuyama'nın "*Güven: Sosyal Erdemler ve Refahın Yaratılması*" başlıklı yapıtında güven, bireylerin ve kurumların aralarındaki ilişkilerde canlılık oluşturan; taahhütlerini yerine getirme, içtenlik, gerçeklik, dürüstlük ve erdemi kapsayan *bilinçli tutarlılık* olarak tanımlanmaktadır.[1] Bireysel yaşantının, toplumsal düzenin ve ekonomik gelişmelerin temelini oluşturan güven duygusunun ortaklaşa paylaşılan normlara dayalı, dürüst ve işbirliği kurmaya istekli üyelerin oluşturduğu bir toplulukta ortaya çıkması beklenmektedir. Güven duygusunun temeli olan normlar etik ve adalet gibi derin değerler üstüne kurulabileceği gibi çalışma hayatında da güven davranış kodlarına dayalı gönüllülükle benimsenmiş standartlara karşılık gelmektedir. Normların kaynağı ne olursa olsun bireyler ve örgütler kesintisiz işbirliği ve dürüst davranış beklentisini sağlayacak biçimde normları paylaştıkça güven duyguları yükselebilecektir.

Gönüllülükle paylaşılan normlardan doğan kurallar kurumlarla, ilgili taraflar arasındaki etkileşimlerde belirsizliği azaltarak öngörülebilirlik ve istikrarı sağlayan, ortak çıkarların korunması adına saydamlığı ve hesap verebilirliği güvence altına alan, denetim olgusunun değerini yükselten, ölçülemeyen, öznel ve örtülü risklere yönelik sınırlamalar getirebildiği oranda girişim serbestîsini güçlendiren yapılardır. Kurallar ve kurumların bu özelliği, geleneksel yönetim yaklaşımlarının kısıt ve zayıflıklarının aşılmasında güçlü bir araç olan kurumsal yönetim (corporate governance) olgusunun da temel dayanağıdır. Toplumsal düzende olduğu gibi, iş yaşamında da önemli olan kuralların uygulanmasında karar verme yetkisini elinde tutan kişilerin varlığı değil, normlardan türemiş kural ve kurumların dürüstlük ve açıklığının güvencesi olarak algılanıp, zorlama olmadan işletilmesidir.

Kurumsal yönetim kavramının *modern yaşamda insanların bir amaca ulaşmak için oluşturduğu herhangi bir kurumun yönetiminin düzenlenmesi* biçimindeki tanımı bu anlamda tutarlı tanımlamadır. Kavramın, *bir kurumun beşeri ve mali sermayeyi çekmesine, etkin çalışmasına ve böylece ait olduğu toplumun değerlerine saygı gösterirken uzun dönemde ortaklarına ekonomik değer yaratmasına olanak sağlayan her türlü kanun, yönetmelik, kod ve uygulamalar*[2] biçimdeki daha dar anlamdaki ifadesi de normların üstünlüğüne atıf yapan bir tanımlamadır.

İnsanlara refah getirecek politik hedeflerin yakalanmasında makro ekonomi ile yapısal politikalar arasındaki sinerjiyi hissetmekte olan Türkiye gibi ülkelerde, kurumsal yönetim, ekonomik verimliliği ve büyümeyi artırmanın aynı zamanda yatırımcı güveninin kazanılmasının anahtar unsurlarından birisidir. Kurumsal yönetim şirketin hedeflerinin belirlendiği bir yapıyı ortaya koymakta ve bu hedeflere nasıl ulaşılacağının ve performansın nasıl denetleneceğinin yollarını çizmektedir. Kurumsal yönetim ilkelerinin doğru bir şekilde kurgulanmış olması, üst yönetim için şirket çıkarları doğrultusunda hedeflere yönelme açısından uygun teşvikleri sağlamakta ve etkin denetimi kolaylaştırmaktadır. Etkili kurumsal yönetimin şirketler bazında ve ekonominin genelinde var olmasıyla, piyasa ekonomisinin işleyebilmesi için gerekli olan güvenin sağlanabileceği düşünülmektedir.

Geniş bir ekonomik çeşitliliğin odağında yer alan kurumsal yönetimin çerçevesi, yasal, düzenleyici ve kurumsal etkenlerin varlığına ve et-

1 Francis FUKUYAMA, *Güven: Sosyal Erdemler ve Refahın Yaratılması*, Çev: Ahmet Buğdaycı, Türkiye İş Bankası Yayınları, Ankara, 1998, 37

2 TÜSİAD *Kurumsal Yönetim En İyi Uygulama Kodu: Yönetim Kurulunun Yapısı ve İşleyişi* İstanbul 2002, 9

kinliğine dayanmaktadır. Kurumsal yönetimin özünü ifade eden ortak normların kamu çıkarı adına yasal zeminde tanımlanması, normlara bağlılık ve uyumluluğun kamu çıkarı adına izlenmesi, normlarda kurumsallaşmanın özendirilmesi, en iyi uygulamaların yaygınlaştırılması, kuralı çiğneyen uygulamaların kamu çıkarını zarara uğratmadan belirlenmesi ve önlenmesi, toplum için temiz ve güvenilir bir ortamın yaratılması ve korunması gereksinimlerini sağlamak amacıyla tarafsız ve bağımsız kurumların görevlendirilmesi gereğini doğurmaktadır.

BDDK tarafından yayınlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" gerek kurumsal yönetim kültürüne getirdiği katkı gerekse ortaya koyduğu kurumsal yönetim kültürünün yaşatılmasında büyük etkisi bulunan bilgi sistemlerinin yönetim normları ile sağlam bir çıkış noktası oluşturmaktadır. Tebliğ'in rehber olarak benimsediği Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) ve Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından geliştirilmiş "Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (CobIT)" dokümanının ilkelerinin gözden geçirilmesi, şirketler için kurumsal yönetim kültürünün yerleştirilmesi adına akılcı ve yapılabilir çözümleri kolaylaştıracaktır. Bu çalışmada kurumsal yönetim kavramının ayrılmaz bir parçası ve kaldıracı olarak gördüğümüz bilgi sistemleri denetimi alanında son iki yıl içinde yaşanan güncel gelişmeler de açıklanarak, bilgi sistemleri denetimi konusundaki uygulamada gözlenen kavramsal karışıklıkları yalınlaştırarak şirketlere yol gösterici bazı saptamalara ulaşılmaya çalışılmıştır.

2. BDDK TEBLİĞİ

2.1. Tebliğin Yasal Dayanakları

BDDK tarafından yayınlanan, "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" yasal dayanaklarını 5411 sayılı "Bankacılık Kanunu"nun iç sistemlere dair yükümlülüklerin yer aldığı ikinci bölümündeki 29 uncu ve 30 uncu maddelerinden almaktadır. Bu maddelere göre bankalar "*maruz kaldıkları risklerin izlenmesi, kontrolün sağlanması, faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara uygun, tüm şube ve konsolidasyona tâbi ortaklıklarını kapsayan yeterli ve etkin bir iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle*" yükümlü kılınmışlardır. Kanun, kurulacak iç kontrol sistemi kapsamında, *"faaliyetlerin mevzuata, iç düzenlemelere ve bankacılık teamüllerine uygun olarak yürütülmesini, finansal raporlama sisteminin bütünlüğünü, güvenilirliğini ve bilgilerin zamanında elde edilebilirliğini her düzeydeki personel tarafından uyulacak ve uygulanacak sürekli kontrol faaliyetleri ile sağlamak, görevlerin fonksiyonel ayrımlarını, yetki ve sorumlulukların paylaşımını, fon ödemelerini, banka işlemlerinin mutabakatını, varlıkların korunmasını ve yükümlülüklerin kontrol altında tutulmasını temin etmek, maruz kalınan her türlü riskin tanınması, değerlendirilmesi ve yönetimi için gerekli alt yapıyı hazırlamak ve yeterli iletişim ağını oluşturmak"* konularındaki zorunluluklar belirtilmiştir.

Kurumsal yönetim bakımından kanun maddeleri sistemin bütünlüğü, güvenilirliği ve zamanlılığına vurgu yapmakta, sürekli kontrol etkinliği ve görevler ayrılığı ilkesini gündeme getirmektedir. Kanunla, bu ilkeler ışığında bankacılık faaliyetleri, varlıkların korunması ve yükümlülüklerin denetimini sağlamakla ilişkilendirilerek bu ilkelerin yetersiz olmaları halinde kendi başlarına risk kaynağı olabileceği bilinci oluşturulmaya çalışılmıştır. Diğer taraftan gerekli alt yapının kurulması ve yeterli iletişim ağının oluşturmasıyla risklerin önemli ölçüde denetim altına alınabileceği sonucuna gönderme yapılmaktadır. Kanun somut kanıtlar sunacak bir altyapının kurulması halinde üst yönetime bağlı iç kontrolden sorumlu birimlerin *teftiş* etkinliğini geleneksel

kalıplardan çıkararak, risk yönetimi felsefesinin uygulanmasına yönelik bir bakış açısı getirmektedir.

BDDK'nın, 5411 sayılı Bankacılık Kanunu'nun ilgili maddelerinin uygulanması amacıyla yayınladığı "Bankaların İç Sistemleri Hakkındaki Yönetmelik" ile bankaların kuracakları iç kontrol, iç denetim ve risk yönetim sistemlerine ve bunların işleyişine ilişkin usul ve esaslar düzenlenmiştir. Yönetmeliğin 9 uncu maddesinde iç kontrol sisteminin amacı "*bankanın varlıklarının korunmasını, faaliyetlerin etkin ve verimli bir şekilde Kanuna ve ilgili diğer mevzuatlara, banka içi politika ve kurallara ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve finansal raporlama sisteminin güvenilirliğini, bütünlüğünü ve bilgilerin zamanında elde edilebilirliğini sağlamaktır.*" ifadesine yer verilerek iç kontrol sistemini muhasebe sisteminden sorumlu kılmıştır. İç kontrol sisteminden beklenen amacın sağlanabilmesi için[3];

- Banka bünyesinde işlevsel görev ayrımının yapılması ve sorumlulukların paylaştırılması,
- Muhasebe sisteminin, bilgi sisteminin ve banka içi iletişim kanallarının etkin çalışacak şekilde kurulması,
- Acil durum planı hazırlanması,
- İç kontrol faaliyetlerinin oluşturulması,
- Bankanın iş süreçleri üzerinde kontrollerin ve iş adımlarının gösterildiği iş akım şemalarının oluşturulması

koşullarını getirilmiştir. Yönetmelikle getirilen bu koşullar, bilgi sisteminin bankanın iş akışları üstüne kurgulanarak iş süreçleriyle içselleştirilmiş denetimlerin yapılmasıyla sağlanabilecektir.

İlk bakışta bilgi sistemlerinin doğası gereği aksi düşünülemeyecek bu yönelim, pek çok işletmede bilgi sistemlerini sadece teknolojik servisler sunmakla sınırlı ve ikincil önemde bir destek etkinliği olarak algılayan bakış açılarıyla birlikte düşünüldüğünde izlenmesi gereken bir bakış açısı değişikliği getirmektedir. Yönetmelik bilgi sistemleri yapısının;[4]

- Bankayla ilgili tüm bilgilerin elektronik ortamda güvenli saklanması ve kullanılması,
- Risk ölçüm yöntem veya modelleri kullanılarak risklerin ölçülebilmesi ve zamanında ve etkin bir şekilde raporlanabilmesi,
- Sunulan ürünler, faaliyet türleri, coğrafya veya risk doğuran gruplar bazında veri toplulaştırması yapılabilmesi,
- Yıllık bütçe hedeflerinden sapmaların belirlenmesi,
- Önceden belirlenen risk limitlerine yaklaşılması halinde uyarıcı bilgiler verilmesi,
- Belirlenen azami risk düzeylerine ilişkin aşımların zamanında raporlanabilmesi,
- Risk alma düzeyine göre sunulan hizmetlere ve faaliyetlere ilişkin sermaye yükümlülüğünün tahsisi,
- Stres testi ve senaryo analizi yapılabilmesi,
- Muhasebe sisteminin Türkiye Muhasebe Standartları Kurulu tarafından yayımlanan Türkiye Finansal Raporlama Standartlarına uygun olarak oluşturulmasına

olanak sağlayacak şekilde kurulmasını istemektedir. Bu talepte öne çıkan noktalar, bilgi sistemlerinin öncelikli bir risk yönetim işlevi olarak algılanması ile sistemlerin tasarımda uluslarara-

3 BDDK, *Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik*, 16 Mayıs 2006 tarih ve 26170 sayılı Resmi Gazete 2006, Madde 9

4 BDDK,a.g.e, 2006, Madde 11

sı kabul gören standartlara bağlanmış muhasebe standartlarının bilgi sisteminin bir özelliği olarak belirtilmiş olmasıdır. Bankanın iş süreçleri üzerinde kontrollerin ve iş adımlarının gösterildiği iş akım şemalarının oluşturulması yönündeki zorunlulukla birlikte ele alındığında, bilgi sistemlerinin kuruluşunda sadece etkin teknolojik çözümlerin beklenmediğini, belli ölçüde yürütme işlevine de sahip daha geniş ölçekte bir yapılanmanın hedeflendiği düşünülmektedir.

Kuşkusuz, BASEL II yaklaşımında "*yetersiz ve başarısız içsel süreçlerden, personel ve sistemlerden ya da dışsal olaylardan kaynaklanan, doğrudan veya dolaylı zarar riski*" olarak öne çıkarılan, BDDK'nın da "Bankaların İç Denetim ve Risk Yönetimi Hakkında Yönetmeliğinde" "*Banka içi kontrollerdeki aksamalar sonucu hata ve usulsüzlüklerin gözden kaçmasından, banka yönetimi ve personeli tarafından zaman ve koşullara uygun hareket edilmemesinden, banka yönetimindeki hatalardan, bilgi teknolojisi sistemlerindeki hata ve aksamalar ile deprem, yangın, sel gibi felaketlerden kaynaklanabilecek kayıplara ya da zarara uğrama ihtimali*" kuvvetle vurgulanan operasyonel riskler göz önüne alındığında bilgi sistemleri yönetimine yönelik risk-odaklı yaklaşım belirginleşmektedir.

Risk yönetimiyle, bankanın gelecekteki nakit akışlarının içerdiği risk-getiri yapısını, buna bağlı olarak faaliyetlerin niteliğini ve düzeyini izlemeye, kontrol altında tutmaya ve gerektiğinde değiştirmeye yönelik olarak belirlenen politikalar, uygulama usulleri ve belirlenen limitler yoluyla, üstlenilen risklerin tanımlanmasını, ölçülmesini, izlenmesini ve kontrol edilmesini sağlayan bir yapının amaçlandığı dikkate alınırsa bilgi sistemlerinden beklenen işlevselliğin derinleştirildiği görülmektedir. Amaçlanan risk yönetiminin işletme süreçlerini destekleyebilmesi için bilgi sistemlerinin, risk ölçüm modellerinin kurulmasına, modelin günlük ve konsolide raporlar üretmesine, risk limitlerine yaklaşıldığı veya aşıldığı takdirde uyarılar oluşturulmasına, risk faktöründeki değişmelerin elde edilecek hâsılat ve katlanılacak maliyetlere etkisini ölçebilecek kapasiteye sahip olması gerekmektedir. Muhasebe sistemine gömülü olarak kurgulanacak bilgi sistemleri böylelikle dikey bir boyut kazanacaktır. Risk ve süreç odaklı bu yaklaşım bilgi sistemlerine kontrol hedefleri atanması ve ölçülmesi gereksinimini doğuracaktır. Bu gereksinim belirlendikten sonra bilgi sistemlerine verilen önemle ilgili en dikkat çekici hükümlere Yönetmeliğin 16 ncı maddesinin üçüncü bendinde yer verilmiştir. Bilgi sistemlerinin kontrollerine ilişkin bu hükümler altında genel bilgi sistemi kontrolleri, "*bilgi sistemi ve yönetimine ilişkin faaliyet ve bu faaliyetlere ilişkin süreçlerin kontrollerini"* kapsayacağı belirtilerek uygulama kontrollerinin "*bilgi sistemleri içerisinde yer alan ve bankacılık faaliyetlerini yürütmek veya desteklemek için kullanılan finansal verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi gibi tüm iş süreçlerinde kullanılması gereken iç kontrolleri*" kapsayacağı söylenmektedir. Kurul, genel bilgi sistemi kontrolleri ile uygulama kontrolleri çerçevesinde yapılacak asgari kontrollerin kapsamına ilişkin usul ve esasları belirlemeye yetkili olduğunun altını çizerek bilgi sistemlerinin yönetimi ve denetimi konusundaki normların tanımlanması, izlenmesi, düzenlenmesi gerekliliğini işaret etmektedir.

"Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"in uygulanması konusunda atılan adımları destekleyen önemli bir karar da bilgi sistemleri denetimi faaliyetinin üçlü bir yapı üstüne kurulmuş olmasıdır. Bu üçlü yapı bankaların iç kontrol birimlerini, bağımsız denetim kuruluşlarını ve kamu otoritesinin denetimini içermektedir. Denetim konusunda farklı yönlerden sorumlu ve etkin olabilecek söz konusu taraflar arasında işbirliği ve paylaşım ortamı yaratılmasının yanısıra, bu yapıda

önemli bir nokta da sorumluluğun bölüşümü yoluyla saydamlık ve hesap verebilirliğin güvence altına alınmasıdır. Kurumların *doğru beyan* yükümlülüğü iç kontrol birimlerine, *kanıta dayalı tarafsız görüş* gereksinimi bağımsız denetim kuruluşlarına ve *kamu yararı adına gözetim* gereği otoritenin yetkisine bırakılmıştır.

Öngörülen kurgunun diğer önemli bir niteliği zaman içinde sistemde birikecek bilginin ve eğilimlerin en iyi uygulamalar olarak tanımlanmasına ve yaygınlaştırılmasına olanak verecek olmasıdır. Böylelikle, gerek içerik birliğinin sağlanmasına gerekse bilgi sistemleri denetim mesleğinin gelenek ve normlarıyla kurumsallaşmasına destek verilmiş olacaktır. BDDK'nın 17/08/2006 tarihli ve 26262 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" ve takiben 5/12/2006 tarihli ve 26367 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ" ile denetim faaliyetleri mesleki usul ve ölçütlere bağlanarak konuya bütünlük kazandırılmıştır.

2.2. Tebliğde Öngörülen Bilgi Sistemleri Denetim İlke ve Yöntemleri

Tebliğ'de bilgi sistemleri yönetiminin önemine 4 üncü maddede "*bilgi sistemleri yönetiminin kurumsal yönetim uygulamalarının bir parçası olduğu*" ifadesi yer almakta ve bankanın operasyonlarını istikrarlı, rekabetçi ve gelişen bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejinin iş hedefleri ile uyumlu olmasının sağlanması, bilgi sistemleri yönetimine ilişkin unsurların yönetsel hiyerarşi içerisinde uygun yere yerleştirilmesi ve gerekli finansman ve insan kaynağının sağlanabilmesi konuları hükme bağlanmaktadır. Diğer bir önemli vurgu ise, bilgi sistemleri üzerinde kurulan yönetimin etkinliğinin; risk yönetimi, iç kontrol sistemi ve iç denetim kapsamında yürütülecek çalışmaların da katkısıyla sağlanacağıdır. Bu noktadan hareketle, bilgi sistemlerine ait risk yönetimi ve iç kontrollerin kurulması amacıyla kurumlarca bilgi teknolojilerinin bankacılık faaliyetlerinde kullanılması nedeniyle oluşan risklerin temel kaynağı olarak kabul edilebilecek aşağıda sıralanan unsurların göz önüne alınması gerekmektedir:

- Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda bu gelişmelere uymamanın olumsuz sonuçları ve bu gelişmelere uyma konusundaki zorluklar,
- Bilgi sistemlerinin bilinenlerden farklı hatalara ve hilelere zemin hazırlayabilmesi,
- Bilgi sistemlerinin bankacılık faaliyetlerinde kullanımının artmasına bağlı olarak yaygınlaşan destek hizmeti alımı, buna bağlı olarak operasyonlarda destek hizmeti kuruluşlarına bağımlılığın doğmuş olması,
- Bankanın iş sürekliliğinin bilgi sistemlerinin işlerliğine bağlı duruma gelmesi,
- Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin ve tutulan, aktarılan, işlenen verilerin güvenliğinin sağlanmasının zorlaşmış olması.

Bilgi teknolojilerinden kaynaklanan risklerin *operasyonel risk* kapsamında değerlendirilmesinin yanı sıra bu risklerin bankacılık faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceğinden, bilgi teknolojilerinden kaynaklanan riskleri de içeren bütünleşik bir risk yönetim yaklaşımı tüm bankacılık faaliyetleri için benimsenmesi gerekmektedir.[5] Bilgi sistemlerine

[5] Varlı Ahmet Türkay, *Basel II ve Teknoloji* sunumu, http://www.bddk.org.tr/turkce/Raporlar/Sunumlar/1989bddk_basel2_teknoloji%20%5BRead-Only%5D.pdf , www.bddk.org.tr içinden 27 Temmuz 2008, 2006, s.14

ilişkin risklerin yönetimi amacıyla geliştirilen politika ve prosedürlerin gerekleri, bankanın *organizasyonel yapısı içerisinde* fiili olarak işleyecek şekilde yerleştirilmesi, bunların işlerliğine ilişkin gözetimin gerçekleştirilmesi gerekmektedir. Bilgi teknolojilerinin özel niteliklerinden kaynaklanan risk yönetim kuralları, üst yönetim gözetimi, güvenlik kontrolleri, yasal risk ve itibar riski yönetimi başlıkları altında yapılması gerekenler ifade edilmektedir.

Burada esas olan bankanın, kendi risk profiline, operasyonel yapısına, kurumsal yönetim kültürüne ve ilgili diğer mevzuat ile çizilen çerçeveye uygun olarak bilgi sistemlerine ilişkin risk yönetim süreçlerini geliştirmesi ve bilgi teknolojilerinden kaynaklanan riskleri de bu kapsamda değerlendirmeye almasıdır. Bu yönetim süreçleri aşağıdaki başlıklar altında toplanabilmektedir[6]:

- Bilgi sistemleri kullanımından kaynaklanan risklerin yönetilmesi için etkin bir üst yönetim gözetimi,
- Bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, güvenlik kontrol süreci,
- Alınacak destek hizmetleri bağlamında, doğabilecek risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve yeterli bir gözetim mekanizması,
- Bilgi sistemleri üzerindeki işlemler için uygun bir kimlik doğrulama mekanizması,
- Kritik işlemlerde, inkâr edilemezlik ve sorumluluk atama olanaklarını içeren teknikler,
- Bilgi sistemleri, veritabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görevler ayrılığı prensibi,
- Uygun bir yetkilendirme ve erişim kontrolü sağlanması,
- Bilgi sistemleri üzerinden gerçekleşen işlemlerin, doğruluğunun, tamlığının ve güvenilirliğinin sağlanması, geliştirilecek önlemlerin verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsaması,
- Bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması geliştirilmesi,
- Veri güvenliği ve gizliliğini sağlayacak önlemlerin alınması,
- Risklerin etkisini azaltmaya yönelik güvenlik prensipleri ve bu risklerden korunmak için kullanıcı ve müşterilerin bilgilendirilmesi,
- Bilgi sistemlerine ilişkin iş süreklilik ve kurtarma planı ile acil durum ve beklenmedik olay planları ve uygun bir yedekleme altyapısı,

Belirtilen yönetim süreçleri üzerinde işletilecek denetim yöntemleri oluşturulurken, BDDK muhasebenin temel kavramlarından *önemlilik* kavramına atıfta bulunarak seçtiği yaklaşımın doğruluk ve tutarlılığını artıracak bir kavramsal boyut ortaya koymaktadır. Türkiye Muhasebe Standartları Kurulu (TMSK) tarafından hazırlanan kavramsal çerçeve'de önemlilik kavramı: "*Eğer bir bilginin verilmemesi ya da yanlış verilmesi mali tabloları kullanarak ekonomik kararlarını verecek olan kullanıcıları etkileyebilecekse, o bilgi önemliliğe sahip bir bilgidir. Bilginin eksikliği veya yanlışlığı durumlarında*

6 BDDK, *Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğde Değişiklik Yapılmasına Dair Tebliğ, 05* Kasım 2007 tarih ve 26691sayılı Resmi Gazete, 2007a, Madde 5

önemlilik hususunun olup olmadığına karar vermek için bilgi verilmeyen kalemin ya da hatalı verilen kalemin büyüklüğüne bakmak gerekir. Bu nedenle, önemlilik, bilginin faydalı olması için öncelikle taşıması gereken niteliksel bir özellik olmaktan ziyade, bir ayrım ya da ayrıştırma noktasını gösterir." şekilde yorumlanmaktadır.

Bilgi sistemleri denetiminin kavramsal bütünlüğü içinde önemlilik kavramının önemi, söz konusu kavramı etkileyen niteliksel ve niceliksel etkenlerin çoğunun bilgi sistemleri içinde saklanıp işleniyor olması nedeniyle tartışılmaz niteliktedir. Bu nedenle gerek hata, eksiklik ve varsa kasıtlı hilelerin belirlenmesi gerekse muhasebe sisteminin doğruluk ve güvenilirliğinin kanıtlanması açılarından bilgi sistemleri denetimine temel olacak kontrollerin iş süreçlerine gömülü olarak tasarlanması gerekmektedir. Tasarlanacak kontroller, hem bilgi sistemleri üzerinden iş sürecinin kontrolünü hem de bilgi sistemlerinin yürürlükteki politikalara uygun biçimde işletilip işletilmediğinin denetimini kapsayan çift katmanlı bir yapıda oluşturulacaktır. Örneğin, bankacılık işlemlerinin doğruluğu veri tabanlarında oluşan kayıtlarla kıyaslanarak denetlenecek, diğer yandan bu işlemleri gerçekleştirmekle ilgili sorumluların yetkileri dâhilinde işlem yapıp yapmadıkları, işlemlerin önceden izin verilen akış içinde gerçekleştirilip gerçekleştirilmediği bilgi sistemleri denetim izlerinden doğrulanacaktır.

05 Aralık 2006 tarihinde BDDK tarafından yayımlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ"de önemlilik kavramının, mesleki deneyime dayalı bir yargı konusu olduğunun tekrarlanması dikkat çeken bir başka noktadır. Bu tekrar ile önemlilik kavramının denetim sürecinin her aşamasında (denetimin planlanması, gerekli alanlarda yoğunlaştırılması, bulguların değerlendirilmesi ve kanıtların toplanması) kullanılabileceği belirtilmiştir.

2.3. Bilgi Sistemlerinde Kurulacak İç Kontroller

Kurumsal varlıkların korunmasını, faaliyetlerin etkin ve verimli bir şekilde yasalara ve ilgili diğer mevzuatlara, kurum içi politika ve kurallara ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe sisteminin güvenilirliğini, bütünlüğünü ve bilgilerin zamanında elde edilebilirliğini sağlamak amacıyla Tebliğ'de bilgi sistemlerine ilişkin kontroller tanımlanmıştır. Tanımlanan kontroller aşağıda belirtilen iki ana sınıf altında oluşturulmuştur. Bunlar[7]:

- Bilgi sistemleri içerisinde yer alan ve bankacılık faaliyetlerini yürütmek veya desteklemek için kullanılan finansal verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi gibi tüm iş süreçlerinde kullanılması gereken iç kontrollere karşılık gelen "**Uygulama Kontrolleri**", ve
- Bilgi sistemlerinin tamamına veya büyük bir bölümüne uygulanan, bilgi sistemlerinin kendilerinden beklenen fonksiyonları doğru bir şekilde yerine getirmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvence oluşturulması ile uygulama kontrollerinin işlevselliği için güvenilir bir ortamın kurulmasını hedefleyen politika ve prosedürlerden oluşan, bankanın bilgi sistemlerinin bir bütün olarak kendisinden beklenen fonksiyonları doğru, zamanında ve güvenilir bir şekilde gerçekleştirilmesine yönelik ortamın sağlanmasına temel olan "**Genel Kontroller**"dir.

7 BDDK, 2007a, Madde 20

Kurumun iş süreçlerinin kontrolünü ifade eden iş döngüsü kontrolleri içerisinde yer alan, bilgisayar destekli ve geleneksel yordamlarla gerçekleştirilen uygulama kontrolleri asgari düzeyde:[8]

- Veri oluşturma/yetkilendirme kontrolleri: Veri hazırlama yordamları, kaynak belge yetkilendirme prosedürleri, kaynak belge verilerinin toplanması, kaynak belgelerdeki hataların ele alınması, kaynak belgelerin saklanması,
- Girdi kontrolleri: Girdi yetkilendirme yordamları, doğruluk, bütünlük ve yetkilendirme kontrolleri, veri girdilerindeki hataların ele alınması,
- Veri işleme kontrolleri: veri işlemede bütünlük, onaylama ve değiştirme, hataların ele alınması,
- Çıktı kontrolleri: Çıktıların alınması ve saklanması, çıktıların dağıtımı, çıktı uyumluluğu, çıktıların gözden geçirilmesi ve hataların belirlenmesi, çıktıların güvenliğinin sağlanması
- Sınır kontrolleri: Aslına uygunluk ve bütünlük kontrolleri, hassas bilginin iletilmesi sırasında korunması,

boyutlarını içermektedir. Bilgi sistemlerinin bir bütün olarak kendisinden beklenen görevleri doğru, zamanında ve güvenilir biçimde yerine getirmesine olanak verecek ortamın kurulmasına esas olan genel kontroller konusunda ise BDDK izlediği yaklaşımla uluslararası kabul görmüş rehber, çerçeve veya metodolojilerden yararlanmak yoluna gitmiş ve bilgi teknolojilerinin kurumsal başarı için kritik önemde olduğu pek çok sektörde yaygın olarak benimsenen "Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (CobIT)" dokümanı lehine bir seçimde bulunmuştur. Piyasa değerlendirme kuruluşlarının araştırmalarına bakıldığında yapılan seçimin yerinde olduğu, CobIT standardının benzer pek çok bilgi teknolojileri çerçevelerince de uyumlu kabul edildiği görülmektedir.

BDDK'nın CobIT seçiminin ardında; iş süreçleri denetimine kolaylık getiren ve risk odaklı bütüncül bir yapı sunması, daha da önemlisi tarafız denetimin yükünü ciddi ölçüde azaltarak değerini yükselten kıyaslama veya derecelendirmeye elverişli ölçülebilir kilit başarı faktörlerini içeriyor olmasının belirleyici olduğu düşünülmektedir. CobIT seçimini destekleyen diğer etkenler olarak yönetilebilirliği destekleyen bir kurumsal yönetim aracı olma niteliği, teknolojiden bağımsızlığı, ISO/IEC 17799:2000 (Bilgi Güvenliği Yönetimi için Uygulama Kodu), ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi), CMMI (Bütünleşik Yetkinlik Olgunluk Modeli) gibi diğer rehberlere uyumlu olmasıdır.

Çalışmanın takip eden bölümünde BDDK tarafından bilgi sistemleri yönetimi ve denetimi alanında tercih edilen "Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (CobIT)" rehberi incelenerek, özellikle kurumsal yönetime getirdiği yorum ve destekler değerlendirilmiştir.

3. CobIT "BİLGİ TEKNOLOJİLERİNE İLİŞKİN KONTROL HEDEFLERİ"

Bilişim teknolojileri yönetiminde kullanılan çerçeve rehberlerden biri olan CobIT (Bilgi Teknolojilerine İlişkin Kontrol Hedefleri-Control Objectives for Information Technology), özü bakımından bilişim teknolojileri süreçleriyle ilgili kontrol hedeflerinden ve denetim çerçevesinden oluşmaktadır. Çerçeve model, ilk olarak ISACA (Bilgi Sistemleri Denetimi ve Kontrol Birliği - Information Systems Audit and Control Association) tarafından 1996 yılında ya-

8 BDDK, 2007a, Madde 21

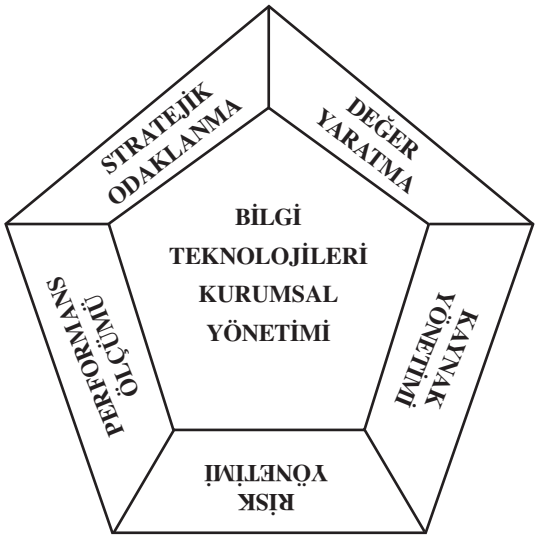
yınlanmıştır. Çerçeve son olarak 2007 yılında güncellenmiş ve 4.1 sürümünde olgunluk düzeylerine ilişkin boyutlar geliştirilmiş ve IT Kurumsal Karne'sine ilişkin bölümler derinleştirilmiştir. Çerçevenin çıkış noktası "*bilgi sistemleri denetimi*"dir. Son sürümüyle ulaştığı aşamada denetim, kontrol, yönetim ve nihayetinde yönetişim kavramlarını kapsamaktadır. CobIT denetim çerçevesinin hedef kitlesi üst yöneticiler olup, muhtemel bilişim teknolojileri risklerini, örneğin; başarısızlıkla sonuçlanabilecek projeleri, yatırım yanlışlıklarını, güvenlikle ilgili zayıflıkları, müşteri / kullanıcı gereksinimlerine uyumlu olmayan çözümleri, olası sistem kayıpları üst yönetime görünür kılmayı amaçlamaktadır.

CobIT, bilgi teknolojilerini etkin ve yaygın olarak kullanımından kaynaklanan risklerin yönetilmesi ve bilgi teknolojilerine dayanan kritik iş süreçlerini bilinçli ve sistematik yöntemlerle desteklemesinin yanında, kurumların bilgi sistemleri üzerinde sağlanacak kontroller ile ilgili yenilikler ve zorunluluklar getirmektedir. CobIT'de yönetim sorunlarını ve gereksinimlerini ön plana alan tanımlamalarla, güvenlik ve kontrollerin etkinliğini tespit ve izleme gereksinimlerini karşılayan belli araç ve yöntemler yer almaktadır. Bu araçlar yardımıyla:

- Risk Yaklaşımı
- Bilgi Teknolojileri Kontrolleri
- Hedef Göstergeleri
- Kritik Başarı Etkenleri
- Performans Göstergeleri
- Kıyaslama
- Olgunluk Modeli

bileşenlerine odaklanılarak süreçlerin kontrol altına alınması sağlanmaktadır. CobIT bu yönleriyle kuruluşlarda bilgi teknolojileri yönetişim modelinin kurumsallaşmasını kolaylaştırmakta ve risk odaklı bir denetim çerçevesi sağlamaktadır. Bilgi teknolojilerinin *hedef ve risk odaklı* yönetimini amaçlayan CobIT stratejik işletme hedefleriyle uyumluluk açısından sergilediği yaklaşım ve içerik ile öne çıkmaktadır.

CobIT, bilgi teknolojilerini iş süreçlerinin destekçisi olarak görmekte ve aralarındaki ilişkileri ortaya koymaktadır. Bu sayede bilgi teknolojileri kaynaklarının işletme stratejileri doğrultusunda etkin biçimde kullanılmasına olanak sağlamaktadır. CobIT, bütünüyle teknik ölçütlere dayanan standartların aksine sadece gizlilik, bütünlük ve devamlılığı değil etkinlik, verimlilik, uyum ve güvenilirliği de kontrol hedeflerine dâhil etmektedir. CobIT'in bilgi teknolojileri bağlamında kurumsal yönetim ortamına katkısı Şekil.1'de gösterilmiştir.



Stratejik Odaklanma İşletme ve bilgi teknolojileri (BT) planlarının bütünleştirilmesi BT tarafından yaratılan değerin tanımlanması, sürdürülmesi ve doğrulanması bilgi teknolojilerinin faaliyetlerinin kurumsal faaliyetlere örtüştürülmesine yöneliktir.

Değer Yaratma BT hizmet döngüsü boyunca değer yaratmanın yürütülmesi BT'nin strateji kapsamında taahhüt ettiği kazançları temin etmesi, BT maliyetlerinin optimizasyonu ve BT yapısal değerinin kanıtlamasıyla ilgilidir.

Kaynak Yönetimi Optimal BT yatırım, yazılım, bilgi, alt yapı ve insan gibi kritik BT kaynaklarının uygun biçimde yönetilmesiyle ilişkilidir.

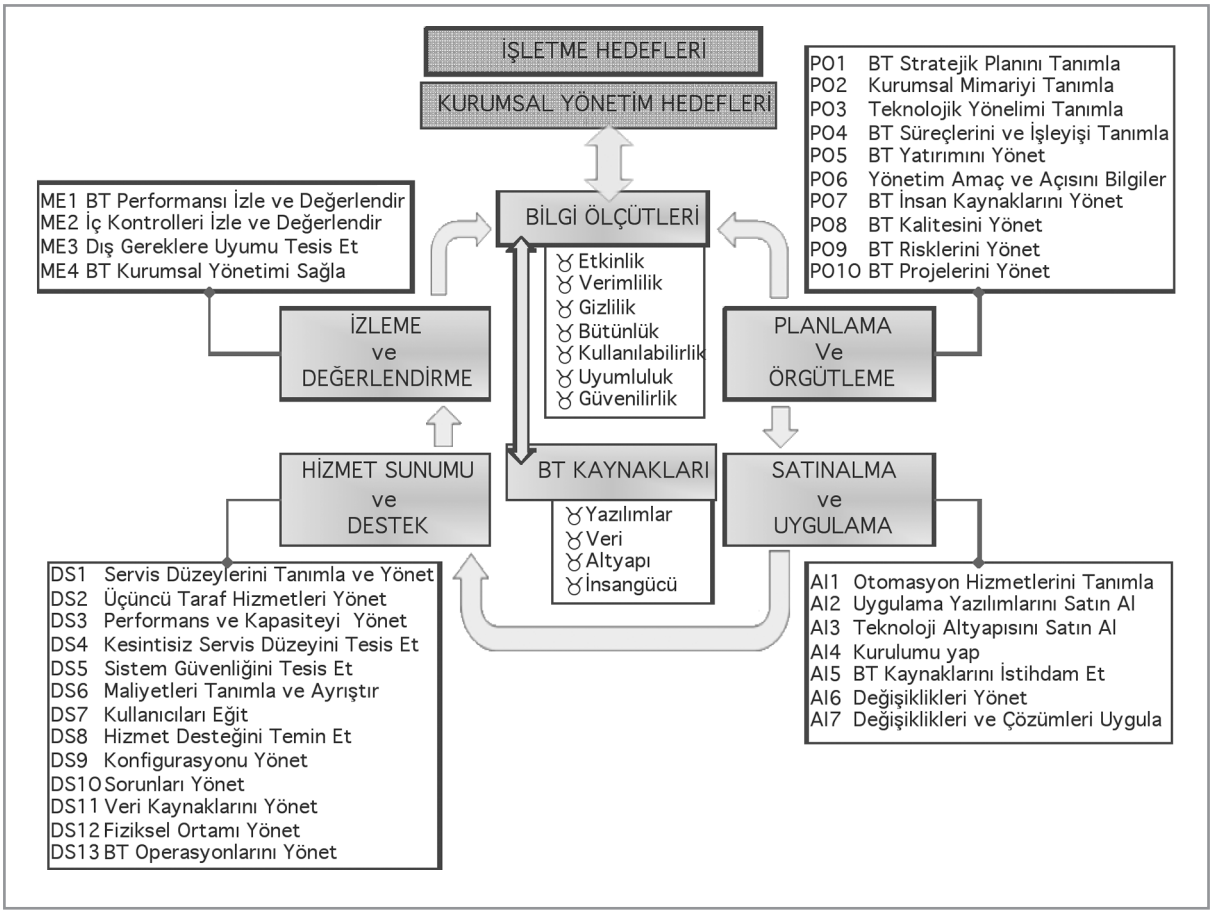
Risk Yönetimi Üst düzey yöneticiler de risk farkındalığı yaratılması, açık bir kurumsal risk tutumu oluşturulması, uyumluluk gereklerinin anlaşılması tanımlanmış riskler için kurumsal saydamlığın sağlanması ve kurum içinde risk yönetim sorumluluklarının yerleştirilmesiyle ilgilidir.

Performans Ölçümü Geleneksel maliyet yöntemlerinin ötesinde hedeflere ulaşmada stratejinin eyleme dönüştürülmesine hizmet eden kurumsal karnelerin kullanımıyla stratejik sonuçların, proje kapanışları, kaynak kullanımı, süreç başarım ve hizmet üretimin izlenmesi ve eğilimlerinin gözetilmesidir.

Şekil.1 Bilgi Teknolojileri Kurumsal Yönetim Odakları (ITGI, 2007b, s.6)

CobIT'in misyonu; yönetim ve denetim kadroları tarafından sürekli kullanılabilmesi amacıyla güncel, genel kabul görmüş bilgi teknolojileri kontrol hedeflerinin araştırılması, geliştirilmesi, yayınlanması ve kullanımına destek verilmesi olarak açıklanabilir; CobIT'in vizyonu ise bilgi teknolojileri yönetişim (IT governance) modeli olmaktır. CobIT salt bir denetim aracı olmanın ötesinde bir yönetişim aracı olma vizyonuna sahiptir. Bu nedenle yönetimden bilgi teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlama amacını gerçekleştirmeyi hedeflemektedir.

CobIT dokümanında, bilgi teknolojileri süreçleri; "*Planlama ve Örgütlenme*", "*Satın alma ve Uygulama*", "*Hizmet Sunumu ve Destek*", "*İzleme ve Değerlendirme*" kategorileri altında sınıflandırılmıştır. Hedefler, kaynaklar, süreç kümeleri ve süreçler bir araya getirildiğinde oluşturulan CobIT Mimarisi ana hatları ile Şekil.2'de yer almaktadır.



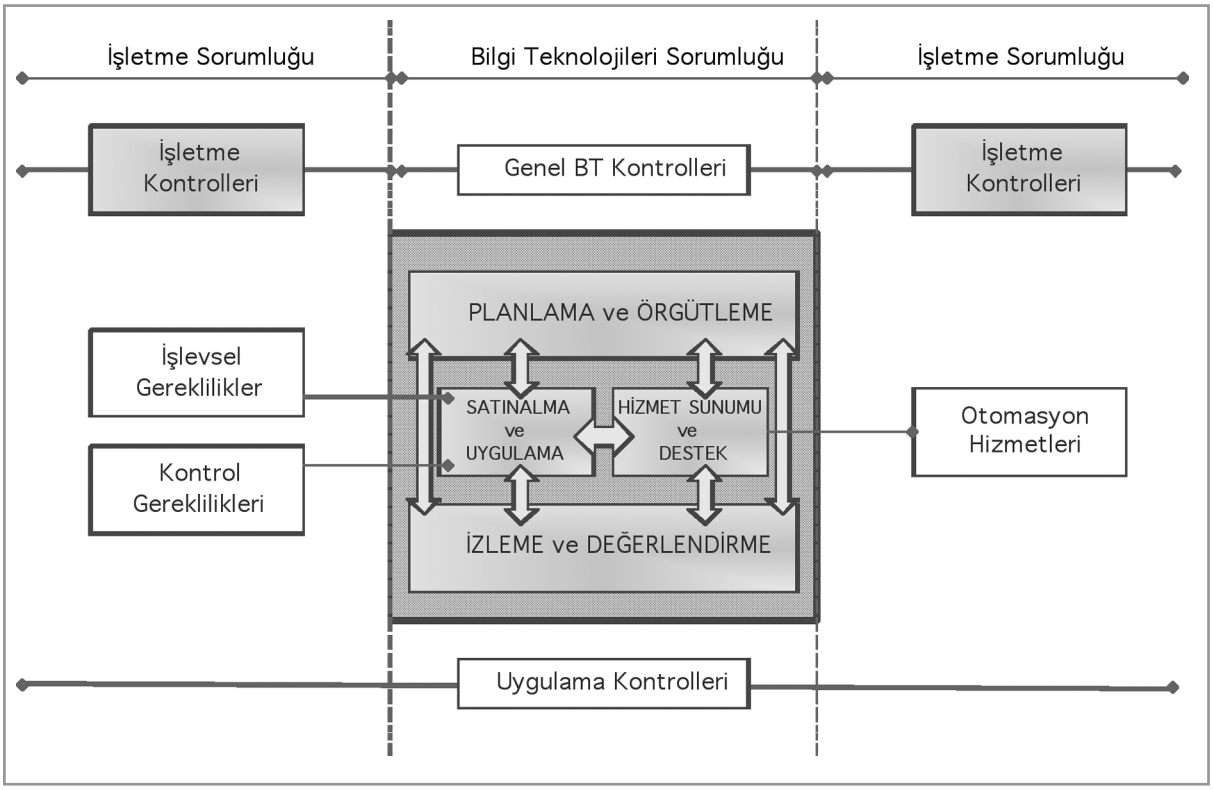
Şekil 2. CobIT Mimarisi (ITGI, 2007b, s.26)

CobIT, bilgi işlem güvenliği için kapsamlı ve iyi bir uygulama niteliği ortaya koymaktadır. CobIT'de yer alan Yönetim Rehberi (Management Guidelines) içerisinde tüm teknoloji süreçleri için Olgunluk Modeli (Maturity Model), Kritik Başarı Etkenleri (Critical Success Factors), Ana Hedef Göstergeleri (Key Goal Indicators) ve Ana Performans Göstergelerinin (Key Performance Indicators) tanımlanmış olması nedeniyle, bilgi teknolojileri süreçleri dahilinde, kuruluşun hedeflerine ulaşma derecesi ölçülebilmektedir.[9]

BDDK'nın CobIT çerçevesini tercih etmesinin nedenlerinden biri olarak düşünülen bu ilişkiler bütünlüğü temelinde *denetim* kavramına yükle-

9 ITGI, 2007b, s.8

nen yeni anlamlarla yakından ilişkilidir. Bu anlam derinleşmesi; sapmalar ve yanlışlıkları belirlemek adına yürütmenin belli aşamalarda doğrulanması anlamından ileriye giderek denetim kavramının işletme hedeflerine erişilebilmesi ve sapmalara yol açacak olguların oluşmadan önlenmesi, risklerin teşhis edilmesi ve düzeltilmesi için *makul ölçülerde* güvence verecek politikaların, yönergelerin, yöntemlerin ve yapıların bütüncül bir kavrayışla işletilmesi içeriğine yakınlaştırılmasıdır. Denetim yaklaşımı bakımından, BDDK'nın CobIT çerçevesi üzerine kurulması ve bu çerçeveden takip edilmesini istediği genel kontroller her bir bilgi sistemleri sürecine ayrıca atanan jenerik kontrolleri kapsamaktadır.[10] Bu doğrultuda CobIT kontrolleri ile iş süreçleri kontrolleri arasındaki sınırlar ve bağlantılar ise Şekil.3'de ortaya konmuştur.



Şekil 3. CobIT Kontrolleri ve İşletme Kontrolleri Arasındaki Sınırlar (ITGI, 2007b, s.16)

10 ITGI, 2007b, s.14

Bilgi Sistemleri denetimi, dolayısıyla kurumsal denetim bakımından CobIT çerçevesinin getirdiği önemli bir boyut iş süreçlerine gömülü olarak işleyen çeşitli bilgi teknolojileri süreçlerinin *yeterlilik düzeylerinin* atanması, ölçülmesi ve izlenmesi için kilit başarı göstergeleri ve göstergelerin bağlanabileceği kurumsal karneler için araçlar sunmasıdır. Bankalar, finans kuruluşları ve elbette uyumluluk gereklerini karşılamak durumunda olan tüm diğer işletmeler için önem taşıyan nokta, işletmenin hangi gereksinimlerinin ne ölçüde temin edecek yeteneğe, kapasiteye sahip olunduğunun doğru ölçülmesi, en iyi uygulamalar belli bir düzeyde tesis edilse dahi, varılan düzeyin işletme beklentilerini ne düzeyde karşıladığı, sergilenen performansın hedeflere erişilmesinde yeterli olup olmadığının anlaşılmasıdır.

Dolayısıyla herhangi bir uygulamanın kendisi son amaç olmamaktadır. CobIT çerçevesinin temel önemi de, herhangi bir uygulamayı dayatmadan, işletmelere başarılı sayılabilmeleri için asgari olarak neyin yeterli olabileceği konusunda bilgilendirme yapmak ve işletmelerin kendi başarı hedeflerine uygun olarak bilgi teknolojileri faaliyetlerini nasıl düzenleyebilecekleri ve işletebilecekleri konusunda yönlendirici olmaktır. Böyle bir yaklaşım gelişmenin önünü açık tutmakta ve hedefler arasındaki farklı başarı düzeylerini kıyaslayarak, kurumsal yönetimin etkinliğini artıracak yönde işletmelerin zayıf yönlerine odaklanılmasına ve genel başarımın dengelenmiş bir eylemler zinciriyle sürekli artırılmasına hizmet etmektedir.

Bir işletmenin kendi başarısını, etkinliğini ve verimliliğini tarafsız biçimde belirlemesi kuşkusuz kolay bir çalışma değildir. Neyin ölçülmesi, nasıl ölçülmesi, ne düzeye kadar ölçülmesi, ölçümleri maliyet-kazanç dengesi, ölçümün doğruluğu ve devamlılığı her zaman karşılaşılan sorulardır. Bu sorulara örgüt için dinamikler, iç yapılanmalar, dengeler ve önceliklerin baskısı altında ve ölçümler üzerindeki etkileme güçleri hesaplanmadan güvenilir yanıtlar bulmak zorlu bir süreçtir. Bilgi sistemlerinin uzmanlığa yaslanan teknolojik dilinden gelen zorluklar da eklendiğinde ifade edilen kısıtlar, üst yönetimleri kurumsal yönetim politikalarını oluştururken ciddi bir engelle yüzleştirmektedir. Bilgi sistemlerinde "Olgunluk Modelleri" bu gereksinime çözüm olarak geliştirilmektedir.

4. BİLGİ SİSTEMLERİ YÖNETİŞİMİNDE YENİ GELİŞMELER

Bilgi teknolojileri süreçlerinin yönetimi ve denetimi için "olgunluk modellemesi" yaklaşımı; kurumsal olarak güncel durumun sektörel görecelik içinde konumlandırılması, hangi strateji üzerinde ilerlenmesi gerektiğine etkin ölçütlere dayanılarak karar verilebilmesi ve belirlenen amaçlara doğru ilerlemenin tarafsızlıkla ölçülebilmesi bütünlüğünde "derecelendirme" veya "kıyaslama" çalışmalarına dayanmaktadır.

Bilgi teknolojileri alanında en çok bilinen ve yaygın olarak uygulanarak kabul gören modeller "Yazılım Mühendisliği Enstitüsü (SEI)" tarafından geliştirilen "Yeterlilik Olgunluk Modelleri Entegrasyonu (CMMI)" rehberleridir. Ancak, yazılım ürünleri geliştirme döngüleri için önceden tanımlanmış ilkelere harfiyen uyularak erişilebilecek mükemmellik düzeylerini tanımlayan CMMI rehberlerinden farklı olarak CobIT olgunluk modelleri sabit ve kesintili hedefler atamamakta, olgunluk düzeyleri arasında ölçekler sunarak hangi alanlarda iyileştirme yapılması gerektiğine ışık tutmaktadır. Böylelikle kontrol hedeflerine ulaşmak derecesine sınırlama getirilmemekte, standart yordamların kullanılmasıyla ortalamanın yakalanmasının yeterli gören görüşlerin önü kesilmektedir.

CobIT çerçevesinin "Bilgi Sistemleri Denetimi" alanında önerdiği yenilik bu anlayış altında ortaya çıkmaktadır. Olgunluk modellerinin sadece

ölçüm araçları olmaktan çıkararak yeterlilik, kapsayıcılık ve denetim üçgeninde algılanması kuruluşlara yeni açılımlar sunacak niteliktedir. Olgunluk modelleri bilgi sistemleri yönetim süreçlerinin ne kadar iyi tasarlandığını (ne kadar yeterli olduklarını) belirleyecek, belirlerken destek oldukları işletme gerekleri için atanmış hedeflere varılmasına ne oranda katkı verebildiklerine bakılacak, dolayısıyla gerçekleşen bilgi teknolojileri yatırımlarının getirisi de geniş ölçüde değerlendirilmiş olacaktır. Kontrol hedeflerinin derecesi ve karmaşıklığı, işletmenin stratejik planları, risk değerlendirme ve uyumluluk gereklerine göre biçimlendirilebilecektir. Gereğince tesis edilmiş bir denetim ortamı, olgunluğun bileşenleri (yeterlilik, kapsayıcılık, denetim) öngörülerek kurulabilecektir.

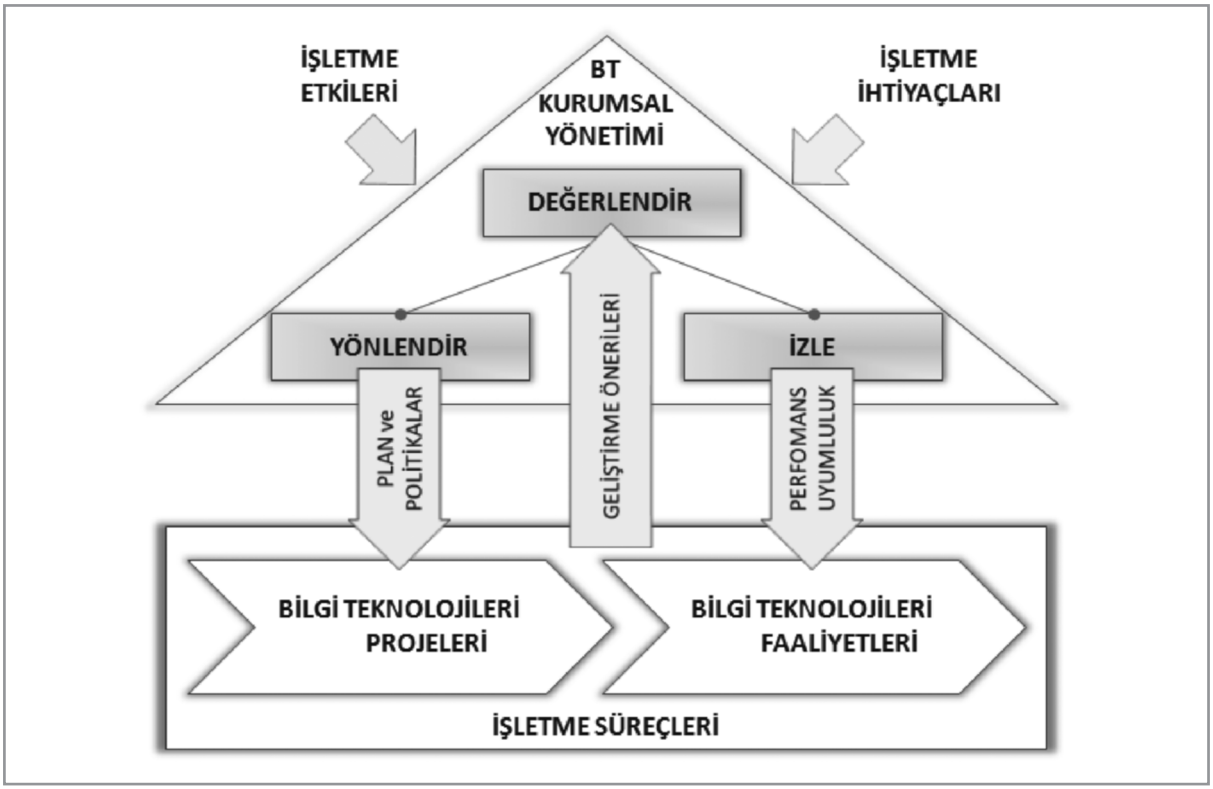
CobIT çerçevesi doğrultusuna kurumların yararına sunulan uygulama kolaylıkları ve deneyimlerin yanısıra, bilgi sistemlerinin kurumsal yönetim alanındaki diğer yeni gelişme ise 2008 içinde Uluslararası Standartlar Enstitüsü tarafından yayınlanan ISO/IEC 38500 "Bilgi Teknolojilerinin Kurumsal Yönetimi" standardıdır.

ISO 38500 standardı bilgi sistemleri yönetişimi konusunda üst yöneticilerin izlemeleri gereken *standart* yaklaşımları kapsayan bir çerçeveyi tanımlamakta ve bu alanda küresel platformda gelinen en uç aşamayı temsil etmektedir. ISO 38500 çerçevesi 2004 yılında güncellenen OECD Kurumsal Yönetim İlkeleri'yle bütünüyle uyumlu olup bilgi sistemleri açısından yönetim (management) ve kurumsal yönetim (governance) kavramlarını yetkin biçimde tanımlayarak, ayrımı açıklığa kavuşturmaktadır. Standart bilgi teknolojileri için iyi kurumsal yönetim kodunu karar vericilere yön gösteren ve yükümlülük getiren altı ilke üstüne inşa etmektedir. Bu ilkeler[11]

- Sorumluluk: Arz ve talep boyutları ile bilgi sistemleri içinde sorumlulukların mutlaka yetki ile donatılmalıdır.
- Strateji: Kurumlar bilgi sistemleri mevcut ve geleceğe dönük yeterliliği anlamında bir stratejiye sahip olmalı, diğer yandan kurumsal stratejiyle örtüşen bir BT stratejisi geliştirilmelidir.
- Tedarik: BT yatırımları mutlaka geçerli nedenlere dayanmalı ve uygun analizlere dayanmalıdır.
- Performans: BT verdiği hizmetler, hizmetlerin düzeyi ve niteliği ile kurumların gerekleriyle örtüştürülmelidir.
- Uyumluluk: BT tüm geçerli yasalara, düzenlemelere uygunluğu tesis etmelidir.
- İnsan Davranışı: BT süreçlere katkısı olan kişilerin güncel ve geleceğe dönük ihtiyaçlarını karşılamalı ve insana saygıya odaklanmalıdır.

ISO 38500 standardı esas aldığı ilkeleri gerçekleştirmek üzere CobIT çerçevesine benzeyen bir model önermektedir. ISO modeli Şekil.6'da gösterilmiştir.

11 ISO/IEC 38500, 2008 Madde 2.1



Şekil 6. ISO 38500 Standardı Modeli (ISO/IEC 38500, 2008 s.7)

5. SONUÇLAR ve ÖNERİLER

Bilgi teknolojilerinin gelişmesi ve İnternet'in tüm dünyadaki iş yapma şekillerinde olduğu gibi bankacılık ve finans sektörünü de doğrudan etkilemektedir. Bilgi teknolojileri ile birçok parasal işlem gerçekte paraya gerek duyulmadan sanal olarak işlenmeye başlamıştır. Bu gerçeğin ışığında bankacılık ve finans kurumlarında iş yapma biçimleri büyük ölçüde bilgi teknolojilerine dayalı olarak yürütülmeye başlanması bu işlemlerin denetlenebilirliğini sağlamak amacıyla düzenlemeler yapma gereğini doğurmaktadır. Bankacılık Denetleme ve Düzenleme Kurumu'nun yayınladığı "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" bu doğrultuda oluşturulmuş bir yasal düzenleme olup, ülkemizde bankacılık ve finans sektöründe bilgi teknolojileri kaynaklı olarak oluşabilecek riskleri asgari düzeylere indirmek amacıyla en iyi uygulamaları yükümlülük olarak getirmektedir. Kıta Avrupa'sında BASEL I ve BASEL II standartları, Amerika Birleşik Devletleri Sarbanes-Oxley standartları ve ülkemizde Bankacılık Kanunu gibi yasal zorunluluklarla birlikte BDDK tebliğinde olduğu gibi bankalar ve finans kurumlarının bilişim faaliyetlerinin denetimine ilişkin kurallar geliştirilmesi ekonomik istikrar ve büyüme açısından önem taşımaktadır.

Kurumlar açısından etkin bilgi sistemleri Teknolojileri yönetişimi için gerekli idari yapılanmaların oluşturulması, bilgi teknolojileri süreçleri-

nin kullanılması ve bilişim konusuyla ilgili tüm paydaşlar arasında dinamik bir işbirliğinin bulunması gerekmektedir. Bu oluşumun temel yapılanması bilgi sistemleriyle ilgili görev ve sorumlukların doğru bir şekilde tanımlanması, bilgi teknolojilerine ilişkin kurumsal yapının tanımlanması, kurumun üst yönetim kurulunda Bilgi Teknolojileri Yöneticisi (Chief Information Officer- CIO) ile temsili, bilgi teknolojilerinin stratejik yönetimi, kurumlar içinde yetkili üst kurulların ve benzeri yapıların oluşturulması yatmaktadır. İdari yapılarla birlikte bilişim teknolojilerinin daha etkin ve verimli kullanımına olanak sağlayan süreçlerin tanımlanması gerekmektedir.

Etkin bir bilgi sistemi kurumsal yönetimin ana süreçleri çalışmamızda da aktarıldığı gibi "Strateji oluşturulması", "Planlama", "Uygulama", "Yönetim" ve "İzleme" olarak teyit edilmekte, bilgi teknolojileri ile işletme yönetimi arasındaki ilişki içinde CIO'nun yerine getirmesi beklenen görevler aşağıdaki gibi ifade edilmektedir:

- Yönetimin temeli işletme hedeflerine varabilmek için stratejinin geliştirilmesi ve yürütmesidir. İzleme ve ölçüm yordamları kurularak üst yönetime bu görevini yerine getirmede gereken girdileri sağlanmalıdır.

- Buna göre, BT stratejisinin kurumsal strateji geliştirilirken bilgi vermesi ve bilgilendirilmesi sağlanmalıdır. Kurumsal stratejinin bilgi sistemleriyle ilgili unsurları stratejik olarak yönetilmelidir.

- Bilgi teknolojileri yönetişimi hedeflenmese dahi, bilgi teknolojileri işlevinde icra düzeyinde yönetici sorumlu olmalı, yönetim kuruluna ve paydaşlara karşı gözetim ve raporlama işlevini üstlenmelidir.

- Günümüzde genel kabul gören bilgi teknolojileri yönetişim yaklaşımlarının kurumsal amaçlar ve planlarla ilişkin olarak bilgi sistemlerini örtüştüren çalışma biçimleri, bilgi teknolojileri stratejinin planlaması, yürütülmesi ve üst yönetime raporlanması faaliyetini destekleyecek yönde sorumlulukları açık biçimde ortaya koyan rollere paylaştırılmalıdır.

Vurgulanan bu asal görevlerin yürütülmesinde uygulamaya dönük yaklaşımların geliştirilmesi gereklidir. Bu yaklaşımlar çoğunlukla bilgi sistemleri yönetimi açısından mevcut durumla amaçlanan düzey arasındaki farkın doğru biçimde belirlenmesine odaklanmaktadır. Sözkonusu kararların doğru ve tutarlı biçimde alınabilmesi, sorumluluklar ve yetkiler açısından çelişkiye düşülmemesi için aşağıda bazı öneriler geliştirilmiştir.

- Öncelikle paydaşların kurumun bilgi teknolojileri stratejisi ile kurumsal yönetim amacı hakkındaki algılarının ve beklentilerinin değerlendirilmesi.

- Güncel durum ve geleceğe yönelik hedefler itibarıyla bilgi sistemleri yönetişime dair bir öz-değerlendirme çalışması gerçekleştirilmesi, CobIT olgunluk modelinden bu çalışmada yararlanılması,

- Öz-değerlendirme çalışması sonuçlarına göre iyileştirme alanlarının önceliklendirilmesi. Önceliklendirme yapılırken, değer katmayan bilgi sistemleri süreçlerinin, parçalanmış BT yatırımları portföyünün, etkisiz BT iletişim kanallarının, görev ve sorumluluk çelişkilerinin, stratejik sahiplenme eksiklerinin ayıklanması veya ortadan kaldırılması,

- Geleceğe dönük olarak tasarlanan bilgi sistemleri yönetişim süreçleri hakkında kurum içinde uzlaşma ve görüş birliği sağlanması, geliştirilecek süreçler hakkında izlenecek ilkeler, alt yapı, kurumsal mimari, etkilenecek işletme süreçleri, yatırım ihtiyacı ve kurulum önceliklerinin açık biçimde tanımlanması,

- Bilgi sistemleri yönetişimin sürekli iyileştirilmesine katkı verebilecek süreç ve danışma ve paylaşım forumların oluşturulması,
- Bilgi sistemleri yönetişimi ile ilgili değişikleri tüm paydaşlara amaç görevler, roller, yetkiler, zamanlama ve performans ölçümleri hakkında yeterince bilgi verilerek uygulanması, değişiklerle sonucunda en iyi uygulamalara yakınlaşması, BT girişimlerinin tatminkâr maliyet-kazanç sonuçlarına dayandırılması ve yeni teknolojilerin kurumlara nasıl ve ne zaman kazandırılacağına dair stratejik yönlenişlerin oluşturulması.

BDDK'nın benimsediği ve sektöre yönelik olarak zorunlu kıldığı bilgi sistemleri denetim yükümlülüklerinin tesis edilmesi ve CobIT çerçevesinden yararlanılarak kurumsal yönetim düzeylerine varılabilmesi anlamında yapılabilecek çalışmalar bunlarla sınırlı olmayacaktır.

KAYNAKÇA

Ahmet Türkay Varlı, *Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi/ Mevzuat Çerçevesinde BDDK Perspektifi* http://www.bddk.org.tr/turkce/Raporlar/Sunumlar/4020TIDE_Sunum.pdf Türkiye İç Denetim Enstitüsü, XI. Türkiye İç Denetim Kongresinde yapılan sunum, İstanbul 2007

Ahmet Türkay Varlı, *Basel II ve Teknoloji* sunumu, http://www.bddk.org.tr/turkce/Raporlar/Sunumlar/1989bddk_basel2_teknoloji%20%5BRead-Only%5D.pdf , www.bddk.org.tr içinden 27 Temmuz 2008 tarihinde ziyaret edildi

Alan Cadler, *IT Governance Today: A Practionner's Handbook,* London, 2006

BDDK, *Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri*

Denetimi Hakkında Yönetmelik, 16 Mayıs 2006 tarih ve 26170 sayılı Resmi Gazete, Ankara www.bddk.org.tr

BDDK, *Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğde Değişiklik Yapılmasına Dair Tebliğ, 05* Kasım 2007 tarih ve 26691sayılı Resmi Gazete, Ankara www.bddk.org.tr

BDDK, *Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ*, 14 Eylül 2007 tarih ve 26643sayılı Resmi Gazete, Ankara www.bddk.org.tr

BDDK, *Bankaların İç Sistemleri Hakkında Yönetmelik*, 01 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete, Ankara www.bddk.org.tr

BDDK, *Yeni Sermaye Yeterliği Uzlaşısı (Basel II) ve Geçiş Süreci Yol Haritası sunumu http://www.bddk.org.tr/turkce/Raporlar/Sunumlar/1985__www.bddk.org.tr_turkce_yayinlarveraporlar_sunumlar_12122003_rygtd.pdf* Ankara, 2003

Francis Fukuyama, *Güven: Sosyal Erdemler ve Refahın Yaratılması*, Çev: Ahmet Buğdaycı, Türkiye İş Bankası Yayınları, Ankara, 1998

GARTNER, *Creating an Effective IT Governance Process* ID Number: COM-21-2931, Stanford 2003

GARTNER, *Defining IT Governance: Roles and Relationships* ID Number: G00139986, Stanford 2006

GARTNER, *Making IT Governance Work in Your Organization,* Orlando Florida 2006

GARTNER, *Toolkit: Making Application Governance Relevant,Simple, Usable and Active*

ID Number: G00142844, Stanford 2006

ISO/IEC 38500 *Corporate Governance for Information Technology*, İsviçre 2008

ITGI ve PricewaterhouseCoopers, *IT Governance Global Status Report—2008,* Meadows Illionis, 2008

ITGI, *CobIT 4.1,* Meadows Illionis, 2007

ITGI, *CobIT Control Objectives* 3rd Edition, Meadows Illionis, 2003

ITGI, *CobIT Implementation Tool Set* 3rd Edition , Meadows Illionis, 2000

ITGI, *Enterprıse Value: Governance of IT Investments : The Val IT Framework 2.0 Extract,* Meadows Illionis, 2008

ITSMF, *Frameworks for IT Management,* Amsterdam 2006

McKinsey and Co., *Managing IT for Scale, Speed and Innovation*, Londra 2006

Preben Jocabsen, *HP's Adaptive Enterprise ITVision,* Kopenhag 2004

PricewaterhouseCoopers, *Governance Survey: From Compliance to Strategic Advantage,* Londra 2004

Sermaye Piyasası Kurulu, *Kurumsal Yönetim İlkeleri* 2. Basım, Ankara 2005

Steve McMillan ve Alicia Dellario, *Linking Business with IT,* Gartner ITxpo sunumu, IBM Corporation 2005

Türkiye Muhasebe Standartları Kurulu, *Finansal Tabloların Hazırlanma ve Sunulma Esaslarına İlişkin Kavramsal Çerçeve Hakkında Tebliğ Sıra No: 1* 16 Ocak 2005 tarih ve 25702 sayılı Resmi Gazete, Ankara www.tmsk.org.tr

TÜSİAD, *Kurumsal Yönetim En İyi Uygulama Kodu: Yönetim Kurulunun Yapısı ve İşleyişi* İstanbul, 2002