TC
YILDIZ TEKNİK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI
İŞLETME YÖNETİMİ YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

BİLGİ SİSTEMLERİ DENETİMİ VE YÖNETİM BEYANI

Mehmet Murat HUYUT
09713021

TEZ DANIŞMANI
Yrd.Doç.Dr. Hayri BARAÇLI

İSTANBUL
2011

TC

YILDIZ TEKNİK ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME ANA BİLİM DALI

İŞLETME YÖNETİMİ YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

BİLGİ SİSTEMLERİ DENETİMİ VE YÖNETİM BEYANI

Mehmet Murat HUYUT
09713021

Tezin Enstitüye Verildiği Tarih: 02.12.2011

Tezin Savunulduğu Tarih: 05.01.2012

Tez Oy birliği / ~~Oy çokluğu~~ ile başarılı bulunmuştur.

	Unvan Ad Soyad	İmza
Tez Danışmanı:	Yrd.Doç.Dr. Hayri BARAÇLI	
Jüri Üyeleri:	Doç.Dr. Ali Fuat GÜNERİ	
	Yrd. Doç. Dr. Ceren ERDİN GÜNDOĞDU	

İSTANBUL

2011

ÖZ

Bilgi Sistemleri Denetimi ve Yönetim Beyanı

Mehmet Murat Huyut

Aralık, 2011

Araştırma çalışmamızın temel amacı; Bilgi Sistemleri Denetimi konusunun önemini, gerekliliğini vurgulamak ve Bankacılık Düzenleme ve Denetleme Kurulu Bilgi Yönetimi Dairesi tarafından 30.07.2010 tarihinde yayınlanan genelge ile bankaların 2011 yılı denetim döneminden itibaren ilk kez hazırlayacakları Yönetim Beyanı ve uygulaması hakkında detaylı bilgi vermek, Yönetim Beyanına mesnet teşkil edecek Bilgi Sistemleri Denetimlerinden örnekler sunmaktır.

Banka yönetim kurulu onayı ardından bağımsız denetçilere sunulacak olan Yönetim Beyanı; bankanın bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontrollerinin Bilgi Sistemleri Denetim dönemi açısından etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, bu çerçevedeki mevcut durum ve yürütülen çalışmalara ilişkin güvence sunacaktır. Yönetim Beyanı konusu akademik bir çalışmaya ilk kez konu olarak alınmış ve literatüre kazandırılmıştır.

Çalışmamızda Yönetim Beyanı hazırlama çalışmaları farklı danışmanlık firmalarının önerileri göz önüne alınarak makul bir metodoloji oluşturulmuş, Yönetim Beyanı kapsamında Bilgi Sistemleri Denetimlerinden Konfigürasyon Yönetimi denetimi örnek olarak yapılmış ve raporlanmıştır.

Anahtar Kelimeler: Yönetim Beyanı, Bilgi Sistemleri Denetimi, Uygulama Kontrolleri, Bilgi Teknolojileri Genel Kontrol Alanları, Bankalarda Bilgi Sistemleri Denetimi

ABSTRACT

Management Declaration and Information Technology Audit

Mehmet Murat Huyut

December, 2011

The main purpose of this thesis is to emphasize the necessity of Information Systems Audit and give detailed information about the implementation of Management Declaration, the circular which published on 30.07.2010, issued by the banks for the first time since the 2011 audit period by Banking Regulation and Supervision Board of Office of Information Management, prepare and provide examples for Declaration of Management's Information Systems Controls.

Following the Bank's board of directors submitted this Management Declaration, it reported to the independent auditors. This framework will provide assurance regarding the current situation and the work conducted the bank's information systems and internal controls related to the processes of banking activity in terms of Information Systems audit period. Management Declaration handle in an academic study firstly and gain it to the literature with this thesis.

In thesis we got consulting firms' preparation of proposals taking into account the different studies and created a reasonable methodology. Amoung Management Information Systems Controls, Configuration Management control whole audit made and reported.

Keywords : Management Declaration, Information Technology Audit, Application Controls, General Information Technology Controls, IT Audit in Banks

ÖNSÖZ

Türkiye Bankacılık sektörünün global krizlerden diğer ülkelerdeki bankalardan daha az etkilendiği tüm ekonomi çevrelerince malumdur. Bunu Türkiye'nin krizler ülkesi olması ve krize bağışıklık kazanmış olan bankacılık sisteminin yeni krizlere karşı güçlü bir savunma sistemine sahip olması şeklinde de yorumlayabiliriz. BDDK tarafından yapılan güçlü mevzuat düzenlemeleri sektörün daha sağlam bir yapıya kavuşmasında en önemli faktörlerdendir.

Yine bu yönde bankaların bilgi sistemlerine yönelik denetim çalışmalarını ve bilgi sistemleri süreçlerine bağımlı tüm bankacılık süreçlerinin denetimini kendi iç denetim sistemlerince denetlenmesi, bunu yıllık olarak sunması ve yönetim kurulu tarafından onaylatması bu konuda olgunluk seviyemizi artırmıştır.

Bilgi Sistemleri Denetimi ve Yönetim Beyanı konusunda yapılan ilk akademik çalışma sırasında yoğun iş temposuna rağmen desteklerini esirgemeyen tez danışmanım İETT Genel Müdürü Sayın Yrd.Doç.Dr.Hayri Baraçlı Hocama, kurul üyelerinin eğitim ve gelişimi için geniş imkanlar sunan KuveytTürk Teftiş Kurulu Başkanı Sayın Bahattin Akça Üstad'a, çeviriler konusunda yardımcı olan Bilgi Sistemleri Müfettişi Sayın Tuğrul Bozbey ve tüm yöneticilerime teşekkürlerimi sunarım.

Hayatım boyunca desteklerini esirgemeyen aileme en içten duygular ile sevgi ve saygılarımı sunarım.

İstanbul, Aralık 2011 **Mehmet Murat Huyut**

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

ISACA : Bilgi Sistemleri Denetimi ve Kontrolü Derneği (Information System Auditing Control Association)

BDDT : Bilgisayar Destekli Denetim Teknikleri

BDDK : Bankacılık Düzenleme ve Denetleme Kurulu

COBIT : Bilgi Teknolojileri Kontrol Hedefleri (Control Objectives for Information and related Technology)

BS : Bilgi Sistemleri

BSD : Bilgi Sistemleri Denetimi

BT (IT) : Bilgi Teknolojileri (Information Technology)

BSD: Bilgi Sistemleri Denetimi

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

SOA(SOX) : Sarbanes Oxley Act

SPK : Sermaye Piyasası Kurulu

TTK : Türk Ticaret Kanunu

ITIL: IT Infrastructure Library - Bilişim Teknolojileri Altyapı Kütüphanesi

ITSM: IT Service Management - Bilişim Teknolojileri Servis Yönetimi

CI: Konfigürasyon Öğesi (Configuration Item **)**

ITGI: Bilgi Teknolojileri Yönetişim Enstitüsü (Information Technology Governance Institue)

ISO: Uluslararası Standartlar Organizasyonu (International Organization for Standardization)

PO : Planlama ve Organizasyon (Plan and Organize)

AI : Tedarik ve Uygulama (Acquire and Implement)

DS : Hizmet Sunumu ve Destek (Delivery and Support)

ME : İzleme ve Değerlendirme (Monitor and Evaluate)

TBB: Türkiye Bankalar Birliği

1. GİRİŞ

Bankacılık sektörü her geçen gün bilişim teknolojilerini daha fazla kullanmaktadır. Hatta bu sektör teknolojiyi kullanan, aynı zamanda yönlendiren ve gelişmesi için girişimlerde bulunan etkin bir sektördür. Mevcut finansal kaynaklarını teknolojik ve inovatif gelişmeler için yönlendirebilen bankalar bu alanda yaptıkları yatırımların karşılığını hızlı bir biçimde alabildikleri ve müşteri odaklı işletmecilik anlayışlarına uygun bir yapı içinde gelişmelerini sağlayabildikleri için bu alanda gelişmelere en açık sektörlerden biri olmaktadır.

Paranın artık data olduğu günümüz mobil para ekonomisi dünyasına bankalar teknoloji sayesinde ayak uydurabilmiştir. Bilgi sistemleri sayesinde saniyede milyonlarca işlem yapılabilir bir hale gelmiştir.

Bilgi teknolojilerindeki hızlı gelişim bankaların mevcut tüm süreçlerini inovatif çözümler ile güncellemelerini sağlamıştır. Bu güncellemeyi yapamayan veya teknoloji atılımında geç adımlar atan bankalar rekabetin üst düzeyde yaşandığı sektörde sıralamaların gerilerinde kalabilmektedirler.

Tüm bu bilgi sistemleri geliştirmeleri günümüz bankacılığını operasyon anlamında ciddi bir şekilde etkilemektedir. Şubedeki bankacılar ancak önündeki ekran el verdiği ölçüde işlem yapabilmektedir. Süreçlerin otomatize olası hataları önemli oranda engellerken mevcut bilgi sistemleri ile sağlanan bu yapının denetlenmesinin önemi artmaktadır.

Bilgi sistemleri denetimi aslında dolaylı olarak tüm bankacılık sistemini denetlemek ile eş olduğunu görebiliriz. Günümüzde bilgi sistemlerine dayalı olmayan yani yazılım, donanım, netwok vb. gereksinimi olmadan yapılabilen bir bankacılık işlemi neredeyse kalmamıştır.

Bu bağlamda günümüz Türkiye Ekonomisinin mihenk taşı durumundaki Bankacılık Düzenleme ve Denetleme Kurulu bilgi sistemleri denetimi konusunda ciddi adımlar atmıştır. İlk kez 2011 yılı için tüm bankalar tarafından hazırlanması gereken, Yönetim kurulu tarafından onaylanmış "Yönetim Beyanı" hazırlanması gerektiği, 13 Ocak 2010 Tarih ve 27461 sayılı Resmi Gazete'de "Bağımsız Denetçiler tarafından

Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik " Madde 33 de açıklanmaktadır. (Yönetmelikte Değişiklik Yapan 7/2011 tarihli, 27270 sayılı Resmi gazete ile güncellenmiş, madde değişmemiştir.)

> MADDE 33 – (1) Banka, bilgi sistemleri ve bankacılık süreçleri üzerindeki iç kontrolleri hakkında denetim dönemi itibariyle yönetim kurulu tarafından düzenlenen yönetim beyanını denetçiye sunar.
>
> (2) Denetçi, denetim görüsünü oluştururken yönetim beyanını ve bu beyana mesnet teşkil eden çalışmaları inceler. Denetçi, bu inceleme sonucunda beyanda eksiklik veya yanlışlık tespit ederse denetim raporunda bu tespitlere yer verir.
>
> (3) Denetlenen yönetim kurulunun yönetim beyanını vermeyi reddetmesi durumunda, BSD raporunu imzalamaya yetkili kişiler şartlı görüş bildirebilir, görüş bildirmekten kaçınabilir veya 34 üncü maddede belirlenen usul ve esaslar çerçevesinde denetimden çekilmek için yetkili kuruluş yönetimine teklifte bulunabilirler. Yetkili kuruluşun çekilme kararı alması halinde durum gerekçeleri ile birlikte en geç yedi gün içinde Kuruma bildirilir.
>
> (4) Bu Yönetmelik kapsamında yönetim beyanına ve uygulanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Yönetim Kurulu tarafından düzenlenmesi gereken Yönetim beyanı 2011 yılı için tüm bankalarda olanca hızıyla ilk kez hazırlanmaktadır. Bu Beyanın hazırlanmasında Yönetim Kurulunun görevlendirmesi ile Bankaların Teftiş Kurulu ve İç Kontrol Başkanlıklarına büyük görevler düşmektedir.

Türkiye'de ilk kez yapılan Yönetim Beyanı üzerine, ilk kez akademik bir çalışma yapılmaktadır. Bu alandaki bilgi eksikliğini gidermesi açısından hazırlanan çalışma önem arz etmektedir. Tez; Bilgi sistemleri denetimi ve Yönetim Beyanı konusunda bilgiler verip örnek bir bilgi sistemleri sürecinin Yönetim Beyanı Kapsamında denetimi çalışması ile tamamlanmaktadır.

2. Bankacılıkta Bilgi Sistemleri (BS) ve Denetim Gereksinimi

Bankacılık bilgi sistemleri ve denetimini incelemeden önce kavramları açıklık getirmek gerekmektedir. Denetim, Bilgi Sistemleri, Bilgi Teknolojileri gibi kavramları sırasıyla açıklayacak olursak;

2.1. Denetimin Tanımı

Denetim kavramı insanlık tarihi kadar eski olmakla birlikte yapılan bir işin kontrol edilmesi olarak kısaca açıklanabilir. Bir Alman atasözünde "Güven ama Denetle" ifadesi güven duygusunun yanında her zaman denetimin gerekli olduğunu açıklamaktadır. Aslında Denetimin güven artırıcı bir eylemdir. Denetlenen iş yada süreç işin doğruluğunu teyit veya özelliklerinin, kalitesinin uygunluğunu kontrol etme gibi bir çok amacı içerebilir. Bilgi Sistemleri Denetimi konusu yeni bir konu olmasına rağmen Denetim konusu oldukça eski bir konudur. Tarihi hakkında Ali Kamil Uzun makalesinde şu şekilde bilgiler vermiştir.

> Auditing veya meslek unvanı olarak "auditor" ilk defa 1289 yılında İngiltere'de kullanılmıştır. Bu kelime Latince audire kelimesinden türetilmiş olup, dinlemek anlamına gelmektedir.
>
> Eski Mısır ve Roma'da işyeri adına yapılan tahsilat ve ödemeler bir uzman, bilge kişiye okunur, anlatılırdı. Bu kişi tahsilat ve ödemeleri tek tek dinler ve onların uygun olup olmadığına karar verir, audit ederdi. Profesyonel denetçiliğin ilk örgütü de Venedik'te 1581 yılında kurulmuştur. 1850'li yıllarda "İskoçya Fermanlı Muhasebeciler Enstitüsü" ile modern muhasebe denetim standartları yazılı hale getirilmiştir. İngiltere'den Amerika'ya göç eden muhasebeciler 1886 yılında New York'ta Diplomalı Kamu Muhasipleri Kanunu'nun çıkarılmasını sağlamıştır.
>
> Sanayi devrimiyle birlikte iş hayatındaki gelişmeler, profesyonellere yetki devrini uygulamaya sokmasıyla birlikte, iç denet im mesleğinde önemli gelişmelerin sağlanmasını da beraberinde getirmiştir. Önceleri sadece muhasebe ve işletme varlıklarının korunması ile görevlendirilen iç denetçiler sonraki yıllarda uygunluk denetimi, risk değerlemesi gibi alanlarda da görev alarak mesleğin çalışma alanının gittikçe genişlemesine yol açmış ve kurumsallaşmış işletmelerin ayrılmaz bir parçası halini almışlardır.[1]

[1] Ali Kamil Uzun, "Organizasyonlarda İç Denetimin Fonksiyonu ve Önemi", **Active Bankacılık ve Finans Dergisi**, s.6, (1999):2.

Türk Dil Kurumu'na göre denetleme, bir görevin yolunda yürütülüp yürütülmediğini anlamak için yapılan araştırma, denetim, bakı, teftiş, murakabe, kontrol anlamına gelmektedir.[2]

Melih Erdoğan denetimin tanımını şu şekilde yapmaktadır; "Denetim, ekonomik faaliyetler ve olaylara ilişkin savlarla, kabul edilmiş ölçütler arasındaki uygunluğun derecesini araştırmak ve sonuçlarını ilgili kullanıcılara iletmek amacıyla, nesnel biçimde kanıt toplayan ve değerleyen sistematik bir süreçtir."[3]

Ersin Gürerdin'in benzer bir tanımı "Denetim, iktisadi faaliyet ve olaylarla ilgili iddiaların önceden saptanmış ölçütlere uygunluk derecesini araştırmak ve sonuçları ilgi duyanlara bildirmek amacıyla tarafsızca kanıt toplayan ve bu kanıtları değerleyen sistematik bir süreçtir." [4]

[2] Türk Dil Kurumu, http://www.tdk.gov.tr [11.10.2011]
[3] Melih Erdoğan, **Denetim**, 2.bs, (Ankara: Maliye ve Hukuk Yayınları , 2005) ,1.
[4] Ersin Güredin; **Denetim ve Güvence Hizmetleri**, 11.bs, (İstanbul :Arıkan Yayınları, 2007),11.

2.2. Bilgi Sistemleri

Bilgi; toplanmış, organize edilmiş, yorumlanmış ve belli bir yöntemle etkin karar vermeyi gerçekleştirmek amacıyla ilgili birime iletilmiş, belirli bir amaç doğrultusunda süreçlenen, yararlı biçime dönüştürülmüş ve kullanıcıya değer sağlayan verilerdir. Bilgi, çoğulculuğu, çeşitliliği, kurum içi etkileşimleri ve organizasyon faaliyetlerinin mantıksal arka planını oluşturmaktadır. Ünlü savaş uzmanı Napolyon'a göre, doğru bilgiyi doğru zamanda temin etmek savaşın onda dokuzunu kazanmak demektir.[5]

Bilgi sistemleri, bir organizasyonda karar vermeyi, koordinasyon ve kontrolü sağlamak amacıyla bilginin toplanması, işlenmesi, saklanması ve dağıtılmasını sağlayan birbirleriyle ilişkili bileşenlerin bütünüdür.[6]

Bilgi sistemleri kurumsal başarı açısından yaşamsal rol oynamaktadır. Bilgi sistemlerinde teknoloji ve insanın birlikte çalıştıkları unutulmamalıdır. Yeni bir bilgi sistemi yüzeysel bir donanım ve yazılım değişikliğinden çok, bir teknoloji-insan uyumu projesi olarak algılanmalıdır.[7]

Bilginin amacı, gelecekte ortaya çıkabilecek bir olay ya da durumla ilgili olarak belirsizliği azaltmak iken, bilgi sistemlerinin hedefi, en genel anlamda karar alma sürecinde gereksinim duyulan bilgileri sağlamaktır. Bilgi sistemleri, kurumsal etkinlik, rekabetçi üstünlük, nitelikli hizmet sunumu gibi amaçları gerçekleştirmeye yönelik bilgileri gerektiği zaman, arzulanan formda ve nitelikte sunabilmektir. [8]

Bilgi sitemleri bilgi toplama, işleme, saklama, sınıflama ve dağıtımı için güncel teknolojik gelişmeleri izlemiştir. Bilgi Sistemleri çoğu kez Bilgi Teknolojileri ile karıştırılır olmuştur. Konuşma dilinde birbirini yerlerine kullanılan kelimeler haline gelmişlerdir. Bilgi Toplamak için bilgisayar programları yazılım araçları geliştirilmiş, özel donanımlar üretilmiştir. Bunlar en basitinden kelime işlemci programından, istatiksel analizleri tek tıkla yapan gelişmiş yazılımlara kadar geniş bir yelpazede

---

[5] Şerif Şimşek, **Yönetim ve Organizasyon**, (Konya: Günay Ofset, 2002),408.
[6] Kenneth C. Laudon, Jane P. Laudon, **Management Information Systems : Managing The Digital Firm,** 7.bs (USA:Prentice Hall, 2001),12.
[7] M. Levent Demircan, Moltay, C. Arda, **Bilgiyi Yönetmek**, (İstanbul :Beta Basım Yayım Dağıtım A.Ş,1997),59.
[8] Kate Behan, , Holmes, Diana, **Understanding Information Technology**, 2.bs, (New York:Prentice Hall Inc.,1990),1.

sunulmaktadır. Geliştirilen donanımlar ile daha hızlı ve doğru bilgi elde edilmektedir. Alınan bu bilgiler daha uzun süre hasar görmeden saklanabilmektedir. Sınıflama işlemleri ise kullanılan yazılımlar ile bir kaç tıklama ile doğruluk oranı yüksek bir biçimde yapılabilmektedir. Dağıtım işlemleri gelişen Network ağı ile istenen mekana istenen zamanda yüksek güvenlik önlemleri ile yapılabilmektedir. Tüm bu Teknolojik gelişmeler Teknoloji yönetiminin önemini ortaya koymaktadır. Teknoloji Yönetimi "Bir organizasyonun stratejik ve taktik amaçlarının şekillendirilmesinde ve bunlara ulaşılmasında ihtiyaç duyulan teknolojik kapasitenin planlanması geliştirilmesi ve uygulanmasıdır."[9]

Sayılan tüm bu Bilgi sistemleri operasyonları günümüz dünyasında Bilgi Teknolojileri kullanılarak yapılabilmekte ve bu açıdan birbirilerinin yerini tutabilen anlamlar çıkarılabilmektedir.

Bilgi sistemleri ile hayatın her alanında verimli ve etkin fonsiyonlar oluşturulabilmektedir. Bankacılık alanında da insanlığın faydasına sunulan birçok hizmet bulunmaktadır.

[9] Yrd.Doç.Dr.Hayri Baraçlı, "Kriz ve Teknoloji Yönetimi", **3Gen Dergisi**, (2001).

2.3. Bankacılık ve Bilgi Sistemleri

Banka işletmeleri çeşitli uzmanlıkların karmaşık eşgüdümüne gereksinim duydukları kadar, teknolojik gelişmelere de gereksinim duymaktadırlar. Sektörde önemli bir rekabet söz konusudur. Günümüzde bilginin elektronik ortamlarda saklanılarak kullanılması yaygınlaşmıştır.[10]

Bankalar bilgi sistemlerini kullandıkları oranda büyüyebilmekte ve gelişmelerini hızlandırabilmektedirler. İşlem maliyetlerini, operasyonel giderlerini bilgi sistemleri ile düşürmeye çalışmakta aynı zamanda hızlı ve standart hizmeti tüm müşterilerine sunabilmektedirler. Sunulan hizmetin kalitesi her geçen gün artmakta ve bu şekilde hizmet kalitesinin artmasında bilgi sistemleri kullanımı önemli bir faktör olarak bulunmaya devam etmektedir. Tüm bu faydalar bankaların örgüt yapıları içersine bilgi sistemleri yapılanmaları oluşumunu sağlamıştır. Bankacılık ve bilgi sistemleri giderek ayrılmaz bir bütün haline gelmiştir.

Bir banka işletmesinin örgüt yapısı içinde bilgi işlem hizmetleri veren birimlerin yer alması, beraberinde 'bilgi işlem personeli' olgusunu da gündeme getirmektedir. Bilgi işlem personeli görevleri açısından dört grupta tanımlanabilir. Bunlar, yazılım, işletim, donanım ve idari personel gruplarıdır.

• Yazılım grubunda yer alan personel; sistem çözümleyici, sistem programcısı, analist programcı, uzman programcı, uygulama programcısı, yardımcı programcı, veri tabanı sorumlusu, veri tabanı yönetim sistemi uzmanı,

• İşletim grubunda, operasyon şefi, sistem operatörü, veri kayıt operatörü, yardımcı operatör, vardiya sorumlusu, veri iletişim uzmanı, network operatörü,

• Donanım grubunda; donanım bakım mühendisi, donanım bakım teknisyeni, donanım bakım teknisyen yardımcısı,

[10]Fatih Aydoğdu , "Bankacılık Sektöründe Kurum Kimliğinin Oluşumunda Yeni İletişim Teknolojilerinin Kullanımı: Türkiye İş Bankası Örneği" (Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Anabilim dalı, 2010),11.

• İdari personel; koordinatör, daire başkanı, grup müdürü, müdür, müdür yardımcısı, şef, şef yardımcısı, memur gibi unvanlarla görev yaparlar.[11]

Yukarıda geçen tüm bu bilgi sistemleri gereksinimlerini karşılamak için kurulan insan kaynakları gün geçtikçe büyümekte ve artan ihtiyaçları alanında uzman ve yetkin kişilerce gerçekleştirmektedir. Bilgi sistemleri karşılama maliyetleri oluşturulan yetkin personelin istihdamı ve birimlerin giderleri yüksek de olsa oluşturulan yapıların getirileri ile karşılaştırıldığında önemli bir yatırım olduğu ve giderlerini karşılamakta olduğu görülebilir.

Bilgi çağında artık bilgiye çok kısa sürede en doğru biçimde erişmek bilgi sistemleri sayesinde mümkün olmuştur. Müşterilerin bankacılık hizmetlerini evlerine kadar alabilmelerini sağlayan neredeyse tüm bankacılık hizmetlerine Dünya'nın her yerinden her saatte ulaşabilmelerine olanak tanıyan İnternet bankacılığı bankaların her kişisel bilgisayarda birer şube açmış gibi hizmet verebilmelerini sağlamaktadır. Bu hizmetin her müşteriye oldukça makul hizmet bedelleri ile sunulması yüksek müşteri memnuniyetini ve hizmet kalitesini ortaya koymaktadır.

Ana bankacılık uygulamaları yanında mobil ve internet bankacılığı da son yılların gözde bankacılık hizmetleri arasındadır. Türkiye Bankalar Birliği Haziran 2011 istatistikleri bilgileri ışığında Bankacılık sektöründe Bilgi sistemlerinin milyonların hizmetini karşılamakta olduğunu net bir şekilde görebiliriz. İstatistiklerin oluşturulmasında verilerinden yararlanılan bankaların listesi Ek 1. İnternet bankacılığı istatistikleri gönderen bankalar ekinde açıklanmaktadır.

[11] age,12.

2.3.1. Türkiye'de İnternet ve Mobil Bankacılık

Türkiye Bankalar Birliği tarafından İnternet ve Mobil Bankacılık istatistikleri ismi ile yayınlanan veriler; İnternet bankacılığı yapmak üzere sistemde kayıtlı olan ve en az bir kez giriş işlemi yapmış toplam bireysel müşteri sayısı, Haziran 2011 itibariyle, 16,7 milyon olmuştur. Son bir yıl içerisinde en az bir kez giriş işlemi yapmış toplam bireysel müşteri sayısı ise 8,8 milyon kişidir.

Nisan-Haziran 2011 döneminde 6,7 milyon bireysel müşteri en az bir kez internet bankacılığı giriş işlemi yapmıştır. Bu miktar, toplam kayıtlı bireysel müşteri sayısının yüzde 40'ını oluşturmaktadır. Nisan-Haziran 2011 döneminde, aktif bireysel müşteri sayısında bir önceki yılın aynı dönemine göre 1.196 bin kişi, bir önceki üç aylık döneme göre ise 216 bin kişi artış olmuştur.[12]

Tablo 1: İnternet Bankacılığını Kullanan Müşteri Sayısı Kaynak: TBB

	Haziran 2010	**Mart 2011**	**Haziran 2011**
Bireysel müşteri sayısı (bin kişi)			
Aktif (A) *(son 3 ayda 1 kez login olmuş)*	5.524	6.505	6.721
Kayıtlı (B) *(en az 1 kez login olmuş)*	13.621	16.253	16.696
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	7.248	8.498	8.764
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**41**	**40**	**40**
Kurumsal müşteri sayısı (bin kişi)			
Aktif (A) *(son 3 ayda 1 kez login olmuş)*	624	723	751
Kayıtlı (B) *(en az 1 kez login olmuş)*	1.459	1.697	1.767
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	729	860	887
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**43**	**43**	**43**
Toplam müşteri sayısı (bin kişi)			
Aktif (A) *(son 3 ayda 1 kez login olmuş)*	6.149	7.227	7.472
Kayıtlı (B) *(en az 1 kez login olmuş)*	15.080	17.950	18.463
Kayıtlı (C) *(son 1 yılda en az 1 kez login olmuş)*	7.978	9.358	9.652
Aktif (A) / kayıtlı (B) müşteri oranı (yüzde)	**41**	**40**	**40**

[12]"İnternet ve Mobil Bankacılık İstatistikleri Haziran 2011" , Türkiye Bankalar Birliği, http://www.tbb.org.tr/tr/Banka_ve_Sektor_Bilgileri/Linkler.aspx?RId=1029 [18.10.2011].

İnternet bankacılığı yapmak üzere sistemde kayıtlı olan ve en az bir kez giriş işlemi yapmış kurumsal müşteri sayısı Haziran 2011 itibariyle, yaklaşık 1,8 milyon kişidir. Bunların 751 bini (yüzde 43'ü) Nisan-Haziran 2011 dönemi içerisinde en az bir kez giriş işlemi yapmıştır. Son bir yıl içerisinde en az bir kez giriş işlemi yapmış kurumsal müşteri sayısı ise 887 bin kişidir.

İnternet bankacılığı için kayıt yaptıran ve en az bir kez giriş işlemi yapmış toplam (bireysel ve kurumsal) müşterilerin yüzde 40'ı Nisan-Haziran 2011 döneminde en az bir kez internet bankacılığı işlemi yapmıştır. Nisan-Haziran 2011 döneminde, toplam aktif müşteri sayısında bir önceki yılın aynı dönemine göre 1 milyon 323 bin kişi, bir önceki üç aylık döneme göre ise 244 bin kişi artış olmuştur.

Türkiye'nin genç nüfusu İnternet okur yazarlığı oldukça yüksektir. Bilişim teknolojileri gençler tarafından yakından takip edilmektedir. Türkiye İstatistik Enstitüsünün yayınladığı verilerden de görüldüğü üzere artan sayıda internet bankacılığı kullanımı görülmektedir. Bu sayılardaki artış bankaların sunabildikleri hizmet çeşitlerinin giderek artması ve bankaların internet şubelerine olan güvenin atmasına paralel olduğu söylenebilir.

Gerekli güvenlik önlemlerini sanal ortamda sağlayabilen bankalar neredeyse tüm bankacılık uygulamalarını internet ve mobil bankacılık üzerinden gerçekleştirebilmektedirler.

Aşağıdaki detaylı verilerde de günümüzün yüksek teknoloji ürünleri olan ve maliyetleri her geçen gün düşen cep telefonlarının 3G veya GPRS gibi operatörlerin internet hizmeti sunması ile cep telefonlarının gelişen mobil internet tarama yetenekleri her geçen gün mobil bankacılık uygulamalarının kullanımlarını artırmaktadır. Bu artışta da teknolojik gelişimin payı büyüktür. Büyüyen cep telefonları ekranları kullanıcı dostu ara yüzler ve basit anlaşılır yapıda hizmet sunumu mobil yazılımların ve çeşitli uygulamaların kullanımını her geçen gün artırmaktadır.

Tablo 2: İnternet Bankacılığı Müşteri Sayıları (Kaynak TBB)

Dönem	Sistemde kayıtlı, en az bir kez login olmuş müşteri sayısı	Sistemde kayıtlı, son 1 yıl içinde en az bir kez login olmuş müşteri sa-yısı	Aktif müşteri sayısı	Sistemde kayıtlı, en az bir kez login olmuş müşteri sayısı	Sistemde kayıtlı, son 1 yıl içinde en az bir kez login olmuş m. sayısı	Aktif müşteri sayısı	Sistemde kayıtlı, en az bir kez login olmuş müşteri sayısı	Sistemde kayıtlı, son 1 yıl içinde en az bir kez login olmuş müşteri sa-yısı	Aktif müşteri sayısı
Haziran 2010	13,621,487	7,248,242	5,524,461	1,459,006	729,266	624,371	15,080,493	7,977,508	6,148,832
Eylül 2010	14,827,760	7,725,302	5,715,626	1,571,923	786,972	637,145	16,399,683	8,512,274	6,352,771
Aralık 2010	15,608,554	7,974,788	6,038,342	1,614,365	813,721	655,490	17,222,919	8,788,509	6,693,832
Mart 2011	16,252,954	8,497,721	6,504,651	1,696,649	860,142	722,811	17,949,603	9,357,863	7,227,462
Haziran 2011	16,696,199	8,764,170	6,720,661	1,767,095	887,371	751,120	18,463,294	9,651,541	7,471,781

Tablo 3: İnternet Bankacılığı İşlem Hacmi (Milyon TL) (Kaynak TBB)

Dönem	İşlem Hacmi (Milyon TL)					
	Fatura ödemeleri	Vergi ödemeleri	SSK ve Bağ-kur prim ödemeleri	Kredi ödemeleri	Diğer ödemeler	Toplam
Haziran 2010	1,216	4,304	706	401	212	**6,838**
Eylül 2010	1,377	4,675	749	463	262	**7,525**
Aralık 2010	1,744	4,978	852	530	431	**8,535**
Mart 2011	2,112	7,195	928	603	655	**11,494**
Haziran 2011	2,099	6,844	1,150	776	800	**11,669**

Mobil bankacılık yapmak üzere sistemde kayıtlı olan ve en az bir kez giriş işlemi yapmış müşteri sayısı Haziran 2011 itibariyle, yaklaşık 992 bin kişidir. Bunların 248 bini (yüzde 25'i) Nisan-Haziran 2011 dönemi içerisinde en az bir kez giriş işlemi yapmıştır. Son bir yıl içerisinde en az bir kez giriş işlemi yapmış mobil bankacılık müşteri sayısı ise 431 bin kişidir.

Nisan-Haziran döneminde mobil bankacılık ile gerçekleştirilen 143 bin adet yatırım işleminin hacmi 841 milyon TL olmuştur.

Nisan-Haziran 2011 dönemi itibariyle, mobil bankacılık hizmeti kullanılarak yapılan yatırım işlemleri dışındaki finansal işlemlerin toplam adedi 1,3 milyon, tutarı ise 1,5 milyar TL olmuştur. EFT, havale ve döviz transferi işlemlerini kapsayan para transferleri işlemleri, yatırım işlemleri dışındaki finansal işlem hacminin yüzde 89'unu oluşturmuştur.

Tablo 4: Mobil Bankacılık 2011 verileri (Kaynak: TBB)

Dönem	**Mobil Bankacılık**		
	Sistemde kayıtlı, en az bir kez login olmuş müşteri sayısı	**Sistemde kayıtlı, son 1 yıl içinde en az bir kez login olmuş müşteri sayısı**	**Aktif müşteri sayısı**
Mart 2011	912,788	398,275	230,353
Haziran 2011	992,017	430,563	247,910

Tablo 5: Kredi Kartı İşlemleri (Kaynak: TBB)

Dönem	İşlem Adedi (Bin)				İşlem Hacmi (Milyon TL)			
	Nakit Avans	Kendi kartına borç ödeme	Başkasının kartına ait borç ödeme	Toplam	Nakit Avans	Kendi kartına borç ödeme	Başkasının kartına ait borç ödeme	Toplam
Haziran 2010	450	6,346	660	**7,457**	240	4,522	665	**5,427**
Eylül 2010	401	6,593	696	**7,690**	183	4,935	687	**5,806**
Aralık 2010	451	6,984	767	**8,203**	200	5,157	842	**6,199**
Mart 2011	421	7,164	576	**8,160**	277	5,381	715	**6,373**
Haziran 2011	430	7,157	597	**8,184**	245	5,619	766	**6,630**

Android, iOS, Symbian gibi gelişmiş işletim sistemlerine sahip mobil araçlara özel geliştirilmiş bankacılık uygulamaları ücretsiz olarak indirilerek istenen bankaların küçük birer örneği cep telefonlarına kurulabilmektedir. Tüm bu yükselen trend Bankacılıkta teknoloji denetimi ve yönetimin önemini açıkça ortaya koymaktadır.

2.4. Bilgi Sistemleri Denetimi

Bilgi Sistemleri denetimi, insanlık hayatını kolaylaştıran tüm Bilgi Teknoloji araçlarının, Bilgi sistemleri araştırma, geliştirme, yönetim metodolojilerinin sistematik bir biçimde incelenmesi, kontrol noktaları oluşturarak planlanan ve gerçekleşen tüm Bilgi sistemi bileşenlerinin olması gerektiği gibi değil nasıl daha iyi olabileceği bakış açısıyla kontrol edilmesi ile ilgili tüm süreçleri kapsar.

Bddk ya göre Bilgi Sistemleri Denetimi; "Bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ve bankacılık faaliyetlerine ilişkin süreçler ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreçtir"[13] şeklinde tanımlanmaktadır.

Necip Polat Yönetim Bilgi Sistemi ile ilgili tanımları Sayıştay dergisinde şu şekilde ifade etmiştir;

> "Veri; "datum" sözcüğünün çoğulu olan "data" kelimesinin karşılığı olarak kullanılan bir kavram olup işlenmemiş, bir sonuca varabilmek için gerekli olan ilk bilgi, ham bilgiyi ifade etmektedir. Veri, çeşitli olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimde gösterimidir.
>
> *Bilgi;* verilerin kurallardan yararlanılarak işlenmiş şekli, anlamlı sonuçlarıdır. Diğer bir ifadeyle, verilerin değer kazandırılmış biçimidir. Bilginin üç temel boyutu vardır: Zaman, içerik ve biçim.
>
> *Sistem;* girdiler alıp çıktılar oluşturan, organize bir dönüşüm süreciyle ortak bir amaca yönelik, beraber çalışan ve birbirine bağlı parçalar topluluğudur. Sistemin elemanları girdi, süreç, çıktı, geri besleme ve denetimdir.[14]
>
> *Bilgi Sistemi;* veri kaynaklarını girdi olarak alıp süreçten geçiren ve çıktı olarak bilgi ürünlerini ortaya çıkaran sistemdir. Bilgi sistemleri; veri işleme sistemleri, yönetim bilgi sistemleri, karar destekleme sistemleri, ofis otomasyon sistemleri olmak üzere dörde ayrılabilir."[15]

Örnek olarak, hastane yönetim sistemi, coğrafi bilgi sistemi verilebilir.

---

[13] Bddk, Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik, .07/2011-27270,Md.21

[14] Necip Polat, "Yönetim bilgi sistemi ve Sayıştay'da yürütülen çalışmalar",Sayıştay Dergisi, c.65, http://dergi.sayistay.gov.tr/icerik/der65m14.pdf [21.11.2011]

[15] Christopher Martin, Philip Powell, **Information Systems**, (London: McGraw-Hill, 1991),9.'den aktaran Necip Polat, "Yönetim bilgi sistemi ve Sayıştayda yürütülen çalışmalar",**Sayıştay Dergisi**, c.65, http://dergi.sayistay.gov.tr/icerik/der65m14.pdf [21.11.2011]

Bilişim sistemleri denetimi, "bir bilişim sisteminin, kurum amaçlarına etkin bir şekilde ulaşılmasını, kaynakların verimli kullanılmasını, varlıkların korunmasını ve veri bütünlüğünün sürdürülmesini sağlayacak şekilde tasarlanıp tasarlanmadığını tespit etmeye yönelik kanıt toplama ve değerlendirme süreci"[16] olarak tanımlanmaktadır.

Günümüzdeki iş ortamı, iç denetimden risklerin yanı sıra fırsatları da ortaya koymasını beklemektedir. Gelişen teknoloji bu konuda önemli avantajlar sunmaktadır. Bu nedenle hem iç denetçiler hem de teknoloji firmaları ortak bir görüşte birleşmektedir : "İç denetim, teknoloji ile entegre olmalıdır." [17]

International Organization of Supreme Audit Institutions (INTOSAI) Bilişim sistemleri denetimini, bilişim teknolojisinin gelişimine ve kurumlarda kullanım düzeyine paralel olarak üç şekilde yapılabilmektedir:[18]

- Bilgisayar çevresinde denetim
- Bilgisayarlı denetim
- Bilgisayarın içinde denetim.

2.4.1. Bilgisayar çevresinde denetim

Bilişim teknolojilerinin kurumlar tarafından kullanılmaya başlandığı ilk yıllarda, birçok işlem bilişim teknolojileri ile birlikte manuel olarak da yapılmaktadır. Burada denetçiler denetim izini, bilgisayara giren kaynak dokümanlardan elde edip bilgisayardan çıkan dokümanla karşılaştırarak, kayıtları takip ederek ihtiyaç duyulan kanıtları manuel olarak elde etmektedir. Bu yöntemde, denetçiler bilgisayara girilen veriler ve ürettiği çıktılarla ilgilendiği halde, bilgisayarın kendisi ile ilgilenmemektedir.[19]

---

[16] Weber, R., **Information Systems Control and Audit**, 1999, Akt. ASOSAI, IT Audit Guidelines, ASOSAI Research Project, Eylül 2003.'den Aktaran Özcan Rıza Yıldız, "Bilişim Sistemleri Denetimi ve Sayıştay", **Sayıştay Dergisi**, s.65,(2007):176, http://dergi.sayistay.gov.tr/default.asp?sayfa=4&id=65 [24.11.2011]

[17] Ali Kamil Uzun, "İç Denetim Fonksiyonunu Değiştiren Unsur : Teknoloji", Active Bankacılık ve Finans Dergisi, Kasım-Aralık 2001, No: Active Activity SAS e-risk & e-denetim, s.1.

[18] INTOSAI Geliştirme Girişimi (IDI), **Intorduction of IT Audit e-learning Course Notes**, (2007):5'den Aktaran, Yıldız, age. 176

[19] Özcan Rıza Yıldız, "Bilişim Sistemleri Denetimi ve Sayıştay", **Sayıştay Dergisi**, s.65,(2007):176, http://dergi.sayistay.gov.tr/default.asp?sayfa=4&id=65 [24.11.2011]

2.4.2. Bilgisayarlı denetim

Bilişim sistemlerini yaygın olarak kullanan ve işlemlerini daha az manuel olarak yürüten kurumlarda, bu sistemdeki verileri araştırmak, karşılaştırmak, analiz etmek ve değişik test türlerini uygulamak veya veriler üzerinde matematiksel hesaplamalar yapmak için bilgisayar kullanılmaktadır. Denetimde etkinliği ve verimliliği önemli ölçüde arttırmak için kullanılan bu tekniklere sıklıkla bilgisayar destekli denetim teknikleri denmektedir.[20]

2.4.3. Bilgisayarın içinde denetim;

Manuel olarak üretilen çıktıların minimuma indiği, kurumun bütün bilgileri ve iletişiminin bilişim teknolojileri aracılığıyla sağlandığı karmaşık ve büyük sistemlerin denetimine ilişkin olarak kullanılan bu yöntemde, bilgisayar, sistem içinde var olan işlem mantığını, var olan kontrol mekanizmalarını ve sistem tarafından üretilen kayıtları test etmek için kullanılmaktadır. Denetçi, sistem tasarımı ve sistemin geliştirilmesinde de belli görevler üstlenmektedir. [21]

Eski Sayıştay Başkanı Sn. Mehmet Damar 2003 yılı Hazine Bilişim Sistemleri Denetim Raporu Sunuş yazısında Bilgi Sistemleri Denetiminin gerekliliğini şu şekilde açıklamaktadır;

"Kamu kurumları faaliyetlerinin büyük bir kısmını gerçekleştirirken bilgisayarlardan yararlanmaktadırlar. Bu gelişim, işlemlerin daha hızlı ve etkin bir şekilde yapılmasına imkan tanımaktadır. Ancak, bilgisayarların kullanımı, önceden göz önünde gerçekleştirilen işlemleri sanal ortama taşıdığından, bunların izlenmesi güçleşmekte ve yeni bir risk faktörü oluşturmaktadır." [22]

Sadece Kamu kurumları değil özel sektör de gün geçtikçe faaliyetlerinin büyük bir kısmını bilgi teknolojilerinden faydalanarak yapmaktadırlar. Bu bağlamda Bilgi Sistemleri denetimi her geçen gün önemini artırmaktadır.

---

[20] age.176
[21] age.176
[22] "Hazine Bilişim Sistemleri Denetimi Raporu",
http://www.sayistay.gov.tr/rapor/hazine/diger/Hazine_Bilisim_Sistemleri_Raporu.pdf [26.11.2011]

Bilgi Sistemi denetimi yapan kişilere Bilgi Sistemleri Denetçisi şayet bu kişi ilgili işletmelerin Teftiş kurulunda çalışıyor ise Bilgi Sistemleri Müfettişi gibi isimler almaktadır.

Sayıştay Uzman Denetçisi Özcan Rıza Yıldız meslek unvanlarını Sayıştay dergisi makalesinde şu şekilde açıklamaktadır;

> "Bilişim teknolojisindeki gelişmeye ve denetçilerin çalışma ortamları ve bilgisayar ile ilişkilerine göre bu denetimin isimlendirilmesi de zamanla değişmiştir. Önceleri bu denetim, "Bilgisayar Denetimi" (Computer Audit), "Elektronik Veri İşleme Denetimi" (Electronic Data Processing (EDP) Audit) olarak adlandırılırken, daha sonra "Bilgi Teknolojilerinin Denetimi" (Information Technology (IT) Audit) ve "Bilişim Sistemlerinin Denetimi" (Information Systems (IS) Audit) olarak adlandırılmaya başlanmıştır. Bilişim sistemlerine ilişkin kontrollerin değerlendirilmesinin bilişim teknolojisinin kendine özgü özellikleri nedeniyle, bu konuda belirli düzeyde bilgi birikimi olan kişiler eliyle yerine getirilmesi gerektiği açıktır. Geçmişte ve hatta günümüzde bazı kurumlarda böyle uzmanlar, bilgisayar denetçisi (computer auditor), bilgi işlem denetçisi (EDP auditor) olarak adlandırılmaktadır. Ancak günümüzde birçok kurumda bu uzmanlar bilişim sistemleri denetçisi (IT or IS auditor) olarak nitelendirilmektedir."[23]

Bu unvanlara sahip nitelikli insan kaynakları uygulayacakları denetimler ile ilgili güncel kanun, yönetmelik ve mevzuatı yakından takip etmelidir. Çalışmalarını unvanları haklarında görev ve sorumlulukları işletmelerde farklılıklar gösterse de temel olarak kullandıkları metodoloji aynıdır.

[23] age.177

2.5. Bankaların Denetlenmesi

Bankaların Denetlenmesinin önemini Bülent Şenver şu şekilde açıklamaktadır;

> "Bankalar finans sisteminin temel taşlarıdır. Bankaları sağlıklı olmayan ülkelerin ekonomilerinde istikrarlı kalkınma sağlanamaz, halkın refah düzeyi sağlıklı gelişemez. Yabancı sermaye bu tür ülkelere uzun vadeli, kalıcı yatırımlar yapmaz. Böyle ülkelerin başı mali dertlerden kurtulmaz." [24]

Yukarıdaki paragraf bankaların ülke ekonomisi için önemini kısa ve öz olarak ifade etmektedir. İş bu önemine binaen bankaların denetlenmesi büyük önem arz etmektedir.

Son on yıl içerisinde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim dünyamızı yeni bir çağa taşırken, kamu ve özel sektördeki tüm kurumları da bu değişime ayak uydurmak zorunda bırakmıştır.

Verilere kolay ulaşım, kolay ve rahat iletişim, verimlilik ve etkinliği arttırma gibi konularda sunduğu yeni imkânlar nedeniyle başta finans, medya, eğitim olmak üzere hemen her alanda bilişim teknolojisinin kullanımı giderek yaygınlaşmaktadır. Bugün geldiğimiz noktada bir kurumun varlığını sürdürmesinin artık büyük ölçüde bilişim teknolojilerinden yararlanmasına bağlı olduğu bir gerçekliktir. [25]

Bu değişime en hızlı biçimde ayak uyduran sektör kuşkusuz Bankacılık sektörüdür.

Milli Prodüktivite Merkezi Bankaların denetimlerinin kaynaklandığı genel nedenleri şöyle sıralamıştır;[26]

-Ekonomideki kaynak ve gelir dağılımını etkileyebilmeleri,

-Kaydi para yaratarak ekonomideki para hacmini artırma ya da azaltma gücüne sahip olmaları,

-Enflasyonist baskılara ve ekonomik durgunluğa neden olabilmeleri,

-Kaynaklarını diğer kesimlerden sağlamaları,

-Başarısızlıkları halinde ekonominin tüm kesimlerinin zincirleme olarak etkilenebilmesi.

---

[24] Bülent Şenver, **Muhasebe ve Finansman Dergisi**, s.7, (2000), 22.
[25] Yıldız, age, 173.
[26] Milli Prodüktivite Merkezi , "Türk Bankacılık Sistemine İlişkin Bir Değerlendirme (1973-1988)"; (Ankara: Milli Prodüktivite Merkezi Yayınları, 1990),70.

Yukarıda sayılanlar dışında bir ülkede bankacılık sisteminin yapısının hükümetlerin uygulamayı düşündükleri para ve kredi politikalarının başarısını ve niteliğini belirleyen unsurlardan biri olması da diğer bir denetim nedeni olarak gösterilebilir.

2.6. Bankalarda Bilgi Sistemi Denetimi

KPMG Kıdemli Müdür Tanıl Durkaya bankalarda bilgi sistemleri denetimini şu şekilde açıklamaktadır; "Bankaların iç kontrol ortamına ve dolayısıyla iç denetim yapılanmalarına ilişkin en köklü değişiklik ve düzenlemeler 2000'li yılların başında yaşanan mali kriz ve Bankacılık Düzenleme ve Denetleme Kurumu'nun ("BDDK") kuruluşunun ardından gerçekleşmiştir. Teftiş Kurullarına ek olarak oluşturulan İç Kontrol ve Risk Yönetimi fonksiyonları bankalarda iç denetim ve kontrol ortamı kavramlarını bir anlamda yeniden şekillendirmiştir. Sonraki yıllarda bu kavramların içerik olarak detaylandırılmasına yönelik düzenlemeler de yapılmıştır. Özellikle "Süreç Denetimi" ve "Bilgi Sistemleri Denetimi" kavramları bu köklü değişiklikler arasında öne çıkan yeni kavramlar olarak sıralanabilir.[27]

2.6.1. Bankalarda Bilgi Sistemleri Yönetiminin Önemi

24/01/2009 tarihli ve 27120 sayılı Resmi Gazete ile 01/06/2010 tarihli ve 27598 sayılı Resmi Gazete'de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ Madde 4 1,2 ve 3'nolu maddelerde konunun önemi açıklanmaktadır.

> (1) Banka, bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele alır. Bankanın operasyonlarını istikrarlı, rekabetçi ve gelişen bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejinin iş hedefleri ile uyumlu olması sağlanır, bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde uygun yere yerleştirilir ve bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilir.
>
> (2) Banka, bilgi sistemlerinin yönetimine ilişkin politikalar, prosedürler ve süreçler tesis eder. Prosedürler ve süreçler ilgili iş alanında gerçekleşen değişiklikler veya teknolojik gelişmeler doğrultusunda gerekiyorsa yenilenmek üzere düzenli olarak gözden geçirilir.

[27] Tanıl Durkaya , "Banka İç Denetimlerinde Yeni bir dönem Başlıyor ", **KPMG Gündem Ekim-Aralık 2010** , (2010),23,24. http://www.kpmgvergi.com/tr-tr/SanalKutuphane/yayinlar/guncelyayinlar/Documents/kpmgundemsayi04.pdf [10.11.2011]

(3) Bilgi sistemleri üzerinde tesis edilen yönetimin etkinliği; risk yönetimi, iç kontrol sistemi ve iç denetim kapsamında yürütülecek çalışmaların da katkısıyla sağlanır.[28]

Bilgi Sistemleri denetimin öneminin anlaşılmasında yakın tarihte yaşanan büyük finansal olaylardan örnekler verilebilir. WorldCom daki Finansal bilgi raporlamasında yapılan sahtekarlıklar, aynı şekilde Enrondaki işlemler Amerika'da altmış milyar dolarlık bir kamu zararına yol açmıştır. Örneklere Türkiye'de de rastlamak mümkündür. Türkiye İmar Bankasının çifte kayıt sistemi kullanması ve müşterilerinin mağduriyeti halen hafızalarda yerini korumaktadır. Burada ismi geçen kuruluşlar hem global hem de yerel anlamda teknoloji ile bağlantılı kriz kaynağı olup olağanüstü zarar yaratan kuruluşlar olarak sıralanabilir.

İzzet Gökhan Özbilgin, Dünyada yaşanan bu önemli olayları şu şekilde açıklamaktadır; "Gerek dünyada 2001 yılında yaşanan "Enron Skandalı" gerekse ülkemizde 2003 yılında Bankacılık Düzenleme ve Denetleme Kurulu tarafından T.İmar Bankası T.A.Ş'e ait bankacılık işlemleri yapma ve mevduat kabul etme izninin kaldırılması ve bu bankanın Tasarruf Mevduatı Sigorta Fonuna intikaline sebep olan "çifte kayıt olayı" bilgi teknolojileri denetim kavramının öneminin her kesim tarafından iyice anlaşılması gerektiğini ortaya koymuştur. "[29]

İşte bu sorunlar yararı tartışılamayacak bilgi sistemlerinin, ele alınış şeklinde önemli değişikliklere yol açmış ve konunun disiplinli bir şekilde ele alınmasını tetiklemiştir.

Finans Sektörü Bilgi Teknolojileri Yatırıma kriz dönemlerinde dahi devam etmek durumundadır. Bilgi Teknolojilerinin 2010 yılındaki hızlı büyümesini ele alan Capital dergisi Finans sektörünün bu alandaki gelişmelerin en büyük yatırımcısı olduğunu açıkça ortaya koyuyor. Dergide "Geçtiğimiz birkaç yılda yatırımlar Türk bankacılık sektörüne aktı. Birkaç yabancı banka yerlileri satın aldı. Bunlar arasında BNP Paribas, National Bank of Greece, National Bank of Kuwait, ING Bank ve Unicredit önemli girişimcilerdi. Bu sürecin sonunda doğal olarak finans sektörü genişledi ve BT yatırımlarında finans sektörünün önemli payı oldu." şeklinde açıklamaktadır.[30]

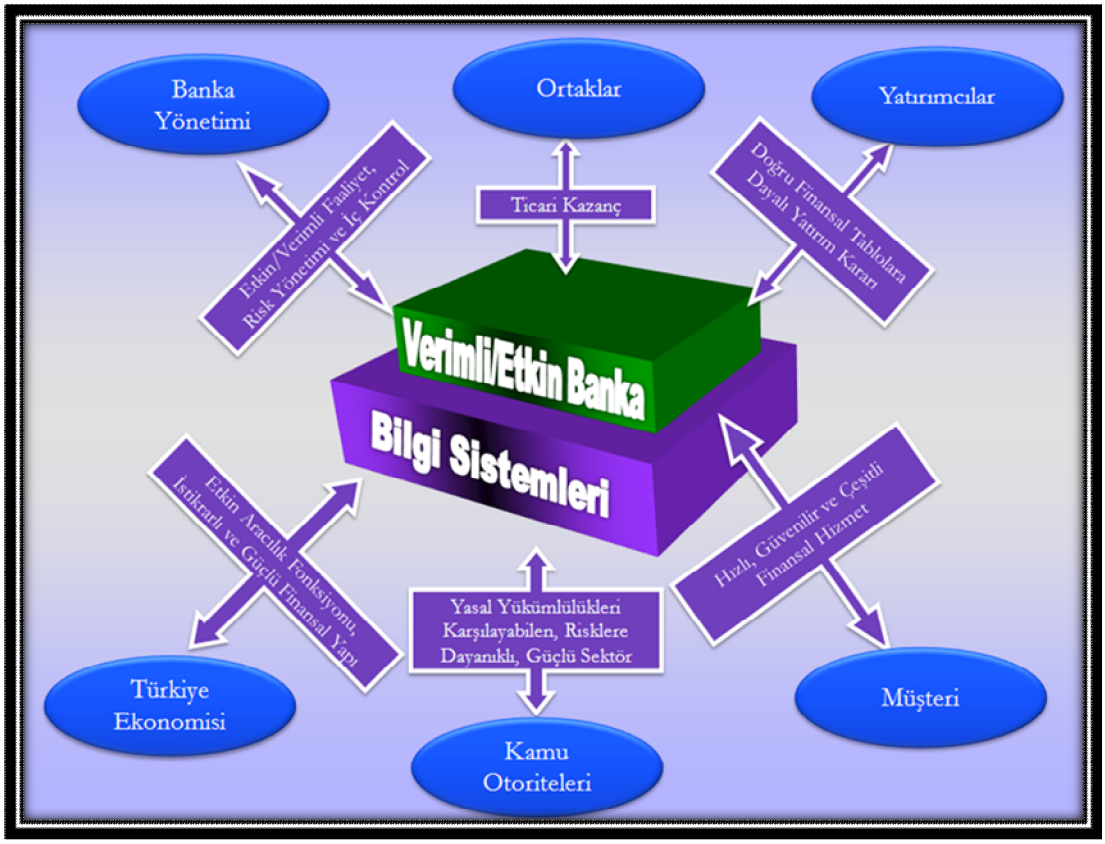
---

[28] BDDK, "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ", **Resmi Gazete,** 27120 , Haziran 2010, Md.4

[29] İzzet Gökhan Özbilgin, "Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar ", **Sayıştay Dergisi, s.49,** (2003):128.

[30] "Bilişimin 10 Milyar $ Yolculuğu", Capital Dergisi, http://www.capital.com.tr/bilisimin-10-milyar-$-yolculugu-haberler/21297.aspx [20.10.2011]

Bankacılık Düzenleme ve Denetleme Kurumu Bilgi Yönetimi Daire Başkanı Ahmet Türkay Varlı Şekil 1'de Verimli/Etkin Bankanın Sağlam Bilgi Sistemleri temelleri üzerine kurulu olduğunu gösterimi ve bankanın tüm paydaşlara hangi yöntem ile fayda sağladığını kısa ve öz bir biçimde ifade etmiştir.



Şekil 1: Bankacılıkta Bilgi Sistemleri ve Paydaşlar ile İlişkileri

Kaynak: Türkiye İç Denetim Enstitüsü, XI. Türkiye İç Denetim Kongresi Sunumu 9 Kasım 2007, İstanbul Ahmet Türkay VARLI Bilgi Yönetimi Daire Başkanı / BDDK

2.7. Bankacılıkta Bilgi Sistemlerinin Yönetimine İlişkin Mevzuat

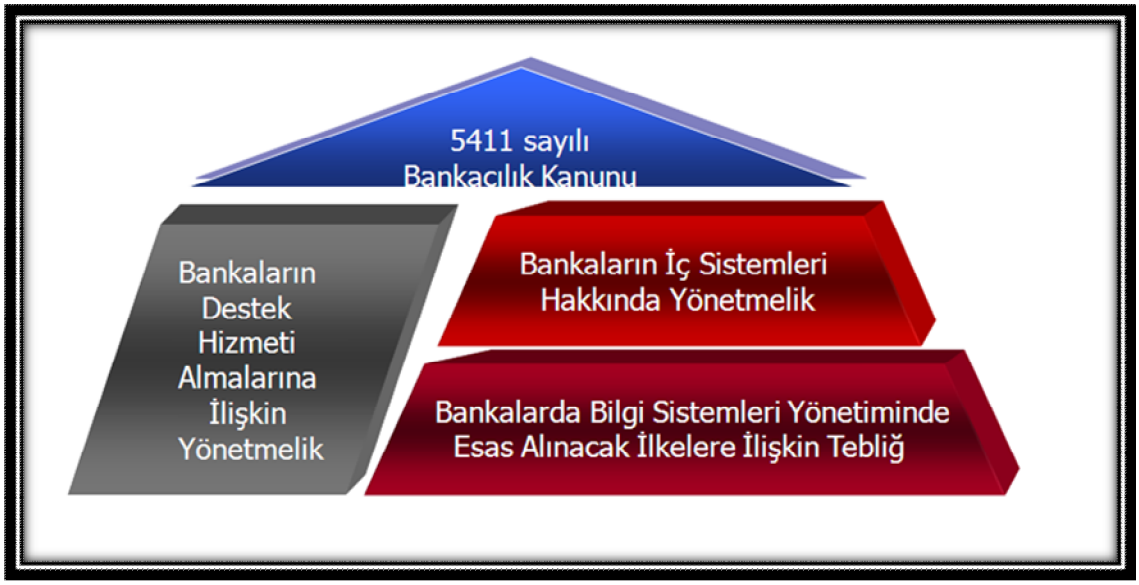
Bankacılık Düzenleme ve Denetleme Kurulu 5411 sayılı Bankacılık Kanununa tabi olan tüm kuruluşları, Resmi Gazete 01/11/2006 Tarihi, 26333 sayılı Bankaların İç Sistemleri Hakkında Yönetmelik ve Resmî Gazete ve Resmi Gazete 14.09.2007/26643 sayılı Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ (En son 01/06/2010 tarih 27598 sayılı resmi Gazete ile değiştirilmiştir) ile denetim sistemlerinin oluşturulmasını ve devamlılığının sağlanması gerekmişti. Ayrıca ilk olarak Bankaların tedarikçilerden alacakları hizmetler için uymaları gereken kurallar ise Resmi Gazete 01/11/2006 Tarihi, 26333 sayılı, Bankaların Destek Hizmeti Almalarına İlişkin

Yönetmelik içerisinde açıklanmıştır.(Tarih: 05/11/2011- Sayı: 28106 Resmi Gazetede güncellenmiştir)

5411 sayılı Bankacılık Kanunu Madde 32 de Bankaların kurmak zorunda oldukları iç denetim sistemi;

> "Bankalar bütün birim, şube ve konsolidasyona tabi ortaklıklarını kapsayan bir iç denetim sistemi kurmak zorundadır. Bu çerçevede, faaliyetlerin mevzuata, ana sözleşmeye, iç düzenlemelere ve bankacılık ilkelerine uygunluğu, banka müfettişleri tarafından denetlenir.
>
> İç denetim faaliyetleri, tarafsız ve bağımsız bir şekilde, gerekli meslekî özen gösterilerek, yeterli sayıda müfettiş tarafından yerine getirilir. Ana ortaklık niteliğindeki bankanın iç denetiminde görev alanlar konsolidasyona tâbi ortaklıklarda iç denetim görevini ifa edebilir. İç denetimle görevli birimce veya yetkili müfettişlerce bu Kanunun 29 uncu maddesinin ikinci fıkrası kapsamında düzenlenecek iç denetim raporunun, en az üçer aylık dönemler itibarıyla ve denetim komitesi aracılığıyla yönetim kuruluna tevdii zorunludur."[31]

Şeklinde açıkça belirtilmiştir.



Şekil 2: Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi/ Mevzuat Çerçevesinde BDDK Perspektifi

Kaynak: Türkiye İç Denetim Enstitüsü, XI. Türkiye İç Denetim Kongresi Sunumu 9 Kasım 2007, İstanbul Ahmet Türkay VARLI Bilgi Yönetimi Daire Başkanı / BDDK

[31] 5411 Sayılı Bankacılık Kanunu Md.32.

2.7.1. 5411 Sayılı Bankacılık Kanunu

5411 Sayılı kanun içeriği BDDK'nın Bilgi Sitemleri Denetim yapısını oluşturmada Bilgi BDDK Bilgi Yönetimi Daire Başkanı Ahmet Türkay VARLI şu kanun maddelerini sıralamıştır.

Bu Kanun maddelerinde Sırasıyla;

- İç sistemlere ilişkin yükümlülükler
- İç kontrol sistemi
- Sorumluluk
- İtibarın korunması

şeklindedir.

2.7.1.1. İç sistemlere ilişkin yükümlülükler

5411 sayılı Bankacılık Kanunu Madde 29 da Bankaların iç kontrol, risk yönetimi ve iç denetim sistemi kurmak ve işletmekle yükümlü oldukları belirtilmektedir.

> ***MADDE 29.-*** Bankalar, maruz kaldıkları risklerin izlenmesi, kontrolünün 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 yükümlüdürler.

2.7.1.2. İç kontrol sistemi

5411 sayılı Bankacılık Kanunu Madde 30 da iç kontrol sisteminin yapısı kısaca özetlenmektedir.

> ***MADDE 30.-*** Bankalar, iç kontrol sistemi kapsamında, faaliyetlerinin mevzuata, iç düzenlemelerine ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve raporlama sisteminin bütünlüğünü, güvenilirliğini ve bilgilerin zamanında elde edilebilirliğini her seviyedeki personeli 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 zorundadır. İç kontrol faaliyetleri yönetim kuruluna bağlı olarak çalışacak iç kontrol birimi ve personeli tarafından yürütülür.

2.7.1.3.Sorumluluk

5411 sayılı Bankacılık Kanunu Madde 41 de yapılacak denetim fonksiyonunun Yönetim Kurulu bünyesinde ve sorumluluğunda olacağı bilgisi mevcuttur.

> ***MADDE 41.-*** Yönetim kurulu, bu Kanunun 37 nci maddesi uyarınca faaliyetlerin muhasebeleştirilmesi, finansal tabloların hazırlanması, onaylanması, denetlenmesi, yetkili mercilere sunulması ve yayımlanması dâhil finansal raporlama sistemini, görev, yetki ve sorumlulukları belirlemek, bilgi sistemlerini yeterli hale getirmek ve uygulamayı gözetmekle yükümlüdür.

2.7.1.4. İtibarın korunması

5411 sayılı Bankacılık Kanunu Yedinci Kısım Kanuni Yükümlülükler bölümü Madde 41 de Bankaların itibarının korunması için önlem alınmaktadır.

> ***MADDE 74.*** - 5187 sayılı Basın Kanununda belirtilen araçlarla ya da radyo, televizyon, video, internet, kablolu yayın veya elektronik bilgi iletişim araçları ve benzeri yayın araçlarından biri vasıtasıyla; bir bankanın itibarını kırabilecek veya şöhretine ya da servetine zarar verebilecek bir hususa kasten sebep olunamaz ya da bu yolla asılsız haber yayılamaz.

2.7.2. Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik

Bugün bankaların artan Bilgi Sistemleri ihtiyaçlarını karşılamaya yönelik oluşturmuş oldukları Bilgi Teknolojileri Grupları departmanları veya şirketleri mevcut Bilgi Sistemleri yapılarını sürdürmeleri ve geliştirmeleri için çalışmalarına devam etmektedirler. Ancak her ne kadar büyük bir yapıda birimler, departmanlar hatta ayrı bilişim teknolojileri şirketleri iştirakleri kursalar da bilgi sistemleri gelişimi ve çok geniş bir düzeyde oluşu her sektörde olduğu gibi bankaları da Destek hizmeti veren taşeron firmalara yönlendirmektedir.

Ahmet Türkay Varlı, dışarıdan destek hizmeti alma konusunun kaçınılmaz bir gerçek olduğunu, İster banka ister diğer şirketler olsun yürütmek zorunda oldukları tüm faaliyetleri, bizzat kendi kaynaklarını kullanarak yürütemediklerini, kaynakların verimli kullanılması adına, dış kaynaklara başvurmak durumunda kaldıklarını belirtmiştir.[32]

Bu konuda BDDK amacı aşağıda Madde1 de belirtilmiş olan düzenlemeyi 26333 sayılı Resmi gazetede yayınlamıştır. 1/11/2006 tarihli ve 26333 sayılı Resmî Gazete'de yayımlanan "Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik" yürürlükten kaldırılmıştır. Bunun yerine Bankacılık Düzenleme ve Denetleme Kurumundan 5 Kasım 2011 tarihli Resmî Gazete Sayı: 28106 "Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik" yayınlanmıştır.

İntibak süresi Geçici Madde 1'de şu şekilde belirtilmiştir; "Bu Yönetmelik kapsamındaki konularda destek hizmeti alan bankalar ile destek hizmeti kuruluşları imzaladıkları sözleşmeleri ve durumlarını bu Yönetmeliğin yayımı tarihinden en geç 1 yıl içerisinde bu Yönetmelik hükümlerine uygun hale getirmek zorundadır."

Bu Yönetmelik 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 35, 36 ve 93 üncü maddelerine dayanılarak hazırlanmıştır.

[32]Ahmet Türkay Varlı, "Yönetim Beyanından Neler Bekliyoruz", **Türkiye İç Denetim Enstitüsü İç Denetim Dergisi**, 10.yıl Özel Sayısı Sonbahar, (2011):7.

> ***MADDE 1*** - (1) Bu Yönetmeliğin amacı, bankalarca destek hizmeti alımına ilişkin usul ve esasları düzenlemektir. [33]

Yönetmelik Madde 5 içerisinde destek hizmeti almak isteyen bankaların yükümlülükleri belirtilmektedir.

2.7.2.1. Destek hizmeti kuruluşlarında aranacak şartlar

5 Kasım 2011 Tarihli, 28106 sayılı Destek Hizmeti Alımına İlişkin Yönetmelik kapsamında bankalara destek hizmeti verecek kuruluşların sahip olması gereken özellikler ve hizmet verebilme şartları Madde 6 da belirtilmiştir.

> ***MADDE 6 –*** (1) Bu Yönetmelik kapsamında bankalara destek hizmeti verecek kuruluşların;
>
> a) Sermaye şirketi seklinde kurulmuş, ortaklık yapılarının şeffaf ve açık olması,
>
> b) Destek hizmetini gerçekleştirebilecek yönetim yapısına, yeterli sayı ve nitelikte personele, gerekli teknik donanıma, belge ve kayıt düzenine, is devamlılığı planına sahip olmaları; sözleşme konusu hizmeti kendi bünyesinde verecek ise, olası güvenlik risklerine, yangın ve doğal afetler gibi acil durumlara karsı gerekli önlemleri almış olmaları ve bu sartların sağlandığının banka tarafından yerinde tespit edilmiş olması,
>
> c) Hizmet verdikleri bankalarca talep edilmesi ya da Kurulca gerekli görülmesi halinde, verdikleri hizmetlerden doğabilecek zararları karşılamak amacıyla sorumluluk sigortası yaptıracaklarını taahhüt etmeleri,
>
> ç) Yurt dışında ya da Türkiye'deki yetkili otoritelerce faaliyette bulundukları alanla ilgili yetkilerinin iptal edilmemiş veya kısıtlanmamış olması,
>
> d) Kanunun 8 inci maddesinin birinci fıkrasının (a) bendi kapsamında bulunmamaları,
>
> e) Nitelikli pay sahiplerinin, yönetim kurulu başkan ve üyeleri ile sirketi temsil ile yetkili yöneticilerinin
>
> 1) Kanunun 8 inci maddesinin birinci fıkrasının (a), (b), (c) ve (d) bentlerinde belirtilen nitelikleri haiz olmaları,
>
> 2) İşin gerektirdiği mali güç ve itibara sahip bulunmaları,
>
> 3) Yurt dışında ya da Türkiye'deki yetkili otoritelerce bulunduğu alanla ilgili yetkileri iptal edilmiş veya kısıtlanmış destek hizmeti kuruluşlarında ortak, yönetim kurulu başkanı, üyesi veya denetçi ya da yönetici olmamaları veya çalışan olarak yetki iptaline veya kısıtlamaya neden olan işlemlerde sorumluluklarının tespit edilmemiş olması zorunludur.

[33] BDDK, "Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik", **Resmî Gazete** 5 Kasım 2011 Sayı : 28106

2.7.2.2. Sözleşmenin unsurları

Bankaların alacakları destek hizmetleri sırasında yapacakları hizmet alım sözleşmelerin yapısı Madde 9 da belirtilmiştir. Bankaların yoğun bir şekilde dış hizmet aldığı bilişim sektörü şirketleri ile aralarında yaptıkları tedarikçi sözleşmeleri ve hizmet düzey anlaşmaları temel sözleşmeyi oluşturmaktadır. Şekil şartları kanunda belirtilmektedir. Bankaların ihtiyaçları itibariyle zenginleştirilebilir.

> ***MADDE 9 –*** (1) Bankalar ile destek hizmetleri kuruluşları arasında imzalanacak sözleşmelerde;
>
> a) Destek hizmetinin konusu, kapsamı ve süresi, alınan hizmet karşılığı ödenecek ücret ile tarafların sorumlulukları gibi hususların açık, anlaşılır ve hiçbir tereddüde mahal vermeyecek şekilde ifade edilmesi,
>
> b) Destek hizmeti kuruluşlarının gerçekleştirdiği faaliyetlere ilişkin olarak Kurumun denetimine tabi olduğu ve Kurumca talep edilen her tür bilgi ve belgeyi zamanında ve doğru olarak vermekle ve bunlara ilişkin her türlü mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki kayıtları ve bu kayıtlara erişim ve kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifreleri incelemeye hazır bulundurmak ve işletmekle yükümlü olduğu hususlarının belirtilmesi,
>
> c) Destek hizmeti kuruluşu tarafından sağlanan hizmet dolayısıyla öğrenilen bankalara ve müşterilerine ait bilgi ve belgelerin, yapılan anlaşmada belirtilen amaçlar dışında kullanılmasının ve üçüncü kişilere açıklanmasının yasak olduğu, destek hizmeti kuruluşunun söz konusu bilgi ve belgelerin korunmasında gerekli özeni göstermekle yükümlü bulunduğu ve bunlara aykırılık halinde banka tarafından sözleşmenin tek taraflı olarak feshedileceği hususlarının belirtilmesi,
>
> ç) Destek hizmeti kuruluşuna belirli hallerde sözleşmeyi süresinden önce sona erdirme hakkı tanınmakta ise, bu durumda alınan hizmetin başka bir destek hizmeti kuruluşu veya bizzat banka tarafından sağlanmasına imkan verecek bir müddetle destek hizmeti kuruluşu tarafından sağlanmasına devam olunmasına ilişkin hüküm konulması,
>
> d) Destek hizmeti kuruluşunca verilecek hizmetlerden doğabilecek zararların karşılaması amacıyla mesleki sorumluluk sigortası yaptırılacağı hususunun taahhüt edilmesi,
>
> e) Destek hizmeti kuruluşları tarafından sağlanan hizmetlerin tamamen veya kısmen alt yüklenici kuruluşlara devrinin mümkün kılınması halinde (a), (b), (c), (ç) ve (d) bentlerinde belirtilen hususlara alt yüklenici kuruluşlarla yapılacak sözleşmelerde de yer verileceğinin destek hizmeti kuruluşu tarafından taahhüt edilmesi, zorunludur.

2.7.2.3. Destek hizmeti kuruluşlarının denetimi

Alınan Destek hizmetine yönelik denetim yapma yetkileri Bankalarca Dışarıdan Temin Edilen Bilgi Sistemleri Hizmetleri Yönetmeliği Madde 12'de belirtilmektedir.

> ***MADDE 9*** – (1) Kurum, destek hizmeti kuruluşlarından Kanun ve bu Yönetmelik hükümleri ile ilgili göreceği bütün bilgileri gizli dahi olsa istemeye, tüm defter, kayıt ve belgelerini incelemeye yetkili olup, destek hizmeti kuruluşları da istenilen bilgileri vermekle, sistem, süreç, defter, kayıt ve belgeleri incelemeye hazır bulundurmakla, tüm bilgi işlem sistemini denetim amaçlarına uygun olarak Kurumun yerinde denetim yapan meslek personeline açmakla, verilerin güvenliğini sağlamakla ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda bulundukları bilgilere ilişkin elektronik, manyetik ve benzeri ortamlardaki kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifrelerini inceleme için ibraz etmek ve işletmekle yükümlüdür.
>
> (2) Denetim komitesi, destek hizmeti alınmasında bankanın iç sistemlerinin etkin ve yeterli bir şekilde isletilmesini veya iç kontrol ya da iç denetim faaliyetlerinin yürütülmesini engelleyici ya da risk doğurucu herhangi bir hususun oluşup oluşmadığı ve destek hizmeti kurulusunun nitelikli pay sahiplerinin ve şirketi temsil ile yetkili yöneticilerinin 6 ncı maddede belirlenen şartları idame ettirip ettirmedikleri hususlarında, üç ayda bir banka yönetim kuruluna sunmak üzere bir değerlendirme raporu hazırlar.
>
> (3) Bankaca talep edilmesi ya da Kurulca bankadan istenilmesi halinde ilgili destek hizmeti kurulusunca sorumluluk sigortası yaptırılır.

2.7.3. Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik

Bankaların bilgi sistemleri ile bankacılık süreçlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesi ile ilgili usul ve esasları düzenlemek için Resmi Gazete'de 13/1/2010 Sayı: 27461 ile yayınlanmıştır. En son 26/07/2011 tarihli ve 28006 sayılı Resmi Gazete'de yayımlanan Yönetmelik ile değiştirilmiştir.

İlk olarak Resmi Gazete'de 16/05/2006 Sayı: 26170 ile yayınlanan Yönetmelikte 31 Aralık 2007 tarihi itibariyle "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" kapsamında bilgi sistemi denetime dair zorunlu esaslar belirlenmiştir. Bilgi sistemleri ve finansal veri üretimine ilişkin süreçler ve sistemlerin üzerindeki uygulama kontrollerine ve genel kontrol alanlarına dair bağımsız denetim faaliyetleri Türkiye'deki tüm bankalar için zorunlu hale getirilmiştir. Bu yönetmelik ile birlikte 14 Eylül 2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"de belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesi zorunlu hale getirilmiştir. 2006 yılı içinde yayınlanan ve 31 Aralık 2007 itibariyle uygulanan Yönetmelikte bankalarda gerçekleştirilecek bilgi sistemleri denetimi, uygulama kontrolleri denetimi ile genel kontrol alanları denetimleri bulunmaktaydı.
Bağımsız denetim kuruluşlarınca her sene uygulama kontrolleri denetiminin gerçekleştirilmesi gerekmemekte, genel kontrol alanlarına yönelik denetim bilgi sistemleri denetimleri iki sene de bir gerçekleştirilmesi zorunlu tutulmuştu.

Değiştirilen 13/1/2010 tarihli Sayı: 27461 Resmi Gazetede yayınlanan Yönetmelik ile Yönetim beyanı kapsamı belirlenmiş ve her yıl bağımsız denetçiye sunulması gerektiği açıklanmıştır.

İçeriği Özetle;

Birinci Bölüm:

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar açıklanır.

İkinci Bölüm; Bilgi Sistemleri ve Bankacılık Süreçleri Denetimine İlişkin Genel Kavramlar;

Önemlilik, Kontrol zayıflığı, Etkinlik, yeterlilik ve uyumluluk, Denetim riski başlıklarını içerir ve kavramsal açıklamalarda bulunur.

Üçüncü Bölüm :Yetkilendirme, İzin ve Meslek Mensupları;

Yetkilendirilecek kuruluşlarda aranan şartlar, Yetki başvurusu sırasında gerekli olan bilgi ve belgeler, Bilgi sistemleri ve bankacılık süreçleri denetimi yapma yetkisinin verilmesi, Bilgi sistemleri ve bankacılık süreçleri denetimi yapma yetkisinin kaldırılması, Banka bilgi sistemleri ve bankacılık süreçleri denetiminin dış hizmet alımı ile gerçekleştirilmesi, Dış hizmet sağlayıcı kuruluşta aranan şartlar, İzin başvurusu sırasında gerekli olan bilgi ve belgeler, Dış hizmet alımı ile bilgi sistemleri ve bankacılık süreçleri denetimi yapma izninin verilmesi, Dış hizmet alımı ile bilgi sistemleri ve bankacılık süreçleri denetimi yapma izninin iptali, Meslek mensubu unvanları başlıklarını içerir.

Dördüncü Bölüm: Tarafların Yükümlülükleri;

Denetlenenin yükümlülükleri, Yetkili kuruluşların ve denetçilerin yükümlülükleri açıklanır.

Beşinci Bölüm: Bilgi Sistemleri ve Bankacılık Süreçleri Denetimine İlişkin Esaslar;

Bilgi sistemleri ve bankacılık süreçleri denetimi ve amacı, Bilgi sistemleri ve bankacılık süreçleri denetiminin kapsamı, Bilgi sistemleri ve bankacılık süreçleri denetimi ile bağımsız denetimin ilişkisi, Bilgi sistemleri denetimi, Bankacılık süreçleri denetimi, İç kontrol ve iç denetim sistemine ilişkin değerlendirme, Bilgi sistemleri ve bankacılık süreçleri denetimi faaliyetlerinin yürütülmesi süreçlerini açıklar.

Altıncı Bölüm: Bilgi Sistemleri ve Bankacılık Süreçleri Denetimi Metodolojisi;

Denetim stratejisi ve denetim planı, Denetim teknikleri ve kontrollerin test edilmesi, Denetim örneklemesi, Denetim kanıtı, Bulguların değerlendirilmesi, Yönetim beyanı, Denetim görüşünün oluşturulması ve denetim mektubu, Denetim çalışmalarının belgelendirilmesi konularını açıklar.

Yedinci Bölüm: Genel İlkeler ve Sorumluluklar;

Bilgi sistemleri ve bankacılık süreçleri denetimi sözleşmesi

Sekizinci Bölüm: Bilgi Sistemleri ve Bankacılık Süreçleri Denetiminde İşbirliği;

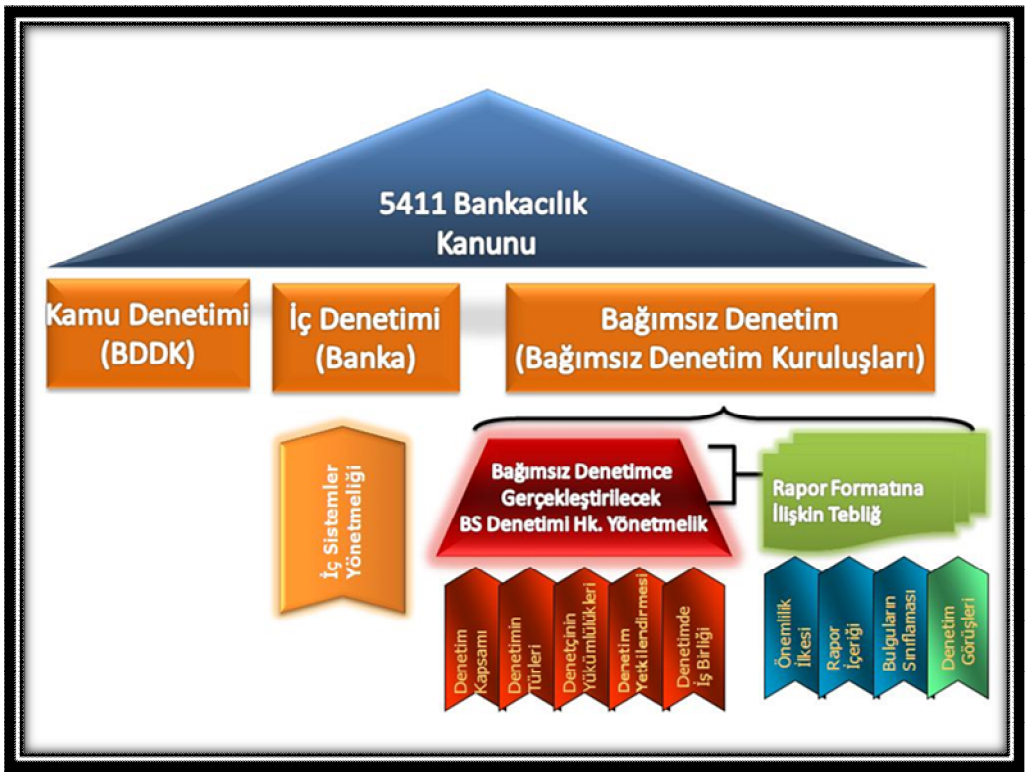
Başka taraflarca yapılan çalışmalardan yararlanma ve işbirliği, Kurum ve yetkili kuruluşlar arası işbirliği, Destek hizmeti kuruluşunun denetlenmesi süreçlerini açıkları

Dokuzuncu Bölüm:

Bilgi Sistemleri ve Bankacılık Süreçleri Denetimi Raporu ve Bildirimi , Bilgi sistemleri ve bankacılık süreçleri denetimi raporu

Onuncu Bölüm: Çeşitli ve Son Hükümler;

Denetçilerinin bankalarda görev almaları, Yönetmelikte hüküm bulunmayan haller, Yürürlükten kaldırılan yönetmelik hakkında bilgiler verir.



Şekil 3: Bankacılıkta BS Denetimi Mevzuat Çerçevesi

Kaynak: Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi/ Mevzuat Çerçevesinde BDDK Perspektifi Türkiye İç Denetim Enstitüsü, XI. Türkiye İç Denetim Kongresi Sunumu 9 Kasım 2007, İstanbul, Ahmet Türkay VARLI, Bilgi Yönetimi Daire Başkanı / BDDK

Yukarıdaki şekilde Bilgi Sistemleri Denetiminin bölüm boyunca sayılmış tüm kanuni boyutu detaylı olarak resmedilmiştir.

2.7.4. Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ

Resmî Gazete'nin Tarihi 14/09/2007 Sayısı 26643 Yönetmeliğin Yayımlanmıştır. Yönetmelikte Değişiklik Yapan Mevzuatın Yayımlandığı Resmî Gazete'nin 01/06/2010 Tarihi 27598 Sayısı ile yayınlanmıştır. Bu Tebliğin amacı, bankaların, faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esasları düzenlemektir.

İlkeler Tebliği Ana Başlıkları

Bilgi Sistemlerine İlişkin Risk Yönetimi ve İç Kontrollerin Tesisi; Bilgi Sistemlerine İlişkin Risk Yönetimi

- Yönetim gözetimi
- Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi
- Destek hizmeti alımı sürecinin yönetimi
- Kimlik doğrulama
- İnkâr edilemezlik ve sorumluluk atama
- Görevler ayrılığı ilkesi
- Yetkilendirme
- İşlemlerin, kayıtların ve verilerin bütünlüğü
- Denetim izlerinin oluşturulması
- Veri gizliliği
- Müşterilerin bilgilendirilmesi
- Müşteri bilgilerinin mahremiyeti
- Bilgi sistemleri süreklilik planı

Bilgi Sistemlerine İlişkin İç Kontrollerin Tesisi ve Takibi

- Bilgi sistemleri kontrolleri
- Uygulama kontrolleri
- Genel kontroller
- Kontrollerin takibi

Özellik Arz Eden İşlemler; İnternet Bankacılığı

- İnternet bankacılığında uygulanacak hükümler
- Yönetim gözetimi
- Güvenlik kontrol sürecinin tesis edilmesi ve yönetilmesi
- Kimlik doğrulama
- İnkâr edilemezlik ve sorumluluk atama
- Denetim izlerinin oluşturulması
- Müşterilerin bilgilendirilmesi
- Servis sürekliliği ve kurtarma planı

ATM; (Ayrıca ATM'lerde Kimlik Doğrulama ile ilgili 05/02/2009 tarihli BDDK Genelgesi bulunmaktadır. ATM'e kartsız para yatırma işlemlerinde nasıl uygulanacağına ilişkin tereddütleri ortadan kaldırmak üzere yayınlanmıştır)

- ATM güvenliği

Çeşitli ve Son Hükümler;

- Kablosuz haberleşme teknolojileri

Tebliğde hüküm bulunmayan haller; MADDE 34 – (1) Bu Tebliğde hüküm bulunmayan hallerde; İç Sistemler Yönetmeliğinde yer alan usul ve esaslar, uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan COBIT dokümanlarında yer alan usul ve esaslar uygulanır.

Özellik Arz Eden İşlemler

- İnternet Bankacılığına özel hükümler
- ATM Güvenliği
- Kablosuz Haberleşme Teknolojileri
- Uyum Süreci

İlkeler Tebliği Madde 3 'ı' fıkrasında " COBIT: Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından yayınlanmış olan Bilgi Teknolojilerine İlişkin Kontrol Hedefleri'nin(COBIT) güncel versiyonunu" kullanılacağı belirtilmiştir.

Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ İkinci Bölümde, Bilgi Sistemlerine İlişkin İç Kontrollerin Tesisi ve Takibi, Bilgi sistemleri kontrolleri aşağıda belirtilen tebliğ maddelerinde açıklanmadır.

> ***MADDE 22*** – (1) (Değişik: RG-24/01/2009-27120) Bilgi sistemleri genel kontrolleri, bilgi sistemlerinden beklenen fonksiyonların doğru bir şekilde yerine getirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvence oluşturulmasını ve uygulama kontrollerinin işlevselliği için güvenilir bir ortamın sağlanmasını hedefleyen, banka bilgi sistemlerinin tamamına veya büyük bir bölümüne tatbik edilen kontroller ile bu kontrollerin tatbik edilmesini sağlayan politika ve prosedürlerden oluşur. Genel kontroller, bankanın bilgi sistemlerinin bir bütün olarak kendisinden beklenen fonksiyonları doğru, zamanında ve güvenilir bir şekilde gerçekleştirmesine yönelik ortamın tesis edilmesini sağlayan temel unsurlardır.
>
> (2) Banka, genel kontrollerin tesisi amacıyla uluslararası kabul görmüş bir standart, çerçeve veya metodolojiyi belirleyerek, buna göre kontrolleri tesis eder. Seçilecek standart, çerçeve veya metodoloji, bankanın faaliyet kapsamı ve faaliyetlerde yararlanılan bilgi teknolojileri ağırlığı ve karmaşıklığı göz önünde bulundurularak belirlenir. Bankanın bilgi sistemleri genel kontrollerini tesis etmek üzere kullanacağı standart, çerçeve veya metodolojinin Cobit'te ele alınan kontrol hedeflerini gerçekleyebilmesi, eğer bu konuda eksiklikleri varsa buna ilişkin kontrollerin ayrıca ele alınarak tesis edilmesi gerekir.
>
> (3) Banka, genel kontrol konusu her bir sürece ilişkin olarak aşağıda sayılan hususlara uygun bir ortam tesis eder:
> a) Süreç sahibi: Her genel kontrol konusu süreç için sorumluluğu açıkça tanımlanmış bir süreç sahibi atanır.
> b) Tekrarlanabilirlik: Genel kontrol konusu süreçler tekrarlanabilir biçimde tanımlanır.
> c) Hedefler ve amaçlar: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açıkça
> tanımlanmış hedefler ve amaçlar oluşturulur.
> ç) Roller ve sorumluluklar: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açık bir şekilde roller, faaliyetler ve sorumluluklar tanımlanır.
> d) Süreç performansı: Belirlenen hedeflere göre her genel kontrol sürecinin performansı ölçülür.
> e) Politikalar, planlar ve prosedürler: Her bir genel kontrol süreciyle ilgili politikalar, planlar ve prosedürler yazılı hale getirilir, belli aralıklarla gözden geçirilir, güncellenir, onaylanır ve tüm ilgili birimlere duyurulur.

2.7.4.1. Benimsenen Esas; "COBIT"

COBIT (Bilgi ve İlgili Teknoloji için Kontrol Amaçları), Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) 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 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. Şirketlerin neler yapması gerektiği ile ilgilidir ama bunların nasıl yapmaları gerektiği ile ilgilenmez.[34]

CobiT, bilgi işlem teknolojilerine dayanan kritik iş süreçlerini desteklemeyi amaç edinmiştir. Teknolojinin etkin ve yaygın olarak kullanımından kaynaklanan risklerin yönetilmesi ve kritik iş süreçlerinin bilinçli ve sistematik yöntemlerle desteklenmesinin önemi yanında, yasal düzenlemeler de, bilgi üzerinde sağlanacak kontroller ile ilgili yenilikler ve zorunluluklar getirmektedir. Bütün bu noktalar dikkate alındığında Bilgi İşlem Teknolojisi ve risklerinin yönetimi, organizasyon yönetiminin ayrılmaz bir parçası haline gelmektedir. Şöyle ki, yönetim karmaşık ortamlarda risk ve kontrol hakkında hızlı ve doğru kararlar vermek için sürekli, yeterli, doğru ve zamanında elde edilebilecek bilginin peşindedir.[35]

CobiT 1996'da ilk kez yayınlanmıştır. CobiT, güncellenerek 2000 yılında 3. versiyonuna ulaşmıştır. Yaklaşık 5 yıllık dönemlerle güncellenmektedir. Şu an versiyon 4.1 mevcuttur, 5.0 hazırlanmaktadır. Cobit 5'e ait İlk Taslak (Exposure Draft) 2011 yılında yayınlanmış uzmanların önerilerine açılmıştır.

CobiT, bilgi işlem süreçlerini, bilgi işlem kaynaklarını, stratejik karar vermeye destek olan ölçüm yöntemleri ve bilgileri birleştiren bir yapı ortaya koymaktadır. Bunun da ötesinde, Planlama ve Organizasyon (Planning and Organization), Alım ve İşletim (Acquisition and Implementation), Destek ve Servis (Delivery and Support) ve İzleme ve Değerlendirme (Monitor and Evaluate) grupları şemsiyesindeki süreçlerin, En İyi Uygulamalar (Global Best Practices) doğrultusunda oluşturulması ve kritik iş süreçlerine sağlamış oldukları desteğin ağırlığı, kontroller ve iyileştirmeler sonucunda daha da arttırılabilecektir. Bu nedenle, CobiT bakış açısı ile teknoloji süreçlerinin ve risklerinin yönetimi ve denetimi bu proje sonucunda mümkün kılınarak, bilgi ve

[34] Vildan Uzunay, **COBIT (Control OBjectives for Information and related Technology),** (Ankara:İç Kontrol Merkezi Uyumlaştırma Dairesi, 2007),2.
[35] Eliza Natasa Artinyan , **CobiT Çerçevesi,** http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf [11.10.2011]

teknolojiden dünya standartlarında faydalanması, iş geliştirme fırsatları yaratması, risklerini minimize etmesi ve teknolojinin sağladığı rekabet avantajını güçlendirmesi hedeflenmiştir.[36]

Şekil 4: Bilgi İşlem Teknolojileri için Kontrol Hedefleri BT Kaynakları ve BT Süreçleri

Kaynak: CobiT Çerçevesi, Eliza Natasa Artinyan, Deloitte Sayfa 1

Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik Onuncu Bölüm, Çeşitli ve Son Hükümler başlığı altında, Madde 42'de Yönetmelikte hüküm bulunmayan hallerin COBIT esas alınarak değerlendirilmesi gerektiği belirtilmiştir.

> MADDE 42 – (1) Bu Yönetmelikte hüküm bulunmayan hallerde; BDYFY, uluslararası denetim standartları ve COBIT'te yer alan usul ve esaslar uygulanır.[37]

Bu noktada BDDK Bankalar için açık bir kapı bırakmıştır. COBIT gruplanmış 4 süreç alanı ve 34 tane temel Bilgi Teknolojisi süreci yer almaktadır. 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

[36] age.s.4
[37] BDDK, "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik", Md.42.

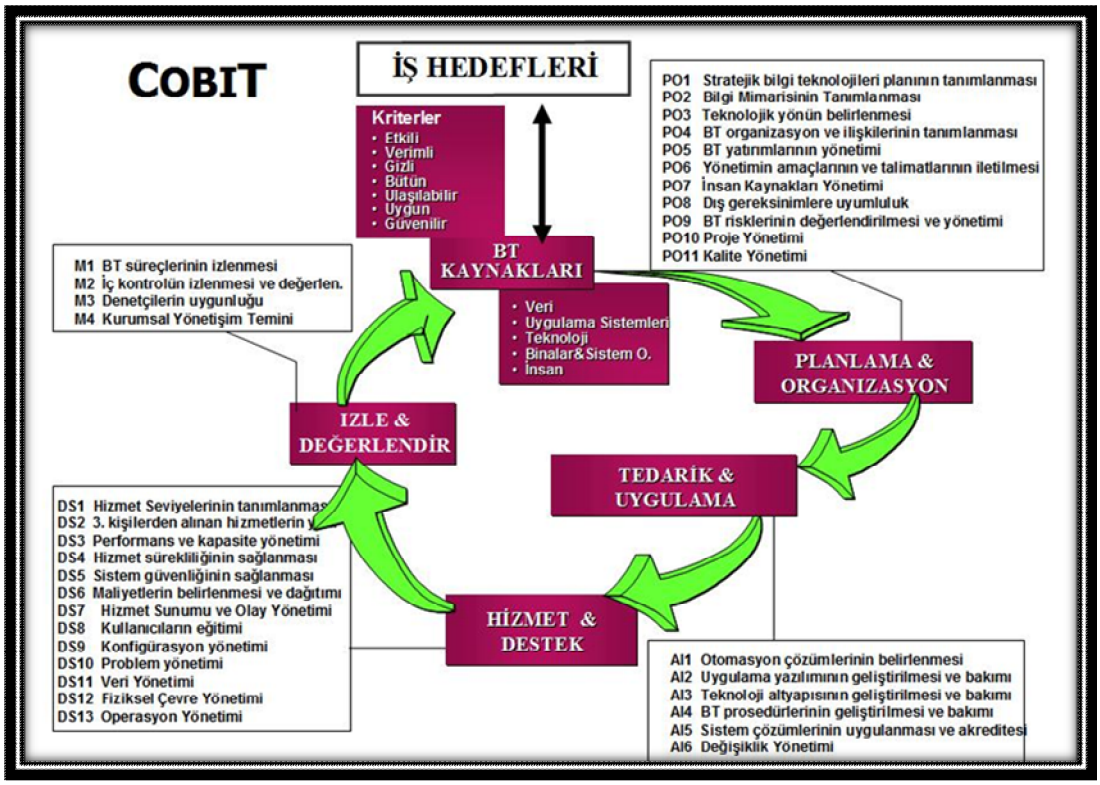
uygulamalar ve standartları (COSO, ISO 9000, Spice, CMM, ITIL, BSI7799 vb.) referans olarak ele almış, dünya çapında akademisyen, uzman, danışman ve analistler ile ortak bir çalışma yürütmüştür. CobiT'de yer alan "Yönetim Rehberi-Management Guidelines" içerisinde tüm teknoloji süreçleri için Olgunluk 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.[38]

Cobit Kontrolleri Ana başlıkları;

1. PO (Plan and Organize) - Planlama ve Organizasyon
2. AI (Acquire and Implement) - Tedarik ve Uygulama
3. DS (Delivery and Support) - Hizmet Sunumu ve Destek
4. ME (Monitor and Evaluate) - Gözlem ve Değerlendirme[39]

şeklindedir.

[38] Artinyan, age.2.
[39] ISACA, **COBIT 4.1**, (USA: ISACA, 2007)12,13.



Şekil 5: Cobit 4.1 34 Alt Süreç Şeması

Kaynak: ISACA,Cobit 4.1

CobiT'de yönetimin sorunlarını ve ihtiyaçlarını baz alan bilgiler ve tanımlamalar ile, güvenlik ve kontrollerin etkinliğini tespit ve izleme gereksinimlerini karşılayan belli araç ve yöntemler de yer almaktadır:

• Performans Göstergeleri ve ölçümlenmesi - İyi performansın göstergeleri nedir? Ölçüm nasıl yapılır?

• Bilgi işlem kontrollerinin profillendirilmesi - Ne önemlidir? Kontrol için kritik başarı faktörleri nelerdir?

• Risk yaklaşımı - Amaçlara ulamamamızın veya ulaşmaya çalışırken karşılaşabileceğimiz riskler nelerdir?

• Benchmarking –-Diğerleri ne yapıyor? Nasıl ölçüyoruz ve karşılaştırıyoruz?

• Olgunluk Modeli - organizasyonun mevcut durumunun tespiti ve bu durumun standartlara, en iyi örneklere ve hedeflere göre karşılaştırılması,

• Hedef Göstergeleri - bilgi işlem süreçlerinin hedefleri ne oranda karşıladığının izlenmesi, Kritik Başarı Faktörleri ile de süreçlerin kontrol altına alınması sağlanmaktadır.

Ahmet Türkay Varlı, İç Denetim Kongresi Sunumunda seçilmiş olan denetim yaklaşımını açıklarken diğer ülkelerde benimsenmiş denetim metodolojilerini Şekil 6 da belirtildiği üzere açıklamıştır. Kendi yaklaşımlarını hazırlayan ülkeler olduğu gibi, Türkiye gibi Cobit'i baz alan ülkeler de bulunmaktadır.

Ülkeler	Benimsedikleri Yaklaşımlar
Finlandiya	"İç Kontrol ve Risk Yönetimi" İle İlgili Geliştirdikleri Kendi Standartları
Norveç	**CobiT** Baz Alınmıştır
Macaristan	**CobiT** Baz Alınmıştır
Çek Cumhuriyeti	IT Yönetişimi ve Operasyonel Risk Kapsamında Sınırlı Düzenlemeler
Makedonya	**ISO 17799** Baz Alınmıştır
Slovakya	Her Yıl Bilgi Sistemleri Güvenliğini Kapsayacak Bir Denetim Raporu
Danimarka	Finansal Denetimin Yanında Sistem, Operasyon, Veri ve İş Devamlılığı Denetimi
Portekiz	Üç Yılda Bir BS Denetimi Yapılmasını Zorunlu Kılan Kanun Tasarısı
İsrail	**ISO 17799** Baz Alınmıştır
Hollanda	Sınırlı Anlamda BS Denetimi'ne de Referansta Bulunan Standardlar
İtalya	Sınırlı Anlamda 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

Şekil 6: Diğer Ülkelerin Bilgi Sistemleri Denetiminde Benimsedikleri Yaklaşımlar

Kaynak: Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi/ Mevzuat Çerçevesinde BDDK Perspektifi Türkiye İç Denetim Enstitüsü, XI. Türkiye İç Denetim Kongresi Sunumu 9 Kasım 2007, İstanbul Ahmet Türkay VARLI/

Cobit Her bir süreçte aşağıdaki tanımlar yapılmıştır:

- Prosesin hedefleri
- Proses Sahipliği
- Süreç tekrarlanabilirliği
- Roller ve Görevler
- Politika, Plan ve Prosedürler
- Sürecin performans iyileştirmesi

2.7.4.1.1. CobiT 5

Bilgi Sistemleri Denetim ve Kontrol Birliği ("Information Systems Audit and Control Association – ISACA") yönetim kurulunun, tüm ISACA ürünlerinin ve bilgi birikiminin bir araya getirilmesi amacıyla oluşturmaya başladığı Control Objectives for Information and related Technology ("CobiT") 5 BT Yönetişim Çerçevesinin 2011 sene sonu itibarıyla yayınlanması planlanmaktadır.

Bilgi ve ilgili teknolojilere ilişkin kurumsal seviyede daha etkin bir yönetim ve yönetişim kurulmasını hedefleyen CobiT 5 Çerçevesi, bu amaçla ISACA'nın değer yönetimi (Value IT), risk yönetimi (Risk IT), BT güvence Çerçevesi (IT Assurance Framework - ITAF) gibi diğer ürünlerini de kendi yapısı dahilinde bir araya getirmektedir.[40]

Özelikle Bankacılık Düzenleme ve Denetleme Kurumu'nun ("BDDK"), CobiT'i denetim standardı olarak kullandığı ve diğer düzenleyici kurumların da benzer hazırlıklar içinde olduğu düşünüldüğünde, bu değişimin Türkiye'de de oldukça fazla kurumu etkileyeceği açıkça görülmektedir.

Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ Madde 3 'ı' fıkrasında " COBIT: Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından yayınlanmış olan Bilgi Teknolojilerine İlişkin Kontrol Hedefleri'nin(COBIT) güncel versiyonunu" kullanılacağı belirtilmiştir.

Cobit'in 5.versiyonun çıkması Yönetim Beyanı çalışmalarını da etkileyecektir. 2012 yılının başlarında yayınlanması planlanan COBIT 5, 4.1 versiyonundan birçok farklılıklar içeriyor.

Kapsamı genişleyen yayın, içeriğine:

- Val IT Framework: Yaratılan değeri yönetilmesi,
- Risk IT Framework: Bilgi teknolojileri risklerinin yönetilmesi için çerçeve,
- BMIS (Business Model for Information Security): Bilgi güvenliğinin yönetilmesi için iş bakış açısı,
- ITAF (IT Assurance Framework): Bilgi teknolojilerinin ortaya koyduğu yararların güvence altına alınması

[40] "CobiT 5, Yakın Bir Zamanda Hayatımızdaki Yerini Alacak! ", http://www.pwc.com/tr/tr/service/it-services/cobit-bes/index.jhtml [12.11.2011]

bakış açılarını ekliyor. Dolayısıyla yeni çerçeve, 4.1 versiyonundan daha kapsamlı olmasıyla beraber COBIT 5 uyumunu sağlayabilmek için de kapsamlı bir çalışmayı beraberinde getirecektir.[41]

[41] "Cobit5 Taslak Dokümanları Yayınlandı ", http://blog.lostar.com/2011/07/cobit5-taslak.html [13.11.2011]

3.YÖNETİM BEYANI UYGULAMASI

Dünyada yaşanan büyük mali skandallar sonrası bankacılık sistemi düzenleme kurumları ülkelerindeki denetim ve kontrol mekanizmalarını kuvvetlendirmek adına bazı güçlü adımlar atmak durumunda kalmışlardır. Bunların başında ABD'deki SOX, Japonya'daki J-Sox, Kanada'da BILL98, Almanya'da "German Corparate Governance Code" gibi kanuni düzenlemeler yapılmıştır. Türkiye'de ise benzeri bir düzenleme BDDK tarafından 13 Ocak 2010 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik" ile Bankalar için her yıl Ocak ayında "Yönetim Beyanı" hazırlama ve bu beyanı ilgili bağımsız denetim kuruluşuna sunma yükümlülüğü getirilmiştir. 1 Ocak 2011'den itibaren başlayacak çalışmalar ile Yönetim Kurulu kararı şeklinde Bağımsız Denetim Kuruluşuna sunulacak beyanlar 2012 yılının Ocak ayında yapılacaktır. Bu konudaki detay düzenleme BDDK tarafından 30 Temmuz 2010 tarihinde yayımlanan bir genelge ile yapılmıştır. Bu düzenleme ile getirilen en büyük değişiklik, Bankaların yönetim beyanına mesnet teşkil edecek iç denetim faaliyetlerinin ilgili yönetmelikte tanımlanan bağımsız denetim kuruluşlarının denetim yaklaşımları ile aynı yöntemler kullanılarak gerçekleştirilmesi zorunluluğudur. "Süreç" ve "kontrol testi" kavramları da bu değişikliğin yine en büyük alt parçalarını oluşturmaktadır. Süreç Denetimi ve Kontrol Noktalarının Testi Getirilen yeni düzenleme kapsamında banka iç denetim birimlerinin çalışma yöntemlerinde yeni bir dönem başlamaktadır. Bu yeni dönemde denetim çalışmalarının planlanmasından gerçekleştirilmesine kadar pek çok alanda ciddi değişiklikler olacağı tabiidir. Bu değişikliklerin başında;[42]

• Önemlilik değerlendirmesi ve denetim planlaması

• Denetim çalışmaları ve kontrol testleri

• Denetim kanıtlarının saklanması

[42] KPMG Gündem, age. 24

• Bulgu sınıflandırmaları ve aksiyonlar gelmektedir. Beyana mesnet teşkil edecek çalışmaların gerçekleştirilmesi ve denetimler gerçekleştirilirken dikkate alınması gereken en önemli adımlar şu şekilde sıralanabilir:

• Denetim alanı olarak süreçlerin ele alınması

• Süreçler içerisinde yer alan ve süreçteki risk noktalarını azaltmak amacıyla oluşturulmuş kontrollerin belirlenmesi

• Bu kontrollerin yeterli olup olmadığına ve etkin bir şekilde çalışıp çalışmadığına yönelik testlerin planlanması / gerçekleştirilmesi

• Kontrollere ilişkin doküman ve kanıtlar ile testlere ilişkin doküman ve kanıtların saklanması

• Tespit edilen eksikliklerin bağımsız denetim kuruluşları tarafından da kullanılan sınıflandırma kriterleri doğrultusunda sınıflandırılması ve iyileştirici aksiyon alınmasının sağlanması. Bu durum iç denetim birimlerinin karşısına kısa vadede üzerinde düşünülmesi, orta vadede de üstesinden gelinmesi gereken bazı önemli zorluklar da çıkmaktadır. Bu zorluklar da;

1. Hali hazırda yürüyen çalışmalar ile düzenleme gereği yapılması gereken çalışmaların koordinasyonu
2. Birden fazla denetim yönteminin bir arada uygulanması aşamasında kaynak verimliliğinin sağlanması
3. Bağımsız denetim ile benzer yöntemleri uygularken farklı risklere odaklanan bakış açısının yitirilmemesi olarak özetlenebilir.[43]

Yönetim Beyanı uygulamasına yönelik detay açıklamalar, 30.07.2010 tarihinde BDDK tarafından yayınlanan BSD B.02.1.BDK.0.77.00.00.010.06.02/3 sayılı BSD.2010/3 Genelge'de yer almıştır.

[43] age.45

Bankalarda bağımsız denetim kuruluşlarınca gerçekleştirilecek bilgi sistemleri ve bankacılık süreçleri denetimine (BSD) ilişkin usul ve esaslar, 13.01.2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik" (Yönetmelik) ile düzenlenmektedir. [44]

Yönetmeliğin 19 uncu maddesinin yedinci fıkrası ile 33 üncü maddesinin birinci fıkrası uyarınca bankalar, bilgi sistemleri ve bankacılık süreçleri üzerindeki iç kontrolleri hakkında denetim dönemi itibariyle yönetim kurullarınca düzenlenecek Yönetim Beyanını bağımsız denetçiye sunmakla yükümlüdür.

Denetlenenin yükümlülükleri; MADDE 19 , (7) Denetlenen, iç kontrolleri hakkında denetim dönemi itibariyle güvence veren ve yönetim kurulu tarafından onaylanmış olan yönetim beyanını denetçiye sunmakla yükümlüdür.

Yönetim beyanı;

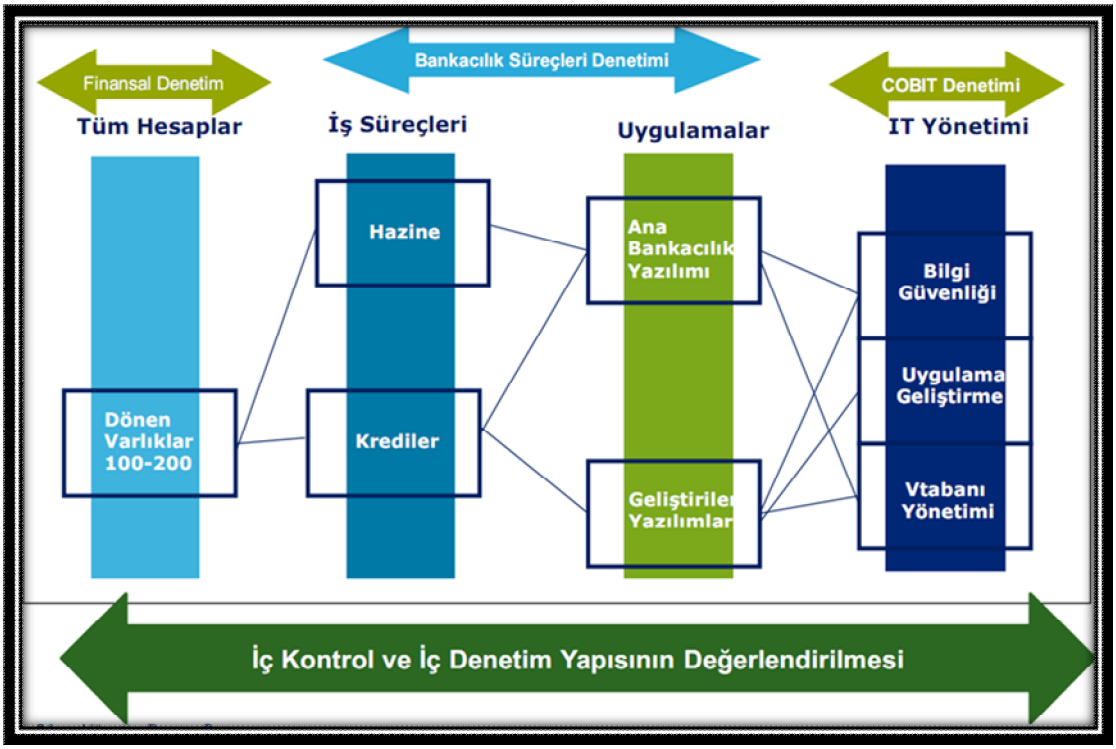
> Madde 33, (1) Banka, bilgi sistemleri ve bankacılık süreçleri üzerindeki iç kontrolleri hakkında denetim dönemi itibariyle yönetim kurulu tarafından düzenlenen yönetim beyanını denetçiye sunar.

"Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik" (Yönetmelik) içerisinde açıklandığı üzerine ilgili maddeler uyarınca yükümlülük açıkça belirlenmiştir.

2011 yılından itibaren Bankalar, bilgi sistemleri ve bankacılık süreçleri üzerindeki iç kontrol sonuçlarını içeren Yönetim Beyanı'nı bağımsız denetçiye sunmakla yükümlü olmuşlardır.

[44] BDDK (Bilgi Yönetimi Dairesi), Yönetim Beyanı Genelgesi, Genelge (BSD.2010/3, 30.07.2010),1.

Bu beyanda, bilgi sistemleri ve bankacılık süreçlerindeki iç kontrollerin etkinlik, yeterlilik ve uyumluluk açısından değerlendirilmesinin sonuçları yer alacaktır.



Şekil 7: Finansal Denetim Banka Süreçleri Denetimi ve Cobit Denetimi ilişkisi

Kaynak: Deloitte, Yönetim Beyanı Hakkında Eylül 2010, Oktay Aktolun, Evren Sezer, Cüneyt Kırlar Eylül 2010, İstanbul

Yönetim Beyanı denetiminin diğer tüm denetim süreçleri ile olan ilişkisi yukarıdaki şekil 7 de görülebilmektedir. Yönetim Beyanı kapsamında Banka Süreçleri Denetimi ve Cobit Denetimi girmektedir. Finansal Denetim iş süreçlerinin üzerinde çalıştığı Uygulamalar yani Bilgi Sistemlerinin yeterli, etkin çalışması sayesinde doğru bilgiler sunabilecek ve denetimleri yapılabilecektir.

3.1. Yönetim Beyanı'na Hazırlık Çalışmaları

Türkiye'de hizmet veren BDDK iznine sahip danışmanlık ve bağımsız denetim faaliyetlerinde bulunabilen Pwc'nin Bankalarda ilk kez yapılacak olan Yönetim Beyanı'na yönelik bilgilendirme toplantılarında banka yetkililerine iletmiş oldukları Yönetim Beyanı hazırlık yöntemi, Deloitte tarafından aynı şekilde Yönetim Beyanı kapsamında verebilecekler denetim ve danışmanlık hizmetlerinin sunumları ve Pwc'nin

de yapmış olduğu gibi kendi Yönetim Beyanı hazırlık çalışmalarını bankalara sunmuşlarıdır.

Bankalar Yönetim Beyanını hazırlarken yukarıda bahsi geçen firmaların yanında BDDK tarafından bankalarda bağımsız denetim ve danışmanlık verme lisansı verilmiş tüm firmalardan bankaların bu konuda danışmanlık veya denetim desteği almalarına izin verilmiştir.

Bankalar danışmanlık hizmeti almış oldukları bağımsız denetim kuruluşlarından aynı zamanda denetim hizmeti alamazlar. Danışmanlık kapsamlarını bankalar istedikleri şekilde içerik belirleyebilirler.

Pwc Yönetim Beyanı hazırlık çalışmalarını aşağıda belirtildiği üzere açıklanmaktadır.

1. Risk Değerlendirmesi

- İş Akışları ve Risk-Kontrol Matrisleri

2. Denetim Kapsamının Belirlenmesi

3. Denetim Planının Hazırlanması

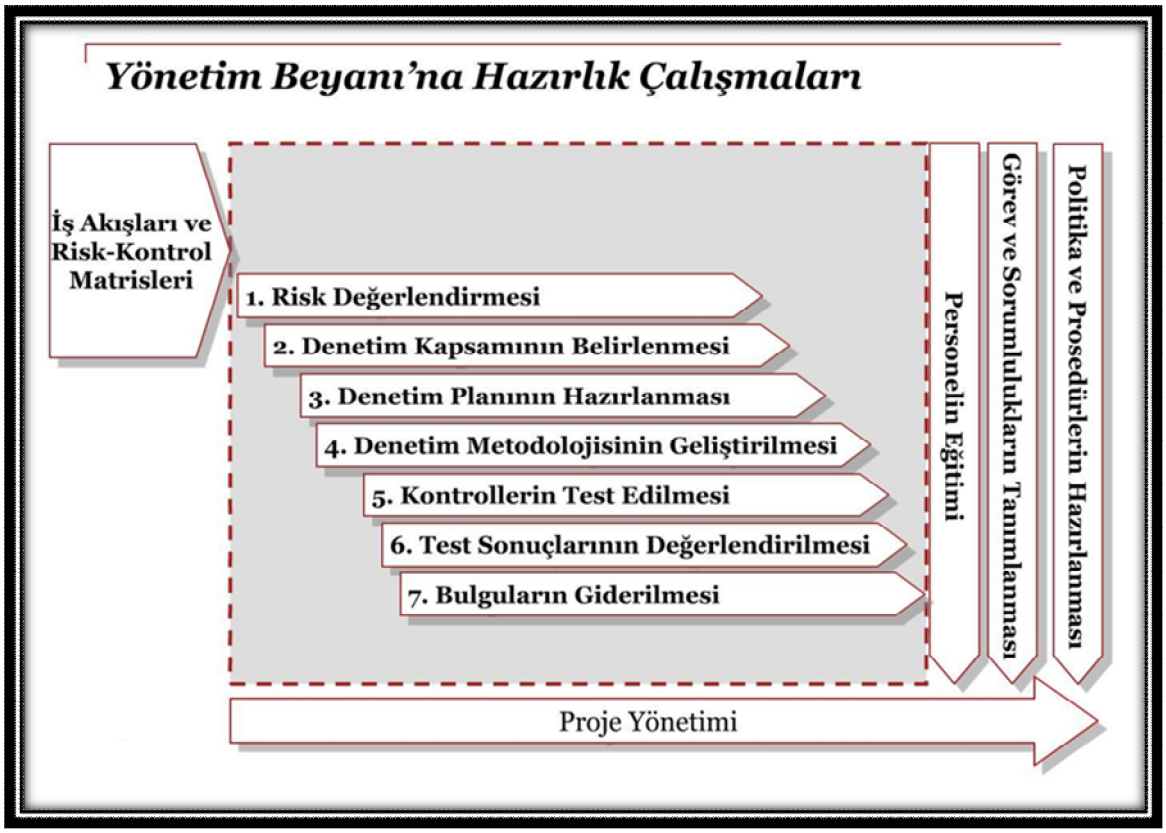
- Personelin Eğitimi
- Görev ve Sorumlulukların Tanımlanması
- Politika ve Prosedürlerin Hazırlanması

4. Denetim Metodolojisinin Geliştirilmesi

5. Kontrollerin Test Edilmesi

6. Test Sonuçlarının Değerlendirilmesi

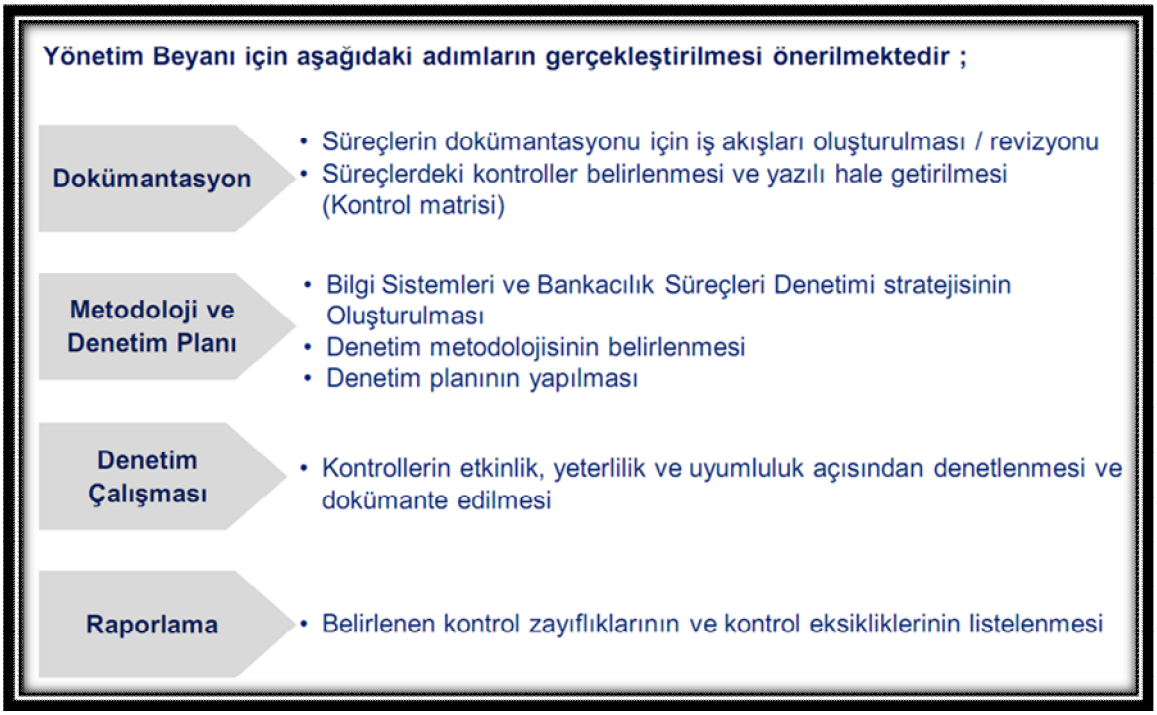
7. Bulguların Giderilmesi



Şekil 8 : PricewaterhouseCoopers Yönetim Beyanı Hazırlık Çalışmaları

Kaynak: ISACA-İstanbul yönetim beyanı sunumu http://www.slideshare.net/ISACA-Istanbul/isacaistanbul-ynetim-beyan-sunumu-29032011

Yukarıdaki şekilde önemli bazı öğeler bulunmaktadır. Özellikle tüm süreç boyunca Personel Eğitiminin devam etmesi önemlidir. Yönetim Beyanını hazırlayan personel yüksek yetkinlikte olmalı özellikle süreç denetimi konusunda deneyim sahibi olmalı veya ilgili denetim metodolojileri gerekli eğitimler sağlanarak denetçilere sunulmalıdır.



Şekil 9 : **Deloitte Yönetim Beyanı hazırlama çalışma adımları**

Kaynak:http://www.deloitte.com/assets/DcomTurkey/Local%20Assets/Documents/turkey-tr-ev-BankalardaYonetimBeyanToplanti_200910.pdf

Deloitte Yönetim Beyanı hazırlık çalışmalarını 4 aşamada oluşturmuştur.

1.Aşama; BSD stratejisinin oluşturulması

2.Aşama; Risk Değerlendirmesi

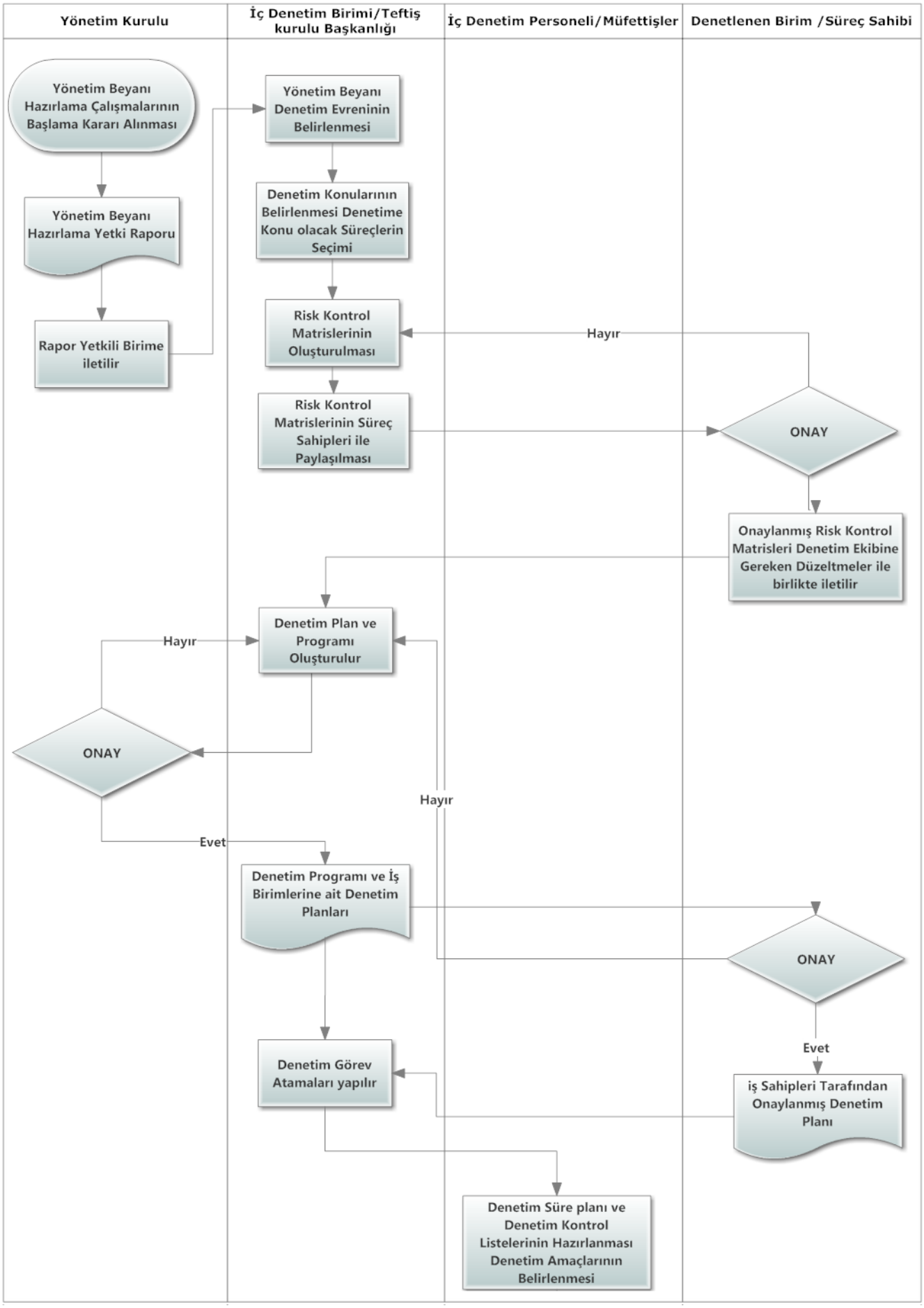
3. Aşama; Sonuçların Önemlilik Aşısından Değerlendirilmesi

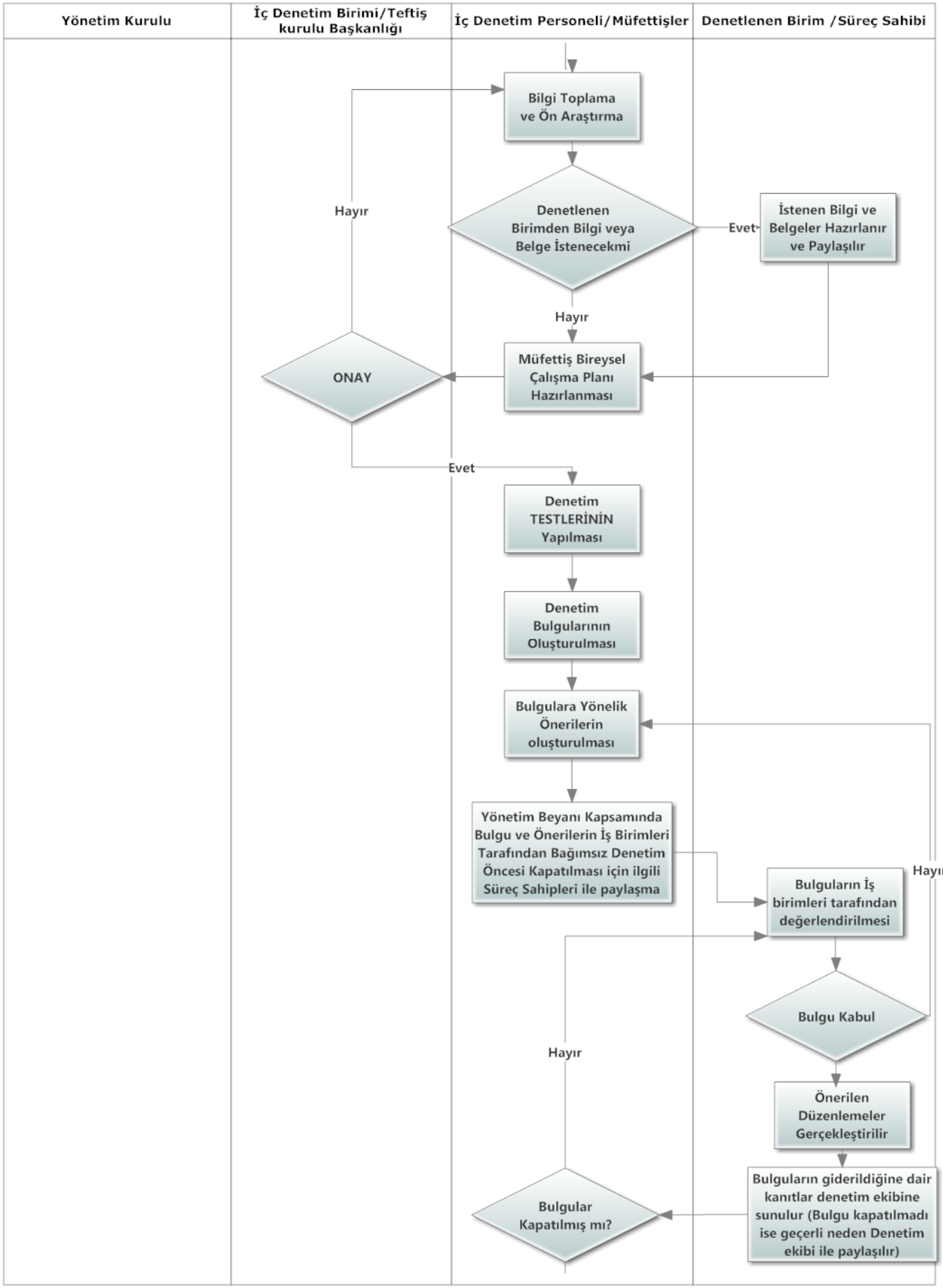
4.Aşama; BSD Planının Oluşturulması[45]

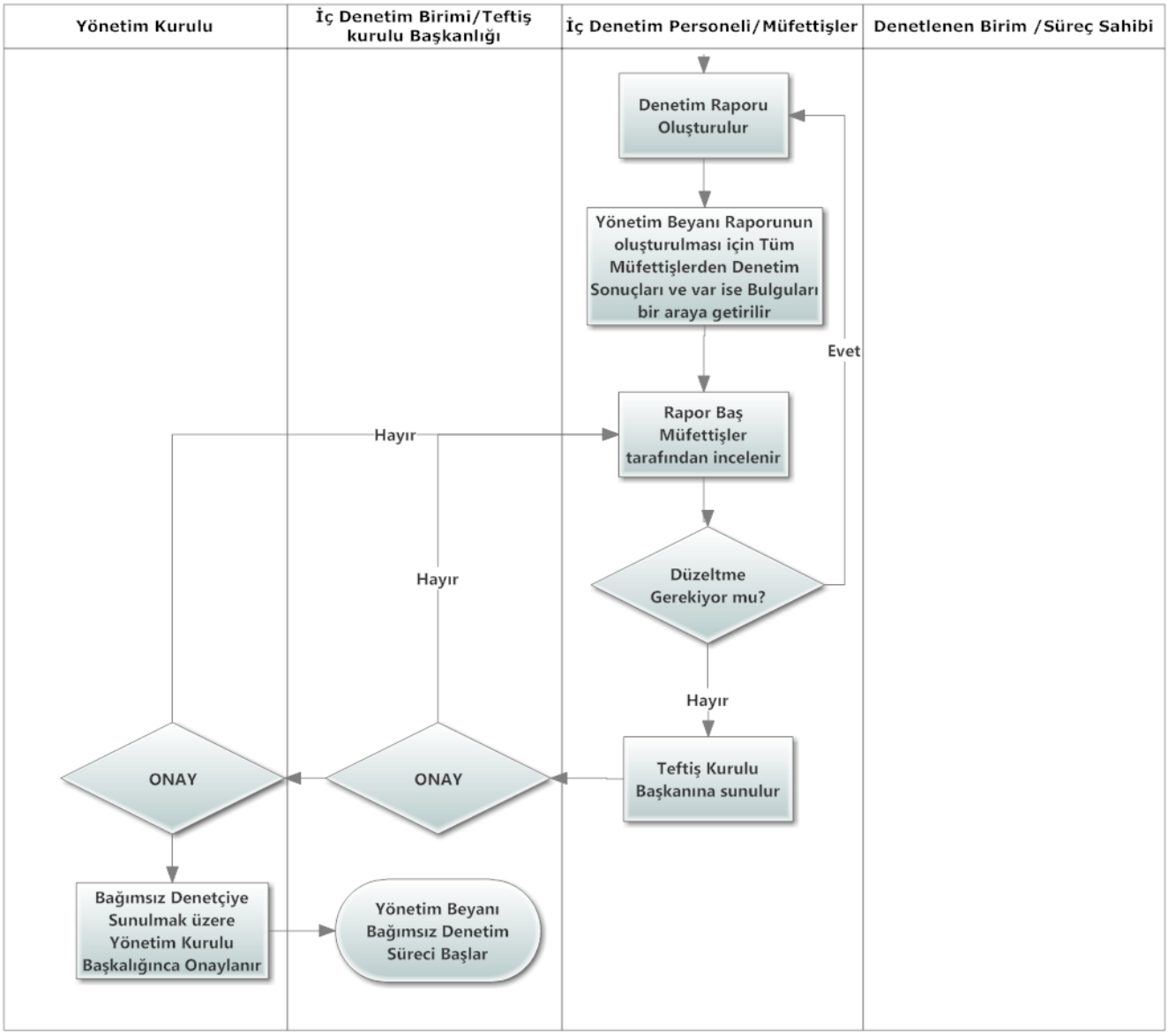
Deloitte ve Pwc'nin Bankacılara sunmuş oldukları Yönetim Beyanı hazırlama çalışmaları genel olarak benzerlik göstermektedir. Her iki süreçte de ilk adımda gerekli onaylanmış dokümantasyon (İş Akışları ve Kontrol Matrisleri) oluşturulup gerekli denetim ön çalışmalarının gerçeklenmesi ve test sonuçların paylaşılması alt süreçlerini içermektedir.

Yönetim Beyanı Hazırlama çalışmalarının Yönetim Kurulu, Yetkili İç denetim Birimi /Teftiş Kurulu, İç Denetim Personeli/ Müfettişler, Denetlenen Bitim /Süreç Sahibi gibi rol bazlı tüm sürecin taslak olarak oluşturulduğu akış şeması oluşturulmuştur. Şema her hangi bir bankada uygulanabilecek Yönetim Beyanı hazırlama çalışmaları sürecine örnek teşkil edebilir.

[45] Oktay Aktolun, Sezer E.,Kırlar C., **Yönetim Beyanı Hakkında** (İstanbul: Deloitte, 2010)


Yönetim Kurulu
İç Denetim Birimi/Teftiş kurulu Başkanlığı
İç Denetim Personeli/Müfettişler
Denetlenen Birim /Süreç Sahibi
Yönetim Beyanı Hazırlama Çalışmalarının Başlama Kararı Alınması
Yönetim Beyanı Hazırlama Yetki Raporu
Rapor Yetkili Birime iletilir
Yönetim Beyanı Denetim Evreninin Belirlenmesi
Denetim Konularının Belirlenmesi Denetime Konu olacak Süreçlerin Seçimi
Risk Kontrol Matrislerinin Oluşturulması
Risk Kontrol Matrislerinin Süreç Sahipleri ile Paylaşılması
Hayır
ONAY
Onaylanmış Risk Kontrol Matrisleri Denetim Ekibine Gereken Düzeltmeler ile birlikte iletilir
Denetim Plan ve Programı Oluşturulur
Hayır
ONAY
Hayır
Evet
Denetim Programı ve İş Birimlerine ait Denetim Planları
ONAY
Evet
Denetim Görev Atamaları yapılır
iş Sahipleri Tarafından Onaylanmış Denetim Planı
Denetim Süre planı ve Denetim Kontrol Listelerinin Hazırlanması Denetim Amaçlarının Belirlenmesi


Yönetim Kurulu
İç Denetim Birimi/Teftiş kurulu Başkanlığı
İç Denetim Personeli/Müfettişler
Denetlenen Birim /Süreç Sahibi
Bilgi Toplama ve Ön Araştırma
Denetlenen Birimden Bilgi veya Belge İstenecekmi
Evet
İstenen Bilgi ve Belgeler Hazırlanır ve Paylaşılır
Hayır
Hayır
Müfettiş Bireysel Çalışma Planı Hazırlanması
ONAY
Hayır
Evet
Denetim TESTLERİNİN Yapılması
Denetim Bulgularının Oluşturulması
Bulgulara Yönelik Önerilerin oluşturulması
Yönetim Beyanı Kapsamında Bulgu ve Önerilerin İş Birimleri Tarafından Bağımsız Denetim Öncesi Kapatılması için ilgili Süreç Sahipleri ile paylaşma
Bulguların İş birimleri tarafından değerlendirilmesi
Hayır
Bulgu Kabul
Hayır
Önerilen Düzenlemeler Gerçekleştirilir
Bulguların giderildiğine dair kanıtlar denetim ekibine sunulur (Bulgu kapatılmadı ise geçerli neden Denetim ekibi ile paylaşılır)
Bulgular Kapatılmış mı?



Şekil 10: Yönetim Beyanı Hazırlama Çalışmaları Örnek Süreç Şeması

Yönetim Beyanı Hazırlama Çalışmalarına yönelik bir öneriyi şu şekilde belirtebiliriz;

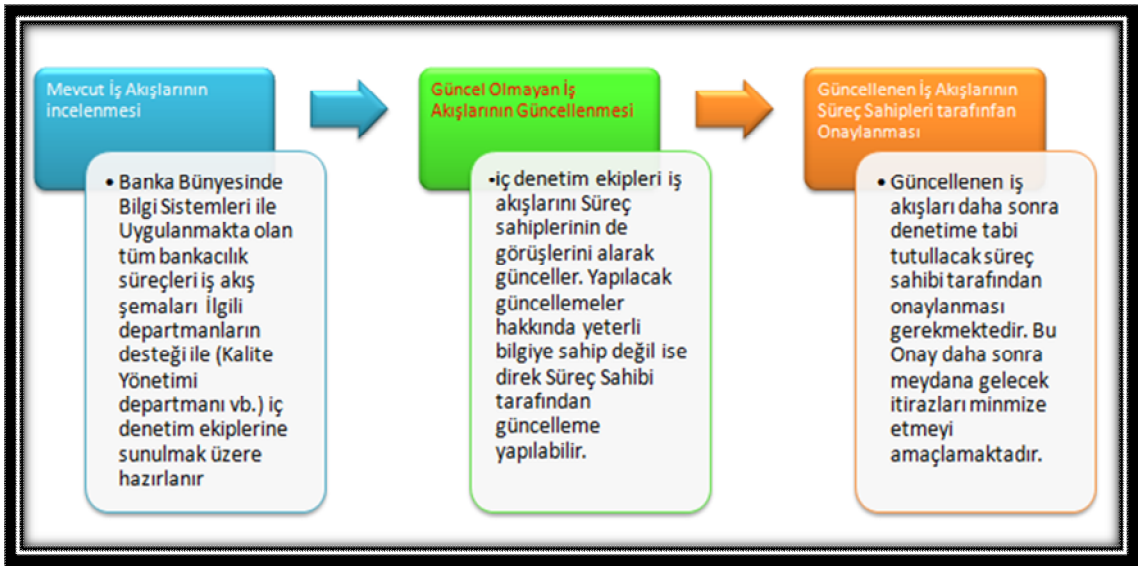
Aşamalar şekil 10'daki iş akışında da belirtildiği üzere detaylı olarak sırasıyla;

1.Yönetim Beyanı hazırlama yetki formu oluşturulur Ek 2. Yönetim Beyanı Yetkilendirme Bildirimi Teftiş kurulu başkanlığına iletilir.

2.Yönetim Beyanı Denetim Evreni Belirlenir. Denetlenecek Bankacılık ve Bilgi Sistemleri süreçleri tayin edilir.

3. İş Akışları ve Risk Kontrol Matrisleri Oluşturulur. (Bu aşamada İç Kontrol Başkanlığı ve Risk Komitelerinden destek alınabilir.)

3.1. Mevcut iş akışları güncellenir. Detayları şekil 11 de açıklanmıştır



Şekil 11: İş Akışları incelenmesi ve onaylanması süreci

4. İş Akışları ve Risk Kontrol Matrisleri süreç sahiplerine onaylatılır. Var ise gerekli değişiklikler yapılmış olarak teslim alınır. Ek 9. Yönetim Beyanı İş Akışı ve Risk Kontrol Matrisleri Süreç Sahibi Onay Tutanağı onaylatılır.
5. Yönetim Beyanı Denetim Çalışmaları plan ve programları hazırlanır. Bankacılık ve Bilgi Sistemleri denetimlerinin entegre bir biçimde işlemesi için denetim ekipleri toplantılar ile planlamada ortak stratejik plan oluşturmak üzerinde çalışırlar. (Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik , (13/1/2010 Sayı: 27461) Bilgi Sistemleri ve Bankacılık Süreçleri Denetiminde İşbirliği)
6. Oluşturulan plan ve programlar yönetim kurulunca onaylanır. (Bu adım 1 Nolu adımdaki yetkilendirme adımı bulunmasına rağmen sürecin yönetim kurulu tarafından izlenebilmesi için yapılabilir. Yetkilendirme yazısı bulunduğu için plan hazırlama ve uygulamada yetkilendirilen birim onay almayabilir.)
7. Denetim planı denetlenecek süreç sahipleri ile paylaşılır. Onay alma durumu yine bankadaki denetim mekanizmasına göre değişiklik gösterebilir. Çalışmalarını aksatmamaları için iş birimlerine denetlenecek süreçleri hakkında denetim planları sunmak iş birimleri için önemlidir. Teftiş sırasında tam destek sunmaları için de ayrıca önemlidir.

8. Denetim planları süreç bazlı detaylandırılarak müfettişlere atanır. Ek 3. Yönetim Beyanı Süreç Denetimi Süre Planı Beyan kapsamında çalışacak denetim ekibi ile paylaşılır.
9. Müfettiş Bireysel çalışma planını Teftiş Kurulu başkanı veya Baş müfettişine sunar ve onaylatır. Ek 3. Yönetim Beyanı Süreç Denetimi Süre Planı baz alınarak Ek 5. Yönetim Beyanı Bireysel Süreç Denetimi Süre Planı hazırlanır. Revizyon gerekiyorsa Ek 4. Yönetim Beyanı Denetim Süresi ve Kaynağı Revizyon Formu doldurularak Teftiş Kurulu Başkanlığına sunulur.
10. Denetlenecek birim ve Denetçiler ile açılış toplantısı yapılır. (Kısa süreçler için açılış toplantısı aynı zamanda test çalışmalarının tamamlandığı toplantı da olabilir) Örneği verilmiş olan Ek 6. Yönetim Beyanı Süreç Sahipleri İle Yapılan Açılış Toplantısı Tutanağı imzalanır.
11. Ek 5. Yönetim Beyanı Bireysel Süreç Denetimi Süre Planı dahilinde denetim adımları gerçekleştirilir. Müfettiş bilgi toplama ve ön araştırmalarını tamamlar. Denetlenecek birimden bilgi ve belge isteğini tedarik eder. Teftiş çalışmalarını tamamlar.
12. Testlerini Çalışma kağıtlarına rapor eder. Denetim kanıtlarını temin ederek düzenli bir şekilde sınıflandırır ve saklar. Belli bir standart sağlanması için çalışma kağıtları örnek olarak hazırlanan Ek 8. Yönetim Beyanı Müfettiş Örnek Çalışma Kağıdı gibi bit template kullanılabilir. Tüm denetim kanıtları süreç bazlı sınıflandırılarak arşivlenir. (Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik 13/1/2010 Sayı: 27461, Denetim çalışmalarının belgelendirilmesi Madde 35)
13. Test Çalışmaları sırasında Müfettişlerin Bulgu tespitleri sonrasında Bulgu formları tam olarak doldurulur.
14. Bulguya yönelik sınıflandırma ve öneriler gerekirse Baş müfettiş veya süreç hakkında bilgi sahibi olan Denetim ve Risk Komitesi üyelerinden görüş alınabilir. (Bulguların değerlendirilmesi, Yönetmelik Madde 32)
15. Test Çalışmaları ve Bulgular gözden geçirilerek süreç sahipleri ile paylaşılır. Kapanış Toplantısı Bulgu bulunmuyorsa yapılabilir. Ek 7. Yönetim Beyanı Süreç Sahipleri İle Yapılan Kapanış Toplantısı Tutanağı toplantı sonrası hazırlanır.

16. Süreç sahibi belirtilen süre içerisinde ilgili bulguyu red ya da kabul gerekçelerini ve yapılan öneriler çerçevesinde yapmış olduğu düzeltme çalışmaları ile birlikte denetim ekibine sunar.
17. Bulgular kapatıldı ise durumları oluşturulan formlarda güncellenir ve mutabakat sonuçları eklenir. Kapatılmayan bulgular raporlanmak üzere gerekçeleri ile birlikte raporlanır.
18. Tüm süreç denetim raporları bir araya getirilerek denetim içerik düzeni uyarınca sıralanır ve Baş Müfettişlerin incelemesi ve tüm hazırlıkların ardından beyan Teftiş Kurulu Başkanı onayına sunulur.
19. Teftiş Kurulu başkanı gerekiyorsa değişiklik yapılmasını isteyerek ilgili müfettişleri vazifelendirebilir.
20. Teftiş Kurulu Başkanı Onayına müteakip beyan Yönetim Kurula onaylatılmak üzere sunulur. Yönetim Kurulu gerekiyorsa değişiklik yapılmasını isteyerek Teftiş Kurulu Başkanlığına beyanı iletir.
21. Yönetim Kurulu tarafından onaylanmış Yönetim Beyanı Bağımsız Denetçiye sunulmak üzere hazırlanmış olur.

3.2. Yönetim Beyanı İçeriği

Yönetim Beyanının amacı, BSD.2010/3 Genelge'de "Banka yönetim kurulunun, bankanın bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontrollerinin BSD dönemi açısından etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, bu çerçevedeki mevcut durum ve yürütülen çalışmalara ilişkin güvence sunmasıdır."

Yönetim Beyanı hazırlanmasına yönelik denetim kapsamı, ana bankacılık süreçleri ve BT süreçleri ile dış destek hizmetlerini de içermelidir.

Yönetim Beyanı, denetim dönemini takip eden Ocak ayı sonuna kadar bağımsız denetim kuruluşuna iletilecek olup BSD raporu ile birlikte BDDK'ya gönderilecektir. Denetçi, denetim görüşünü oluştururken yönetim beyanını ve bu beyana mesnet teşkil eden çalışmaları inceleyecektir.

Yönetim Beyanında Yer Alacak Asgari Hususlar;

Banka yönetim kurulları, "Yönetim Beyanı"nı, beyan ettikleri hususlara ilişkin yeterli kanıtlar beraberinde olmak koşuluyla bağımsız denetçilere sunacaklardır. Yönetim beyanına mesnet teşkil edecek çalışmaların yürütülmesinde iç sistemler birimleri, yani iç denetim, iç kontrol ve risk yönetimi birimleri görevli olacaklardır.

- Yönetim kurulunun etkin ve yeterli bir iç kontrol sistemini banka bünyesinde tesis etme ve yürütme yükümlülüğü

- İç kontrol sisteminin inceleme ve değerlendirmeye tabi tutulduğu

- İç kontrol sisteminin değerlendirilmesi sürecinde, bağımsız denetim kuruluşunca gerçekleştirilmiş bulunan çalışmaların kullanılmadığı

- Var olması halinde, iç kontrol sisteminde yer alan önemli kontrol eksikliklerine ilişkin bulgular ve bu bulguların düzeltilmesine yönelik olarak banka tarafından yapılan çalışmalar

- Kritiklik seviyesine ve dönem sonu itibariyle düzeltilmiş olmasına bakılmaksızın, iç kontrol sistemine ilişkin tüm eksikliklerin bağımsız denetçilere sunumu

- Önceki dönem bağımsız bilgi sistemleri denetimlerinde tespit edilen, fakat henüz banka tarafından düzeltilmemiş bulunan bulguların güncel durumu şeklindedir.[46]

Banka, Yönetim Beyanı çerçevesinde bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin kanaat oluştururken, Yönetmeliğin 24 üncü maddesinde yer verilen bilgi sistemleri denetimi ve 25 inci maddesinde yer verilen bankacılık süreçleri denetimi kapsamını dikkate alır.

Şekil 12: Yönetim Beyanında açık ve net ifadeler ile bulunması gereken konular.

Kaynak: Deloitte, Yönetim Beyanı Hakkında Eylül 2010, Oktay Aktolun, Evren Sezer, Cüneyt Kırlar Eylül 2010, İstanbul

Deloitte'un Banka İç Denetim ekiplerini Yönetim Beyanı konusunda bilgilendirmek ve bu konuda verebilecekleri hizmetleri açıklamak için yaptıkları toplantıda yaptıkları sunumda Yönetim Beyanı içerisinde kesinlikle bulunması gereken hususlar şekil 12 de belirtilmiştir.

Sırasıyla Yönetim Beyanı iki ana başlık içinde hazırlanacaktır. Bunlar sırasıyla Yönetim Beyanı Bankacılık Süreçleri ve Yönetim Beyanı Bilgi Sistemleri Süreçleridir.

[46] Dr. Ender Aykut YILMAZ, "Bankalara Yönetim Beyanı Zorunluluğu", 25.08.2010 - 08:54, http://www.dunya.com/bankalara-yonetim-beyani-zorunlulugu_98522_haber.html

3.2.1. Yönetim Beyanı Bankacılık Süreçleri

Günümüz bankacılık faaliyetlerinin yürütülmesinde bilgi sistemlerinin önemi, her geçen gün artmaktadır. Banka bilgi sistemlerinin doğru bir şekilde yönetilmesi, izlenmesi ve denetlenmesi, bankacılık sektörünün faaliyetlerini gelişen bir şekilde sürdürebilmesi için vazgeçilmezdir.

Dünyada bankacılık otoriteleri, bilgi sistemlerinin denetimine yönelik olarak birçok yeni düzenlemeyi hayata geçirmektedirler. Ülkemiz bankacılık otoritesi Bankacılık Düzenleme ve Denetleme Kurumu da, bu anlamda birçok düzenleme gerçekleştirmiştir. Dinamik bir yapıya sahip olan bu süreç, ortaya çıkan gereksinimler çerçevesinde şekillenmektedir.

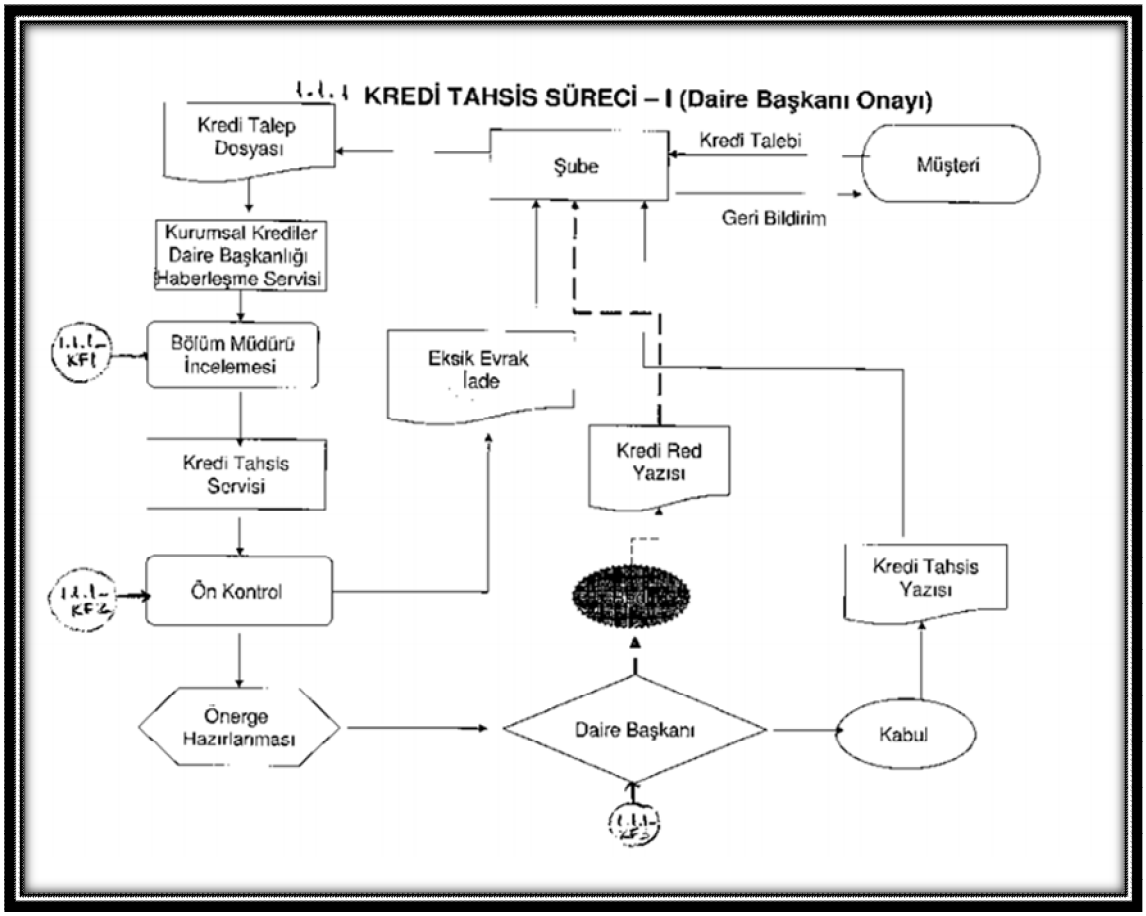
Banka yönetim kurulları, 2011 yılından itibaren bağımsız bilgi sistemleri denetçilerine verecekleri "Yönetim Beyanı" ile birlikte, banka bilgi sistemleri ve bankacılık süreçleri üzerinde tesis edilmiş olan iç kontrollerin etkinliğine ilişkin güvence vereceklerdir. [47]

Örnek Bankacılık Süreçleri;

- Hazine Süreçleri
- Kredi Süreçleri
- Mevduat Süreçleri
- Alternatif Dağıtım Kanalları Süreçleri
- EFT ve SWIFT Süreçleri
- Muhasebe Süreçleri
- Mali Kontrol Süreçleri
- Menkul Kıymetler
- Fon Yönetimi

Şeklinde sıralanabilir.

[47] Dr. Ender Aykut YILMAZ, Bankalara "yönetim beyanı" zorunluluğu, 25.08.2010 - 08:54, http://www.dunya.com/bankalara-yonetim-beyani-zorunlulugu_98522_haber.html



Şekil 13: Örnek bankacılık süreci akış şeması. Kredi Tahsil Süreci

Kaynak: Deloitte, Yönetim Beyanı Hakkında Eylül 2010, Oktay Aktolun, Evren Sezer, Cüneyt Kırlar Eylül 2010, İstanbul

13.01.201 tarih, 27461 sayılı Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik Madde 25 de Bankacılık süreçlerinde denetlenmesi gereken kontroller süreç bazlı verilmiştir.

> **MADDE 25 –** (1) Denetçi, denetlenenin bankacılık süreçlerini ve bu süreçler üzerindeki iç kontrollerini, önemlilik kriterini esas alarak belirlediği kapsam dâhilinde uyumluluk, etkinlik ve yeterlilik açısından incelemeye tâbi tutar.
> (2) Bankacılık süreçlerinin denetimi kapsamında bankacılık faaliyetlerine ilişkin aşağıda yer alan süreçler ve gerekli görülen diğer süreçler ile ilgili hususlar önemlilik kriteri çerçevesinde dikkate alınarak değerlendirilir.
> a) Mevduat Süreci: Mevduat hesaplarına ilişkin işlemler, çek/senet, fon transferi ve tahsilat işlemleri, mevduatın sınıflandırılması, tasarruf mevduatı kapsamının belirlenmesi ve tasarruf mevduatı sigorta primlerinin hesaplanması gibi

hesaplama kontrolleri, kara para aklanmasına ilişkin kontroller, işlemlerin muhasebeleştirilmesi ve süreçteki diğer kontrolleri,
b) Bireysel/Kurumsal Kredi Süreçleri: Kredi başvurularının alınması, değerlendirilmesi, kredi tahsisi ve kullandırımı işlemleri ve onayları, teminatlandırma, kredi limitleri ile kredi geri ödeme tabloları ve hesaplamalarına ilişkin kontroller, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, kredilerin sınıflandırılması, yaşlandırma raporlarının hazırlanması ve yeniden yapılandırma işlemleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,
c) Muhasebe Süreci: Faiz, gelir/gider tahakkuku ve reeskont hesaplamaları, işlem bazında tek düzen hesap planına uygunluk, amortisman hesaplamaları, muhasebe fişi kesilmesine ilişkin yetkilendirme süreci, mizanın oluşumu, geriye dönük muhasebe fişi kesilmesi işlemleriyle ilgili yetkilendirmelerin varlığı ve ilgili kayıtların bütünlüğü ve izlenebilirliği, işlem numaralarının ardışıklığının sağlanması, işlem limitlerinin ve yetkilerinin kontrolü, şube ve genel müdürlük kayıtları arasındaki mutabakatlar, hesap planı düzenleme ve değişikliklerine ilişkin kontroller, defteri kebir hesapları ile yardımcı, alt ve geçici hesapların mutabakatı, yasal ve yardımcı defterler arası mutabakatlar, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,
ç) Alternatif Dağıtım Kanalları Süreci: Elektronik bankacılık/alternatif dağıtım kanalları ile ilgili yetkilendirme, kimlik doğrulama, muhasebeleştirme ve diğer süreç kontrolleri,
d) Banka ve Kredi Kartları Süreci: Banka ve kredi kartı başvuru değerlendirme, limit tahsisi, kart basım ve dağıtım işlemleri, üye işyeri ve POS işlemleri, kartların kullanımı ve hediye puanı gibi uygulamalara ilişkin kontroller, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, yaşlandırma raporlarının hazırlanması ve yeniden yapılandırma işlemleri, banka ile kart merkezi mutabakatları gibi mutabakat kontrolleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,
e) Finansal Raporlama Süreci: Banka kayıtlarının ve bilgi kaynaklarının finansal raporlamalarda kullanım sürecinin kontrolü ve diğer süreç kontrolleri,
f) Ödeme Sistemleri Süreci: EFT, EMKT, Takasbank, SWIFT işlemleri ve bunlarla ilgili güvenlik kayıtları gibi ödeme sistemi kontrolleri, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri,
g) Hazine/ Menkul Kıymetler ve Fon Yönetimi Süreci: Menkul kıymet ve fon yönetimi iş süreçlerinin kontrolü, türev ürünleri, nostro, vostro ve loro bakiyelere ilişkin mutabakatlar ve muhabir kayıtlarının kontrolü, işlemlerin muhasebeleştirilmesi ve diğer süreç kontrolleri.
(3) Bankacılık süreçleri üzerindeki kontrollerin etkinliği, ilgili bilgi sistemleri genel kontrollerinin etkin ve yeterli olmasına bağlıdır. Bu nedenle denetçi, bankacılık süreçleri üzerindeki kontrollerin uyumluluk, etkinlik ve yeterliliğine ilişkin incelemelerde bulunurken, gerekli gördüğü bilgi sistemleri genel kontrollerinin etkinlik ve yeterlilik durumunu dikkate alır. Denetçi söz konusu genel kontrolleri, denetim kapsamına dâhil eder, etkinlik ve yeterlilikleri ile bankacılık süreçleri üzerindeki kontrollere olan etkilerini değerlendirir.
(4) Denetçi ikinci fıkrada ifade edilen ve önemlilik değerlendirmesi sonucunda denetim kapsamına dahil ettiği süreçler için asgari olarak aşağıdaki kontrolleri test eder;
a) Yönetimce kontrollerin etkin olarak çalışmasının engellenmesini önleyecek ya da tespit edecek kontroller,

b) Denetlenenin bilgi sistemleri genel kontrolleri ve bankacılık süreçlerindeki kontrollere ilişkin risk değerlendirme süreci,
c) Süreç ve işlemlerin sonuçlarının gözetimine ilişkin gözden geçirme, raporlama, sorgulama ve mutabakat gibi kontroller,
ç) Kontrollerin gözetimine yönelik kontroller,
d) Dönem sonuna ilişkin muhasebe ve finansal raporlama süreci üzerindeki kontroller,
e) Mükerrer bilgi sistemleri ve çift kayıt sistemi gibi sahtecilik ve usulsüzlüklerin önlenmesine ve tespit edilmesine ilişkin kontroller,
f) Faiz, masraf, komisyon, stopaj vs oran ve miktarları, vade ve valör bilgileri ile diğer önem arz eden bankacılık bilgilerine ilişkin veri, işlem ve kayıtların bütünlüğü ve güvenilirliğine ilişkin kontroller,
g) Görevler ayrılığı prensibinin uygulanmasına ilişkin kontroller,
ğ) Yetkilendirme ve erişim kontrolleri ile bu kontrollerin gözden geçirilmesine ilişkin kontroller,
h) Risk arz eden işlemlerin gerçekleştirilmesinde yer alan/yer alması gereken onay mekanizmaları,
ı) Veri, işlem ve kayıtların gizliliğine ilişkin kontroller,
i) Denetim izlerinin tutulması, güvenliğinin sağlanması ve düzenli olarak gözden geçirilmesi ve değerlendirilmesine ilişkin kontroller.

3.2.2. Yönetim Beyanı Bilgi Sistemleri Süreçleri

13.01.201 tarih, 27461 sayılı Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik Madde 24 de Bilgi sistemleri denetimi kapsamı ve benimsenen esas belirtilmektedir.

MADDE 24 – (1) Denetçi, bilgi sistemleri genel kontrollerini, önemlilik kriterini esas alarak belirlediği kapsam dâhilinde uyumluluk, etkinlik ve yeterlilik açısından incelemeye tâbi tutar.
(2) Genel kontroller, tesis edilmelerinde esas alınan çerçeve, standart ya da metodolojiden bağımsız olarak; bankalarda bilgi sistemleri yönetiminde esas alınacak ilkelere ilişkin Kurum tarafından yapılan düzenlemelerdeki hükümler gözetilerek, COBIT'e göre denetlenir.
(3) Genel kontrollerin uyumluluk, etkinlik ve yeterliliğine ilişkin inceleme çalışmalarını tamamlayıcı bir unsur olarak; olgunluk modeli çerçevesinde ilgili kontrol hedefine ilişkin sürecin olgunluk seviyesi de belirlenir. İlgili kontrol hedefine ilişkin sürecin olgunluk seviyesi değerlendirilirken süreci oluşturan detaylı kontrol hedeflerinin tamamı dikkate alınır.

Yönetim beyanının hazırlanması sürecinde bankacılık süreçleri ve bilgi sistemlerine ilişkin kontrollerin dokümantasyonunun yapılması ya da mevcut dokümantasyonun revize edilmesi, yönetim beyanı kapsamında banka iç sistemler birimleri tarafından gerçekleştirilecek denetim faaliyetlerine ilişkin denetim stratejisinin oluşturulması, denetim metodolojisinin belirlenmesi ve denetim planının hazırlanması ilk etapta gerçekleştirilecek adımlar arasında yer almaktadır. Akabinde, denetim faaliyetlerinin hazırlanan plan dahilinde gerçekleştirilmesi, kontrol zayıflıkları ve kontrol

eksikliklerinin listelenerek bağımsız denetçi ile paylaşılması, kontrol zayıflıkları ve kontrol eksikliklerine ilişkin aksiyon tarihlerinin belirlenmesi ve takip edilmesi, yönetim beyanının hazırlanması ve bağımsız denetçiye özellikle yönetim beyanını ve bu beyana mesnet teşkil eden çalışmaları inceleyecek zamanı verecek şekilde iletilmesi gerekecektir.[48]

Yönetim Beyanı Bilgi sistemleri süreçleri bankalar tarafından kendi bünyelerinde bulunan bilgi sistemleri yapısına göre Cobit süreçleri arasından seçecekleri süreçlerin risk kontrol matrislerini, kontrol hedeflerini ve kontrol çalışmasını planlayıp seçilen denetim yöntemine göre konusunda yetkin personele iş ataması yapılarak denetim çalışmalarının tamamlanması sürecini kapsar.

Cobit 4.1 içersisinde Cobit başlığı altında detaylı açıklandığı gibi 34 alt süreç bulunmaktadır. Bankalar bunlar arasından tamamen kendi bünyelerinde önem verdikleri uyguladıkları süreçleri seçmek durumundadırlar. 34 süreç içerisinde birbirine benzeyen alt süreçlerden dilediklerini ele alarak denetimlerini tamamlar.

Tamamlanan denetim çalışmaları seçilen süreçlerden çıkan Bulguların detaylı raporlanması çalışmalarını içerir. Bulgular ve bulgula yönelik denetçi önerisi ilgili BT süreç sahibi ile paylaşılır. BT süreç sahibi kendisine verilen süre zarfında ilgili Bulguyu gidermek için çalışmalar yapar. Yapılan çalışmaları Denetçiye raporlar. Denetçi süreçte ilgili bulgunun giderilmiş olup olmadığına ilişkin tekrar teftiş yapar. Giderilmiş ise mutabakata varıldığı hakkında Bulguyu kapatır.

Bağımsız Denetçi banka tarafından yapılacak Yönetim Beyanı Bilgi sistemleri tarafı çalışmalarında sürecin başından itibaren görüşmelerde bulunarak Cobit süreçleri içerisinden seçmiş oldukları ve yapılacak iç denetim hakkında bilgilendirme toplantıları yapar. Bu toplantı sonucu seçilen Cobit süreçlerinin bankanın BT yapısına uygun olduğu ve bağımsız denetim sırasında da yapılacak denetimde bankanın seçtiği çerçeve içinde yapılacağı hakkında görüş birliğine varılır.

Bağımsız Bilgi Sistemleri denetçileri yapacakları denetim sırasında karşılaşacakları uygulamalar ve sistemlerin denetlenmediği ve ilgili Cobit süreci kontrollerinin yapılmamış olduğunu görürse ilgili süreç hakkında da bulgu yazabilir. Sadece banka

[48] Köşe Yazarları Haberleri, Ekonometri Dergisi, http://www.ekonometri.com.tr/ index.php?page=habergoster&hbrID=670 [21.11.2011]

tarafından seçilmiş olan süreçler değil tüm bankacılık Bt süreçlerinin bağımsız denetimini geçekleştirmek üzere yapılan bu çalışma tüm Cobit süper setinde bulunan süreçleri içermektedir.

Cobit süreçleri arasından seçilebilecek tüm alt domainler aşağıda belirtildiği gibidir. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Endüstri Mühendisliği Yüksek Lisans programında yayınlanmış Emine Hacısüleymanoğlu'nun yüksek lisans tezi Cobit'in tüm süreçlerini açıklayan önemli bir çalışmadır. Cobit 4.1'in ana domainlerinin içerikleri hakkımda yorumlarından tez içerisinde faydalanılmıştır.

3.2.2.1. Planlama ve Organizasyon

Bu bölüm işletme amaçlarının gerçekleştirilebilmesi için Bilgi teknolojilerinin katkısının hangi yolla olması gerektiğini belirler. Bu bölümde strateji ve taktikler vardır. Stratejik planın gerçekçi olabilmesi için farklı açılardan ele alınması gerekir. Organizasyonun teknolojik açıdan altyapı uygunluğu incelenir. Planlama ve Organizasyon alanı teknoloji kullanımını ve kurumun amaç ve hedeflerini gerçekleştirmeye yardımcı olmak için nasıl en iyi şekilde kullanılabileceğini kapsamaktadır. Bu alan en uygun sonucu elde etmek ve bilgi teknolojileri kullanımından en iyi şekilde faydalanmak için bilgi teknolojilerinin alması gereken organizasyonel ve altyapısal şekli ortaya çıkartmaktadır.[49]

Planlama ve Organizasyon alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

PO1 Stratejik bir BT Planı Tanımlama

PO2 Bilgi Mimarisini Tanımlama

PO3 Teknolojik Yönü Belirleme

PO4 BT Prosesleri, Organizasyon ve İlişkilerini Tanımlama

PO5 BT Yatırımını Yönetme

PO6 Yönetim Hedefleri ve Yönünü Bildirme

PO7 BT İnsan Kaynaklarını Yönetme

PO8 Kaliteyi Yönetme

[49] Emine Hacısüleymanoğlu , "Bilgi Teknolojileri Yönetişim Yöntemleri ve Cobit ile Ulusal Bir Bankada Uygulaması", (Yüksek Lisans Tezi , Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü 2010),21.

PO9 BT Risklerini Değerlendirerek Yönetme

PO10 Projeleri Yönetme

- **Stratejik BT Planı Tanımlanması;** BT Değer Yönetimi, İş-BT Birlikteliği, Mevcut Durumun ve İmkânların Değerlendirilmesi, BT Stratejik Planı, BT Taktik Planları, BT Portföy Yönetimi
- **Bilgi Mimarisi Tanımlanması;** Bilgi Mimarisi Modeli,Kurumsal Veri Sözlüğü,Veri Sınıflama Sistemi, Güvenlik Seviyeleri
- **Teknolojik Yönelimi Belirlenmesi** Teknoloji Altyapı Planı Hazırlanması, Teknolojik Gelişmelerin İzlenmesi, Teknoloji Kullanım Standartlarının Belirlenmesi ve Yayınlanması
- **BT Süreçlerini, Organizasyonunu ve İlişkilerini Tanımlanması;** BT süreçlerinin belirlenmesi, BT Strateji Komitesi Oluşturulması, BT Organizasyonu, BT Görev Tanımları, Yetki ve Sorumluluklar, BT Kalite Sağlama Sorumlulukları, Risk, Güvenlik ve Uygunluk Sorumlulukları, Sistem ve Veri Sahipliği, Görevlerin Ayrıştırılması, IT Ekibi, Anlaşmalı çalışanlarla ilgili politika ve prosedürleri, Diğer bölümlerle ilişkiler
- **BT Yatırımlarını Yönetimi;** Finansal Yönetim Çerçevesi, BT Bütçesi, BT bütçesinde Önceliklendirme, Maliyet Yönetimi, Fayda Yönetimi
- **Yönetim Hedeflerinin ve Yönelimlerinin İletimi;** BT kuralları ve kontrol ortamı, Kurumsal BT riskleri ve kontrol ortamı, BT Politika Yönetimi, Politika, standart ve prosedürlerin açıklanması, BT hedeflerinin ve yönelimlerinin anlatılması
- **BT İnsan Kaynağının Yönetimi;** Personel Temini, Personel Yeteneklerinin Gelişimi, Rollerin personele dağıtılması, Personel Eğitimi, Kişi Bağımlılığının Azaltılması, Çalışanın İş Performansının Geliştirilmesi, İş Değiştirme ve Sonlandırma
- **Kalite Yönetimi;** Kalite Yönetim Sistemi, BT Standartları ve Kalite Uygulamaları, Geliştirme ve Temin Standartları, Müşteri Odaklılık, Sürekli İyileştirme, Ölçme, İzleme ve Gözden Geçirme
- **Risklerin Belirlenmesi ve Yönetimi;** BT Risk Yönetimi Çerçevesi, Risk İçeriğinin Oluşturulması, Olay Tanımlama, Risk Değerlendirme, Risk Cevaplama, Risk Eylem Planının Bakımı ve İzlenmesi

- **Proje Yönetimi**

  Proje Programı Yönetim Çerçevesi, Proje Yönetim Çerçevesi, Proje Yönetim Yaklaşımı, Paydaşların Onayı, Proje Kapsamı belirleme, Proje Safhalarını başlatma, Proje Planı, Projenin Kaynakları, Proje Risk Yönetimi, Proje kalite planı, Değişikliklerin Kontrolü, Güvence İşlemleri için Proje Planlama, Proje performansının ölçülmesi, raporlanması ve izlenmesi, Projeyi kapatmak

3.2.2.2. Tedarik ve Uygulama

Tedarik ve Uygulama alanı BT gereksinimlerini belirleme, teknolojiyi satınalma ve kurumun mevcut iş süreçlerine uyarlama için kurumun stratejilerini adreslemektedir. Bu alan aynı zamanda bilgi teknolojileri sisteminin ve parçalarının hayatını sürdürebilmesi için kurumun kabulleneceği bir bakım planı geliştirilmesini içermektedir. [50]

Tedarik ve Uygulama alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

AI1 Otomatize Edilmiş Çözümleri Tanımlama

AI2 Uygulama Yazılımını Temin Ederek Bulundurma

AI3 Teknoloji Altyapısını Temin Ederek Sürdürme

AI4 Çalışma ve Kullanımı Etkinleştirme

AI5 BT Kaynaklarını Elde Etme

AI6 Değişiklikleri Yönetme

AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu

- **Rutin Çözümlerin Tanımlanması;** İş fonksiyonlarının tanımlanması, bakımı ve teknik gereksinimler, Risk analiz raporu, Verimlilik öğretisi ve alternatif yolların formülize edilmesi, İhtiyaçlar, Verimlilik kararı ve onayı
- **Uygulama Yazılımlarının Temini ve Bakımı;** Üst seviye tasarım, Detaylı Tasarım, Uygulama kontrolü ve denetlenebilirlik, Uygulama güvenliği ve kullanılabilirlik, Sağlanan uygulamanın konfigürasyonu ve kurulumu, Mevcut sistemde ana güncellemeler, Uygulama yazılımı geliştirme, Yazılım kalite güvencesi, Uygulama gereksinim yönetimi, Uygulama yazılımının bakımı

[50] age.40

- **Teknoloji altyapısının Temini ve Bakımı;** Teknolojik alt yapı temin planı, Altyapı kaynaklarının korunması ve kullanılabilirliği, Altyapı bakımı, Verimlilik test ortamı
- **İşletim ve kullanıma İzin Verme;** Operasyonel çözümlerin planlanması, Yönetime bilgi aktarımı, Son kullanıcılara bilgi aktarımı, Operasyon ve destek personeline bilgi aktarımı
- **BT Satınalması;** Satınalma kontrolü, Tedarikçi kontrat yönetimi, Tedarikçi seçimi, BT kaynaklarının temini
- **Değişiklik Yönetimi;** Standart ve prosedürlerin değiştirilmesi, Etkinin değerlendirilmesi, önceliklendirme ve yetkilendirme, Acil durum değişiklikleri, Değişiklik durumunun takibi ve raporlanması, Değişikliğin kapatılması ve dökümante edilmesi
- **Kurulum ve Değişiklik;** Eğitim,Test Planı, Kurulum Planı, Test Ortamı, Sistem ve veri çevrimi, Değişikliklerin test edilmesi, Son onay testi, Yükseltim ve kullanıma alma, Kurulum sonrası gözden geçirmeler

3.2.2.3. Hizmet Sunumu ve Destek

Hizmet Sunumu ve Destek alanı bilgi teknolojilerinin teslim yönüne odaklanmaktadır. Bu alan bilgi teknolojileri sistemindeki uygulamaların hayata geçirilmesi ve sonuçları ile bu BT sistemlerinin etkin ve elverişli uyarlanmasını sağlayan destek süreçlerini de kapsamaktadır. Bu destek süreçleri güvenlik konuları ve eğitimini içermektedir.[51]

Hizmet Sunumu ve Destek alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

DS1 Servis Düzeyi Yönetimi

DS2 Üçüncü Parti Hizmetlerin Yönetilmesi

DS3 Performans ve Kapasite Yönetimi

DS4 Sürekli Hizmetin Sağlanması

DS5 Sistem Güvenliğinin Sağlanması

DS6 Maliyetlerin Tanımlanması ve Dağıtımı

DS7 Kullanıcıların Eğitimi ve Öğretimi

[51] age.52

DS8 Hizmet Masası ve Olaylar Yönetimi

DS9 Konfigürasyon Yönetimi

DS10 Sorun Yönetimi

DS11 Veri Yönetimi

DS12 Fiziksel Ortamların Yönetimi

DS13 Operasyonların Yönetimi

- **Hizmet Düzeylerinin Tanımlanması ve Yönetilmesi;** Service Düzeyi Yönetimi Çerçevesi, Servislerin Tanımlanması, Servis düzeyi anlaşmaları, Operasyon düzeyi anlaşmaları, Servis düzeylerinin gözlenmesi ve raporlanması, Servis düzeyi anlaşmalarının gözden geçirilmesi ve sözleşmeler
- **Dışarıdan Sağlanan Servislerin Yönetimi;** Tüm tedarikçi ilişkilerinin tanımlanması, Tedarikçi ilişki yönetimi, Tedarikçi risk yönetimi, Tedarikçi Performans İzleme
- **Performans ve Kapasite Yönetimi;** Performans ve kapasite planlama, Mevcut performans ve kapasite durumu, Gelecekteki performans ve kapasite, BT kaynak kullanılabilirliği, Gözlem ve raporlama
- **Hizmet Sürekliliğinin Sağlanması;** BT süreklilik çerçevesi, Süreklilik planı, Kritik BT Kaynakları, BT süreklilik planının bakımı, BT süreklilik planının test edilmesi, Süreklilik planı eğitimi, Süreklilik planının dağıtımı, Servisin kurtarılması ve devam ettirilmesi, Uzak yedekleme merkezi, Devamlılığın sağlanması sonrası gözden geçirme
- **Sistem Güvenliğinin Sağlanması;** BT güvenliğinin yönetilmesi, Güvenlik planı, Kimlik yönetimi, Kullanıcı yönetimi, Güvenlik testi, gözlem ve izleme, Güvenlik vaka tanımlama, Güvenlik teknolojisinin korunması, Kriptolama, Yabancı yazılım engelleme, tespit ve düzeltme, Network güvenliği, Duyarlı verinin değişimi
- **Maliyetlerin hesaplanması ve paylaştırılması;** Servislerin tanımlanması, BT muhasebesi, Maliyet modeli ve maliyetlendirme, Maliyet modelinin bakımı
- **Kullanıcı Eğitimleri;** Eğitim ihtiyaçlarının tanımlanması, Eğitimin sağlanması, Alınan eğitimin değerlendirilmesi

- **Olay ve Servis Masası Yönetimi;** Servis masası, Müşteri sorunlarının kaydedilmesi, Olayın ilgiliye yönlendirilmesi, Olayın kapanması, Raporlama ve trend analizi
- **Konfigürasyon Yönetimi;** Konfigürasyon havuzu, Konfigürasyon unsurlarının tanımlanması ve bakımı, Konfigürasyon tutarlılığı
- **Problem Yönetimi;** Problemleri tanımlama ve sınırlama, Problem izleme ve çözüm üretme, Problemi Kapama, Konfigürasyon, Olay ve Problem Yönetimi ile entegrasyon
- **Veri Yönetimi;** Veri yönetimi için iş gereksinimleri, Veri düzenleme, Ortam kütüphanesi yönetim sistemi, İmha etme, Yedekleme ve geri yükleme, Veri yönetimi için güvenlik yönetimi
- **Fiziksel Ortam Yönetimi;** Yer seçimi, Fiziksel güvenlik kriterleri, Fiziksel erişim, Çevresel etkenlere karşı koruma, Fiziksel araçların yönetimi
- **Operasyon Yönetimi;** Operasyon prosedürleri ve talimatları, İş takvimleme, BT Altyapısının izlenmesi, Önemli dokumanlar ve çıkış cihazları, Donanımın koruyucu bakımı

3.2.2.4. Gözlem ve Değerlendirme

Gözlem ve Değerlendirme alanı kurumun ihtiyaçlarını, mevcut BT sisteminin hedefleri karşılayıp karşılamadığını ve yasal gereksinimlerle uyumluluk için gerekli kontrolü tayin etmek için kurumun stratejilerini irdelemektedir. Gözlem ve Değerlendirme aynı zamanda bilgi teknolojileri sisteminin iş hedeflerini karşılamadaki etkinliği ile iç ve dış denetçilerce yapılan kurumun kontrol süreçlerinin bağımsız değerlendirmesi konularını kapsamaktadır.[52]

Gözlem ve Değerlendirme alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

ME1 IT Performansının Gözlemi ve Değerlendirmesi

ME2 İç Kontrol Gözlemi ve Değerlendirmesi

ME3 Yönetmeliklere Uyumluluğun Sağlanması

ME4 BT Yönetimi Sağlanması

[52] age.69

- **Bilgi Teknolojileri Performansını İzleme ve Geliştirme;** İzleme yaklaşımı, İzlenecek verinin tanımlanması ve toplanması, İzleme yöntemi, Performans değerlendirme, Üst yönetime raporlama, İyileştirici faaliyetler
- **İç Denetim İzlenmesi ve Geliştirilmesi;** İç denetim çerçevesinin izlenmesi, Denetimsel gözden geçirmesi, Kural dışı durumların denetlenmesi, İç değerlendirmenin denetimi, İç denetimin güvence altına alınması, Dışarıdan sağlanan iç denetim, İyileştirici faaliyetler
- **Dış Gereksinimlere Uyum Sağlanması;** Hukuki, düzenleyici ya da anlaşmalara dayanan dış zorunlulukların tanımlanması, Dış gereksinimlere verilen cevabın optimize edilmesi, Gereksinimlere cevabın güvence altına alınması, Entegre Raporlama
- **BT Yönetimi Sağlanması;** Bir BT Yönetimi Çerçevesi oluşturulması, Stratejik düzenleme, Değer sağlama, Kaynak Yönetimi, Risk Yönetimi, Performans ölçümü, Bağımsız denetim

Yukarıda bahsi geçen 34 Cobit sürecinin tamamının denetlenmesi bankalar için şart değildir. Ancak tamamımdan sorumludur. Cobit'de bazı alt süreçler birbirilerine benzer yapıdadırlar. Banka bünyesinde Teknoloji yapılanmaları alt yapıları ve almakta oldukları teknolojik üçüncü şahıs firmalar ile olan ilişkilerine göre kendi bünyelerime uyguladıkları tüm süreçleri seçmek ve denetlemek durumundadır.

İlgili süreçler banka bünyesinde bulunmasına rağmen denetimi yapılmamış ise Bağımsız Denetçi denetimlerini yapıp bankaya sunacağı görüşü kendi yapmış olduğu ve tespit etmiş olduğu bulgulara göre şekillendirebilir bunlara istinaden vereceği görüşü bildirir.

4. UYGULAMA

Yönetim Beyanı Kapsamında Bilgi Sistemi denetimi uygulama örneği sunmak üzere DS09 (Delivery & Support) Hizmet Sunumu ve Destek Konfigürasyon Yönetimi sürecinin denetim çalışmaları örneği verilecektir.

Yapılan örnek çalışma sonrası olası bulgular ve denetim çalışmaları her hangi bir banka adı verilmeden tahmini olarak girilmiştir.

4.1. Uygulamanın Problemi

Türkiye'de ilk kez 30 Ocak 2012 tarihinde Bağımsız Denetçilere sunulacak olan Yönetim kurulu tarafından onaylanmış içeriği hakkında detaylı bilgilerin verilmiş ancak ilgili beyanın formatının belirlenmesinde bankalara tanınan serbesti ve bu serbesti karşısında Yönetim Beyanı hakkında beyana mesnet teşkil edecek çalışmaların sunulması ve hazırlama çalışmalarından örnekler gösterilmesi.

4.2. Uygulamanın Amacı

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 30 Temmuz 2010 tarihinde yayımlanan "Yönetim Beyanı" konulu genelgeye göre her yıl Ocak ayı sonuna kadar, bir önceki yılın faaliyetlerine ilişkin olarak Banka Yönetim Kurulları tarafından, bankanın bilgi sistemleri ve bankacılık süreçleri üzerindeki içkontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin güvence veren ve kontrol zayıflıkları ve eksikliklerini içeren bir beyan hazırlanması ve bağımsız denetçiye sunulması gerekmektedir.

Bankaların ilk kez sunacakları Beyan için BDDK tarafından yayınlanmış bir format bulunmamaktadır. Bu konuda bankalar mevcut denetim metodolojilerini kullanarak kendi rapor formatlarını belirleyebileceklerdir. Denetleyecekleri Bankacılık ve Bilgi Sistemleri Süreçlerini bizzat kendileri seçecek olup uyguladıkları tüm bankacılık ve bilgi sistemleri süreçlerinin tamamından sorumlu olacaklardır. Bağımsız denetçiye sunulan beyana yönelik bağımsız denetim çalışmalarının ardından denetçi BDDK ya görüş belirtecektir.

Uygulamada her hangi bir bankanın DS09 kapsamında uygulayacağı denetimler Cobit Denetim metodolojisini sunan "IT Assurance Guide Using Cobit" esas alınarak ilgili kontrole ait Kontrol Amaçları, Değer Unsurları, Risk Unsurları ve Kontrol Uygulamaları gerçeklenmiştir ve örnek denetimler gerçeklenmiştir.

4.3. Uygulamanın Önemi

Uygulama Yönetim Beyanı konusunda henüz hiç bir akademik çalışmanın yapılmamış olması konusundan literatüre yönelik sonraki araştırmaların yapılmasında kaynak teşkil edebilecektir.

Yönetim Beyanı konusunda yayınlanmış olan tüm makaleler ve yayınlar incelenmiş en güncel kaynaklardan ve otoritelerden bilgiler alınmıştır. Düzenlenen bilgileri literatüre kazandırılmış olup. Bu alandaki bilgi eksikliğini gidermesi açısından hazırlanan çalışma önem arz etmektedir.

4.4. Uygulamanın Kapsamı ve Kısıtları

Yönetim Beyanı Bilgi sistemleri denetimi DS09 Konfigürasyon Yönetimi kapsamında uygulayacağı denetimler kapsam dahiline alınmıştır. İlgili denetim sadece 2011 yılı Aralık ayına kadar olan hayali olarak oluşturulmuş XBank'da yapılmış denetim çalışmalarının test sonuçlarını içermektedir.

Denetim metodolojisi Cobit 4.1 ve IT Assurance Guide Using Cobit adlı dökümanlardan faydalanarak oluşturulmuştur. Denetim Metodolojileri Deloitte Touche & Tohmatsu Türkiye Ofisi ve PricewaterhouseCoopers Türkiye Ofisinin ISACA İstanbul Chapter iş birliği ile yapmış oldukları bilgilendirme toplantıları esas alınarak oluşturulmuştur. Her hangi bir bankada uygulanması ihtimal makul bir metodoloji oluşturulmuş ve yukarıda belirtilen Bilgi Sistemleri Süreçlerinden her bankada yapılmakta olan Konfigürasyon Yönetimi çalışmalarının Yönetim Beyanı'na mesnet teşkil edecek çalışmalar sunulmuştur.

Mevzuat açısından Aralık 2011 dönemine kadar çıkmış olan en güncel kanuni ve mevzuat düzenlemeleri dikkate alınmıştır. BDDK tarafınfan yayınlanmış tüm Bilgi Sistemleri Denetimi hakkındaki yönetmeliklerin güncel halleri dikkate alınmıştır.

4.5. Kullanılan Araçlar

Cobit 4.1 kullanılarak Kontroller ortaya çıkarılmış, Cobit Denetim metodolojisini sunan "IT Assurance Guide Using Cobit" esas alınarak ilgili kontrole ait Kontrol Amaçları, Değer Unsurları, Risk Unsurları ve Kontrol Uygulamaları gerçeklenmiştir ve örnek denetimler gerçeklenmiştir.

4.6. Uygulamanın Yapılması ve Sonuçları

Uygulama öncesinde Konfigürasyon Yönetimi terminolojisi çalışmaları sunulmuştur. Konfigürasyon Yönetimi Sürecinde Referans Alınan Standartlar açıklamış Yönetim Beyanı Kapsamında benimsenen esas olan Cobit çerçevesinde örnek denetim çalışmaları yapılmış sonuç raporları oluşturulmuştur.

4.6.1. Konfigürasyon Yönetimi Nedir?

Konfigürasyon yönetimi (Configuration Managenent – CM) geliştirilen bir sistem ürününün yönetimi için standart ve prosedürlerin geliştirilmesi ve uygulanmasıdır. Konfigürasyon yönetimi prosedürleri, önerilen sistem değişikliklerinin nasıl kaydedildiğini ve gerçekleştirildiğini, bunların sistem parçalarıyla nasıl ilişkilendirildiğini ve sistemin değişik versiyonlarının tanımlanması için kullanılan metotları tanımlarlar. Konfigürasyon yönetimi araçları, sistem parçalarının versiyonlarının tutulması, sistemin bu parçalardan inşası ve müşterilere sistem versiyonlarının sürümlerinin bildirilmesi için kullanılırlar.[53]

Konfigürasyon Yönetimi Raporlaması Konfigürasyon öğeleri üzerinde Nelerin yapıldığına, kimin yaptığına, ne zaman yapıldığına ve nelerin etkilendiğine verdiğimiz yanıtların tamamı bir sürecin raporlama düzeyini tanımlar. Konfigürasyon durum raporlaması bu bilgi akışının yapılmasını bir belgeleme düzenine sokmasını sağlar. Bu yapmış olduğumuz değişiklik isteğinden bunların versiyonlanarak yapılmasına test edilmesine, onaylanmasına ortamlara taşınmasına kadar olan tüm süreçte belgelenmesine ve dolayısı ile raporlanmasına yardımcı olur.

Bu raporlardan elde edilecek sonuçların sisteme geri beslenmesi ile de sistemin kendini iyileştirmesi, yapılan faaliyetlerin hem mühendislik hem de maliyet açısından proje incelenmesine alınmasına neden olur. Raporlardan elde edilen değerlendirme sonuçları

[53] Konfigürasyon Yönetimi , http://www.bilgisite.com/yonetim/yonetim_06.html [27.11.2011]

ile sistem geri besleme mekanizması çalışır. Bu geri besleme yolu ise sonraki adımlarda yazılım yaşam döngüsü açısından bir iyileştirme, sistem güncel tutma veya ama daha uyumlu bir sistemsel denetmenin olmazsa olmaz koşuludur. [54]

Konfigürasyon yönetimi aşağıda sıralanan teknik ve yönetimsel direktiflerin uygulandığı ve gözlemlendiği bir disiplindir:[55]

- Konfigürasyon biriminin fonksiyonel ve fiziksel karakteristiklerinin tanımlanması ve dokümante edilmesi,

- Bu karakteristiklerdeki değişikliklerin kontrol edilmesi,

- Değişiklik sürecini ve uygulanan statüleri kaydetme ve raporlama

- Belirlenen gerekliliklerin sağlandığını ve tamamlandığını doğrulama

Konfigürasyon Yönetiminin amacı konfigürasyon tanımlamasını, kontrolünü, durum değişikliklerini ve auditlerini kullanarak ürünlerin entegrasyonunu sağlamak ve korumaktır.

Konfigürasyon Yönetimi süreci şunları içerir:

• Belirlenen zamanlarda, seçilen ürünlerin ana hatlarını oluşturacak konfigürasyonun tanımlanması

• Konfigürasyon birimlerindeki değişimleri kontrol edilmesi

• Konfigürasyon yönetimi altındaki ürünlerin oluşturulması için gerekli şartların oluşturulması ya da sağlanması

• Ana hatların bütünlüğünün sağlanması

• Tam durum (statü) ve halihazırda var olan konfigürasyon

bilgisinin geliştiricilere, kullanıcılara ve müşteriye sağlanması Konfigürasyon kontrolüne alınacak ürünler; müşteriye gönderilecek ürünler, belirlenmiş şirket içi ürünler, tedarik edilmiş ürünler, programcıklar ve ürünlerin meydana getirilmesini ve geliştirilmesini sağlayan şirket içi araçlardan oluşur.

---

[54] Hacısüleymanoğlu, age.s82
[55] Carnegie Mellon University, "Konfigurasyon Yönetimi İçin CMMI Süreçleri", http://ieee.metu.edu/iffet/blog/Konfigurasyon_Yonetimi_CMII-V1.2.pdf [28.11.2011]

4.6.2.Konfigürasyon Yönetimi Sürecinde Referans Alınan Standartlar

4.6.2.1. ITIL

ITIL Birleşmiş Krallık Ticaret Ofisi tarafından 1980‟li yılların sonlarına doğru geliştirilmiş olan standartlardır. Hazırlanma amacı, Birleşik Krallık hükümetinde BT hizmet yönetimini iyileştirmektir. ITIL, BT hizmetlerini en başarılı yöneten örnek uygulamaları esas alarak oluşturulan, süreçleri entegre olarak anlatan bir dizi yazılı rehberdir.

- Eğitim programı,
- Sertifikalandırması,
- Danışmanlık hizmetleri,
- Yazılım destek programları olan uluslararası bir standarda dönüşmüş durumdadır. [56]

ITIL, günümüzde iş odaklı, maliyet etkin IT organizasyonlarını yönetmede fiili standarttır. ITIL yapısı yakın zaman önce süreç odaklı yaklaşımından servis yaşam döngüsü yaklaşımına doğru tekrar tasarlanmıştır. İş stratejisi ile IT' nin uçtan uca entegrasyonunu içeren bu görüş, ITIL'ın son versiyonunun temelindeki beş ana başlıkta bulunmaktadır: [57]

- Servis Stratejisi, IT stratejisinin, genel iş amaç ve beklentilerine eşlendiğinden emin olur.
- Servis Tasarımı, yeni veya değişmiş bir takım iş ihtiyaçları ile başlarken, dokümante edilmiş iş ihtiyaçları için bir çözüm geliştirilmesi ile sona erer.
- Servis Dönüşümü, değişim, risk ve kalite güvenceyle alakadar olup servis dizaynını hayata geçirir ve böylece servis operasyonunun, servis ve altyapıyı kontrollü bir tarzda yönetilebilinmesini sağlar.
- Servis Operasyonu: İş ile olağan aktiviteler kapsamında ilgilidir.
- Devamlı Servis İyileştirilmesi: Bütün diğer elementlerin genel bir görünümüne sahiptir, tüm sürecin ve servis provizyonunun iyileştirilmesi için yollar arar.

[56] E.Hacısüleymanağlu, age.11,12
[57] Bülent Naci Alpay, "ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması ",(Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, 2008)

ITIL da Konfigürasyon Yönetimi; Bir sistem, kaydedilen ve raporlanan konfigürasyon elementlerinin durumu, değişim talepleri ve içindeki konfigürasyon elementlerinin tanımlanması ve konfigürasyon elementlerinin doğruluk ve bütünlüğünün, tanımlanması ve kimliklendirilimesi prosesleridir.[58]

ITIL'da Konfigürasyon Yönetimi süreci BT Hizmet Süreçleri Hizmet Destek süreçleri arasında "BT teknik altyapısını kontrol etmek, sadece onaylanmış yazılım ve donanımların kullanımını sağlamak" [59] olarak açıklanmaktadır.

ITIL'da konfigürasyon yönetiminin amacı BT altyapısında takip edilmesi gereken her öğe için ilgili öğeye ait benzersiz ve tekil bilgileri, öğelerin birbirleri ile olan bağlantılarını ilişkilerini takip eden bir yöntem hazırlamaktır. Bu yöntem sayesinde:[60]

- Bütün BT varlıklarının gerektiğinde hesabı verilebilinir
- Diğer Hizmet Yönetimi süreçlerini destekleyecek doğru bilgiler elde edilir
- Olay, Sorun, Değişim ve Sürüm Yönetimi'ne sağlam bir temel oluşturulur
- İçerdiği verileri belirli zaman aralıkları ile denetleyerek zaman içinde oluşabilecek değişikliklerden etkilenmeyecek güncel bilgiler tutulur.

Planlama; Tüm konfigürasyon öğelerinin seçimi, tanımlanması ve adlandırılmasıdır. Sahip olma, ilişkiler, versiyonlar ve tanımlayıcılar da dahil olmak üzere CI'lar ile ilgili bilgilerin kaydedilmesi faaliyetini içerir.

Tanımlama; Konfigürasyon Öğelerinin (CI-Configuration Item) seçilmesi, tanımlaması, CI'lar arasındaki ilişkinin kurulması.

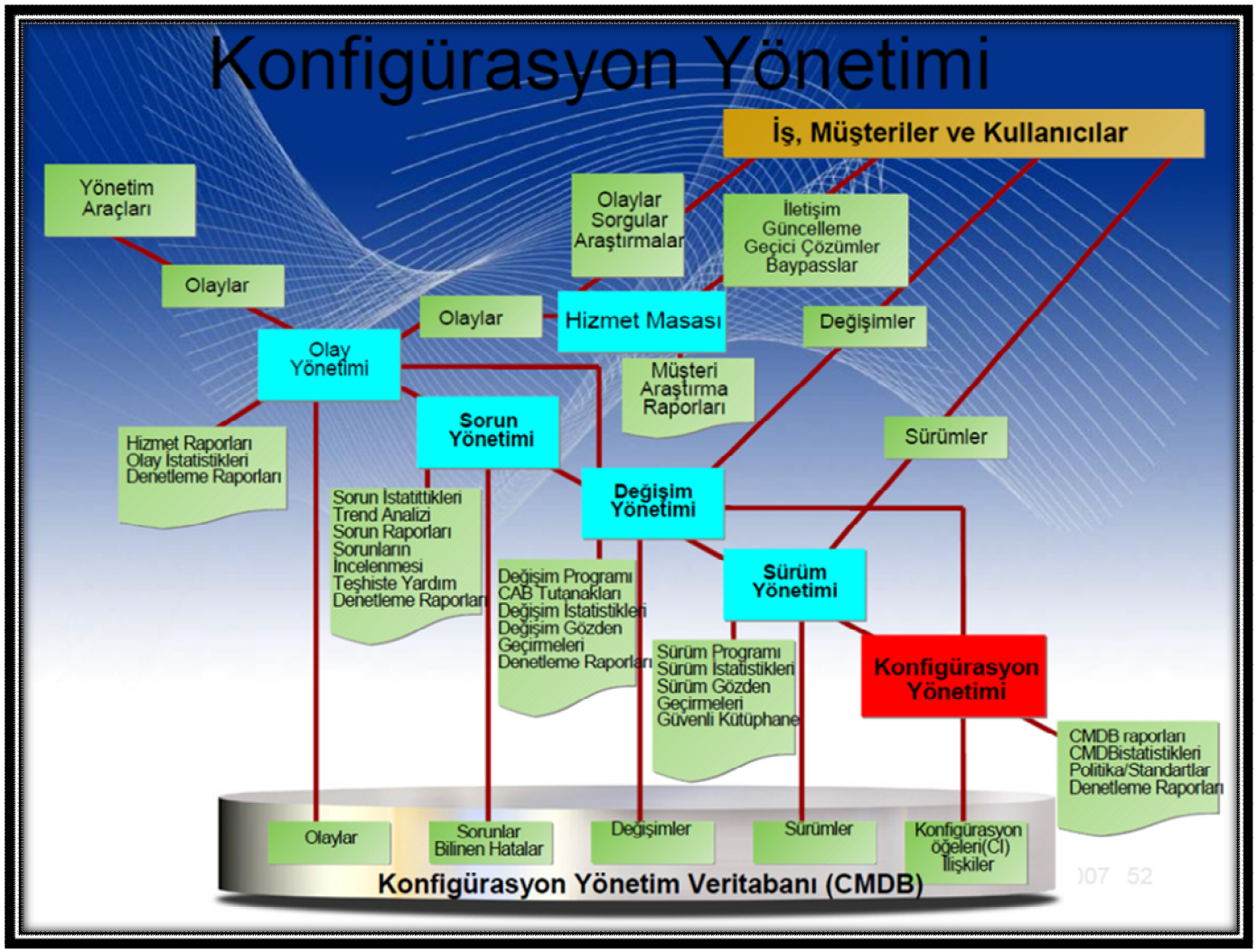
Kontrol; Satın almadan elden çıkartmaya kadar her aşamada yalnızca yetkili ve tanımlanabilir CI'ların kabul edilmesi ve kaydedilmesinin garanti altına alınması.

Konum Belirleme; Her CI'ın yaşam döngüsü boyunca ilişkili olduğu tüm mevcut ve geçmiş verilerin rapor edilmesi (Satın alma, test, kullanım, onarım..).

Doğrulama ve Denetleme; CI'ların fiziksel varlığını ve CMDB'ye doğru biçimde kaydedildiklerini bir dizi inceleme ve denetlemedir.

---

[58] Cem Topkaya, "ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması ", (Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, 2008)
[59] E. Hacısüleymanağlu, age.13.
[60] Özhan Karaman, "ITIL Temelli BT Hizmet Yönetimi", 6. Linux ve Özgür Yazılım Şenliği 6 Mayıs 2007, http://seminer.linux.org.tr/wp-content/uploads/itil_temelli_bt_hizmet_yonetimi.pdf [27.11.2011]



Şekil 14: ITIL Hizmet Yönetimi modülleri arasında Konfigürasyon Yönetimi Adımının yeri ve diğer modüller ile olan ilişkisi.

Kaynak: ITIL Temelli BT Hizmet Yönetimi, Sunumu Özhan Karaman, 6. Linux ve Özgür Yazılım Şenliği 6 Mayıs 2007

4.6.3.Konfigürasyon Veri Tabanı

Konfigürasyon veri tabanı, konfigürasyonlarla ilgili tüm ilgili verileri kaydetmek için kullanılır. Temel fonksiyonları, sistem değişikliklerinin etkilerini azaltmak ve Konfigürasyon Yönetimi süreci hakkında yönetim bilgisi sağlamaktır. Konfigürasyon veri tabanının şemasını tanımlamak kadar, proje bilgilerinin kaydedilmesi ve bulunması için prosedürler de Konfigürasyon Yönetimi planlama sürecinin parçası olarak tanımlanmalıdır.

Bir konfigürasyon veri tabanı, sistem konfigürasyonları hakkında bir dizi sorguya cevaplar sağlamak zorundadır. Tipik sorgular:

1. Sistemin belli bir versiyonunu hangi müşteriler almıştır?
2. Verilen bir sistem versiyonunun çalıştırılması için hangi donanım ve işletim sistemi konfigürasyonu gerekmektedir?
3. Bir sistemin kaç versiyonu oluşturulmuştur ve oluşturulma tarihleri nedir?
4. Belli bir parça değiştirilirse, sistemin hangi versiyonları etkilenir?
5. Belli bir versiyon için kaç değişiklik isteği beklemektedir?
6. Belli bir versiyon için kaç hata bildirilmiştir?

İdeal olarak, konfigürasyon veri tabanı, resmi proje belgelerinin saklanıp yönetildiği versiyon yönetim sistemi ile tümleştirilmelidir. Bazı CASE araçlarıyla desteklenen bu yaklaşım, değişiklik ile etkilenen belge ve parçaların doğrudan bağlanmasına olanak tanır. Tasarım belgeleri gibi belgeler arasındaki bağlantılar, ve program kodu, bir değişiklik gerektiğinde, değişmesi gereken her şeyin göreceli olarak daha kolay bulunmasını sağlar. [61]

Bazı Örnek Konfigürasyon Veri Tabanı uygulamaları

- Microsoft TFS (Team Foundation Server)
- IBM Rational ClearQuest
- SourceSafe (Microsoft)
- SubVersion (Açık Kaynak Kodlu)
- CVS (Açık Kaynak Kodlu)

[61] Konfigürasyon Yönetimi , http://www.bilgisite.com/yonetim/yonetim_06.html [27.11.2011]

Konfigürasyon Yöneticisinin amacı projedeki kod geliştirme, test etme, değişikleri yerine getirme, envanteri yönetme çalışmalarına ait prosedür ve politikaların uygulanmasını temin etmektedir. Kod üzerinde yapılan değişiklerin yapılması için uygulama tekniklerini geliştirir.

Değişiklik Denetim Kurulu'nda değerlendirilerek gelen formal değişiklik isteklerini kontrollü olarak yetkili olarak uygulayan mekanizmayı kurar, uygular. Proje planını tüm çalıma grubunu kapsayacak şekilde iş, görevler ve sorumluluklar bazında hazırlar, yayımlar.[62]

Yazılım Dünyasında Sık Kullanılan Konfigürasyon Yönetimi Süreçleri;

- Versiyon Kontrolü
- Versiyon Yönetimi
- Kaynak Kod Kontrolü
- Kaynak Kod Yönetimi
- SCM (Software Configuration Management)
- Source Control
- Source Control Management

Şeklindedir.

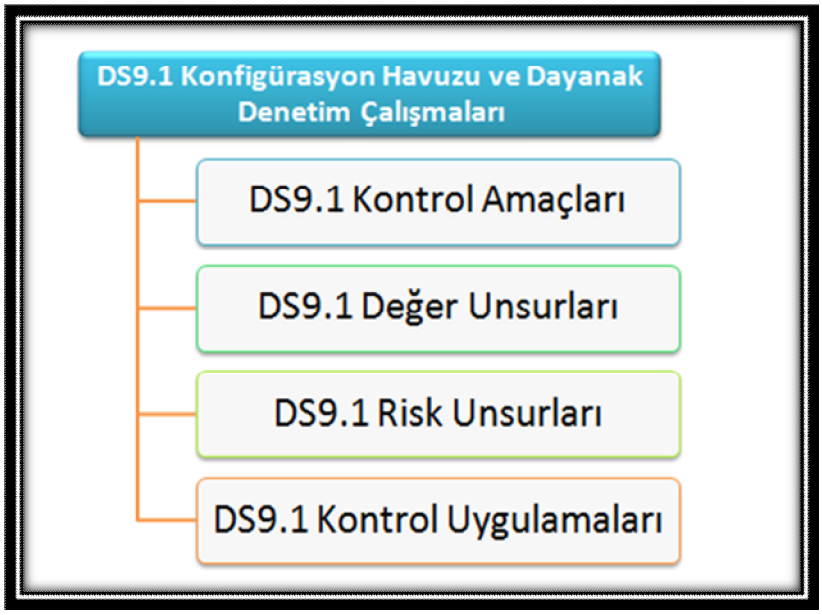
[62] R.Reha Çetin, "Yazılım Mühendisliğinde Uygulama Geliştirmede bir Çözüm: Yazılım Konfigürasyon Yönetimi",(Doktora Tezi,T.C. Trakya Üniversitesi Fen Bilimleri Enstitüsü, 2007)

4.6.4. Cobit DS09 Konfigürasyon Yönetimi

Cobit Konfigürasyon Yönetimini sadece Yazılım Konfigürasyon Yönetimi olarak ele almaz Donanım, Network ve tüm diğer Bilgi Sistemleri süreçlerini inceleyecek şekilde ele alır. Sırasıyla Cobit DS09 Konfigürasyon Yönetimi süreçleri ve Yönetim Beyanı kapsamında denetim çalışmaları çalışılmıştır.

4.6.4.1. DS9.1 Konfigürasyon Havuzu ve Dayanak

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



Şekil 15: Cobit 4.1 Konfigürasyon Yönetimi başlığı altında incelenmesi gereken öğeler

Kaynak: ISACA IT Assurance Guide Using Cobit

4.6.4.2. Yönetim Beyanı Kapsamında Konfigürasyon Yönetimi Denetim Çalışmaları

- **DS9.1.1 Konfigürasyon Havuzu ve Dayanak Kontrol Amaçları**

Konfigürasyon öğelerine ilişkin tüm bilgilerin bulunduğu merkezi bir depo ve bir destek aracı kurulmalıdır. Tüm varlıklar ve varlıklarda gerçekleşen değişiklikler izlenmeli ve kayıt altına alınmalıdır. Her bir sistem ve servis için temel seviyeler belirlenmiş olmalı ve güncelliği sağlanmalı ve bu temel seviyeler gerçekleşecek değişikliklerden sonra bir kontrol noktası olarak kullanılabilmesi amaçlanmaktadır.

- **DS9.1.2 Konfigürasyon Havuzu ve Dayanak Değer Unsurları**

• Donanım ve yazılım seviyelerinde etkin planlama gerçekleştirilebilecek ve iş süreçleri ve servisleri desteklenecektir.

• Tüm kurumda uygulanan konfigürasyonların tutarlılığı sağlanacaktır.

• Değişiklikler genel mimariye uyumlu olarak gerçekleştirilecektir.

• Tedarikçilerin daha iyi belirlenebilmesi sayesinde maliyet düşüşü gerçekleştirilebilecektir.

• Olay çözümleme süreleri kısalabilecektir.

- **DS9.1.3 Konfigürasyon Havuzu ve Dayanak Risk Unsurları**

• Değişiklikler genel teknoloji mimarisini uyumsuz olabilecektir.

• Varlıklar gerektiği gibi korunamayabilecektir.

• Donanım ve yazılım seviyesinde yetkisiz olarak gerçekleştirilen değişiklikler gözden kaçırılabilecektir ve bu nedenle güvenlik açıkları oluşabilecektir.

• Dokümante edilmiş bilgiler mimarinin güncel halini göstermeyecektir.

• Geri dönüşler yapılamayabilecektir.

4.6.4.3. DS9.1 Konfigürasyon Havuzu ve Dayanak Kontrol Uygulamaları

Konfigürasyon Yönetimi Kapsamında Konfigürasyon Havuzu ve Dayanak Kontrol Uygulamaları örnek çalışmaları sırasıyla yapılmıştır. Denetim sonuç raporları tüm Kontrol uygulamaları için oluşturulmuştur.

DS09.01.Konfigürasyon Havuzu ve Dayanak Denetim Çalışmaları Kontrol Uygulamaları		
Denetim Amacı	**Test Çalışması**	**Çalışma Kağıdı Referans No**
1. Konfigürasyon yönetim öğelerini kayıt altına alınacağı bir konfigürasyon deposu oluşturulmalıdır. Sistemlere, servislere, versiyon numaralarına ve lisanslama ayrıntılarına erişebilmek, bunları kullanmak ve işletmek için gerekli olan donanım, uygulama yazılımı, ara katman ekipmanı, parametreler, dokümantasyon, prosedürler depo içeriğinde bulunmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
2. Depodaki konfigürasyon yönetimi bilgilerinin denetim izlerini etkin bir biçimde kayıt altına alacak bir araç kullanılmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
3. Her bir konfigürasyon öğesine tekil bir belirleyici tanımlanmalı ve bu belirleyici kullanılarak öğenin fiziksel varlıklar ve finansal kayıtlar ile ilişkileri izlenebilmelidir.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
4. Geçmişteki, bugünkü ve planlanmış olarak gelecekteki her zaman noktasındaki konfigürasyonun bilgisinin tutulabilmesi için geliştirme ortamı, test ortamı ve gerçek ortamdaki konfigürasyon temel seviyelerinin tanımlanması ve dokümante edilmesi gerekmektedir.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
5. Problem olması durumunda eski konfigürasyon temel seviyesine dönebilmek için bir süreç oluşturulmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
6. Tanımlanmış depo ve temel seviyeler ile değişiklikleri izleyecek ve karşılaştıracak mekanizmalar kurulmalıdır. İstisnalar, mutabakatlar ve karar verme için yönetim raporlaması yapılmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	

Denetlenen Alt Süreçlerde Bulgu Olması Durumu

Süreç Kodu	**2011.DS09.01**	**Süreç**	**Konfigürasyon Yönetimi**
Bulgu Kodu	2011.S.DS09.01.KZ*		
Bulgu Özeti	Konfigürasyon Yönetimi Uygulamasında kritik öğelerin bulunmaması		
Alt Süreç Kodu	Konfigürasyon Havuzu ve Dayanak Denetim Çalışmaları		
Alt Süreç Adı	DS09.01		
Süreç Sahibi	Operasyon Müdürlüğü		
Süreç Kalite Kontrol Ekibi	Kalite Müdürlüğü		
İş Akış Adımı	Konfigürasyon Yönetimi Uygulamasına tüm öğeler girilir.		
Risk Kodu	2		
Bulgu Derecesi	Yüksek		
İş Riski	Tüm varlıklar ve varlıklarda gerçekleşen değişikliklerin izlenmemesi gereksiz kaynak kullanımı veya atıl kaynak sahipliğine yol açabilir. Operasyonel riske sebebiyet verir		
Denetçinin Görüşü	**Yapılan incelemede Konfigürasyon Yönetimi ile ilgili yazılım bulunmakta olduğu görülmüştür. Ancak Kritik konfigürasyon öğeleri sınıflandırılamamaktadır. Programın detaylandırılması ve Öğelerin güncellenmesi gerekmektedir.		
Denetlenenin Görüşü	**Konuyla ilgili olarak Bilgi Teknolojileri grubuna talep iletilmiştir. Kaynak yetersizliği dolayısıyla yönetim programındaki eksik modüllerin geliştirilmesi tamamlanmamıştır.		
Sonuç Değerlendirmesi	Bulgu devam etmektedir.		

*** BDDK.BYD.138/1 sayılı 29 Aralık 2008 tarihli Bilgi Sistemleri Denetimlerinde Tespit Edilen Bulguların Kodlanması Hakkında Genelge'ye göre kodlanır.**

**** Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

Tablo 6: DS09 Konfigürasyon Yönetimi Bilgi Sistemleri Denetimi Konfigürasyon Havuzu ve Dayanak Denetim Çalışmaları Kontrol Durumu Belirleme Çalışması

	DS09 Konfigürasyon Yönetimi Bilgi Sistemleri Denetimi									
Risk Kodu	**Anahtar Kontrol**	**Kontrol Referansı**		**Kontrol**	**Etki**	**Kontrolü Yapan**	**Kontrol Sahibi Birim/**	**Kontrol Sıklığı**	**Kontrol Türü**	**Bankadaki Uygulama**
		Alt Süreç Kodu: Konfigürasyon Havuzu ve Dayanak Kontrolleri								
1	**Evet**	**DS09**	**DS9.1**	**Üst yönetimin konfigürasyon yönetimine ilişkin kapsam tanımlaması yaptığı ve konfigürasyon yönetiminin performansını ölçtüğü sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü <Bu kısımda ilgili bankaya ait kontrol/Süreç sahibi birim belirtilir>**	**Yıllık<Bu kısımda bankada hangi sıklıkla kontrol yapıldığı bilgisi verilir>**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
2	**Evet**	**DS09**	**DS9.1**	**Depodaki konfigürasyon yönetimine ilişkin bilgilerin denetim izlerinin etkin bir biçimde kayıt altına alınmasını sağlayacak bir aracın kullanıldığı sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Gerektiğinde**	**Sistemsel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
3	**Evet**	**DS09**	**DS9.1**	**Bu araca yalnız yetkili kullanıcıların erişebilmesinin sağlandığı belirlenmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
4	**Evet**	**DS09**	**DS9.1**	**Örnek olarak seçilen konfigürasyon öğeleri incelenmeli ve her biri için tekil bir belirleyici tanımlanmış olduğu kontrol edilmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

5	**Evet**	**DS09**	**DS9.1**	**Bileşenler için konfigürasyon temel seviyelerinin tanımlanmış ve dokümante edilmiş olduğu sorgulanmalı ve doğrulanmalıdır**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
6	**Evet**	**DS09**	**DS9.1**	**Konfigürasyon temel seviyelerinin farklı zamanlardaki sistem konfigürasyonlarının bilgisini sağladığı kontrol edilmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
7	**Evet**	**DS09**	**DS9.1**	**Temel seviye konfigürasyonlarına geri dönüşü tanımlayan ve dokümante edilmiş bir sürecin olduğu sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Gerektiğinde**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
8	**Evet**	**DS09**	**DS9.1**	**Örnek olarak seçilecek sistem ve uygulamalar incelenerek temel seviye konfigürasyonlarına geri dönebildikleri test edilmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
9	**Evet**	**DS09**	**DS9.1**	**Tanımlanmış depo ve temel seviyeleri ve değişiklikleri izleyecek ve karşılaştıracak mekanizmaların bulunduğu sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Gerektiğinde**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
10	**Evet**	**DS09**	**DS9.1**	**Yönetime düzenli olarak raporlama yapıldığı ve bu raporların sürekli gelişime katkıda bulunduğu doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

DS09 KONFİGÜRASYON YÖNETİMİ SÜREÇ DENETİMİ SONUÇ RAPORU-2011.DS09.01.01			
SÜREÇ KODU	XBANK.2011.DS09		
ALT SÜREÇ KODU	XBANK.2011.DS09.01-01.01		
ALT SÜREÇ ADI	Konfigürasyon Havuzu ve Dayanak Denetimi		
SÜREÇ SAHİBİ	Operasyon Müdürlüğü		
SÜREÇ KALİTE KONTOL EKİBİ	Kalite Müdürlüğü		
İŞ AKIŞ ADIMI	Merkezi bir Konfigürasyon Yönetimi veritabanının oluşturulması		
DENETİM AMACI/ KAPSAMI	*Depodaki konfigürasyon yönetimi bilgilerinin denetim izlerini etkin bir biçimde kayıt altına alacak bir araç kullanılmalıdır.		
ÖNCEKİ DENETİM KODU/ TARİHİ	2009.DS09.01.01 – Önceki Denetim Tarihi		
BAŞLANGIÇ TARİHİ	Denetim Başlangıç Tarihi Girilir	**BİTİŞ TARİHİ (PLANLANAN)**	Denetim Bitiş Tarihi Girilir
BİTİŞ TARİHİ (GERÇEKLEŞEN)	Denetim Bitiş Tarihi Girilir		
SÜREÇ DENETİM SONUCU			
**Konfigürasyon yönetim öğelerini kayıt altına alınacağı bir konfigürasyon deposu oluşturulduğu görülmüştür. Bankaya münhasır konfigürasyon yönetimi programı, sistem üzerinde gerçekleştirilen bilgilerinin denetim izlerini tutmaktadır.			
HAZIRLAYAN:	Hazırlayan Bilgi Sistemleri Müfettişi	**ONAYLAYAN:**	Onaylayan Bilgi Sistemleri Baş Müfettişi

***ITAssurance Guide Using Cobit® baz alınarak oluşturulmuştur.**

****Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

DS09 KONFİGÜRASYON YÖNETİMİ SÜREÇ DENETİMİ SONUÇ RAPORU-2011.DS09.01.02			
SÜREÇ KODU	XBANK.2011.DS09		
ALT SÜREÇ KODU	XBANK.2011.DS09.01-01.02		
ALT SÜREÇ ADI	Konfigürasyon Havuzu ve Dayanak Denetimi		
SÜREÇ SAHİBİ	Operasyon Müdürlüğü		
SÜREÇ KALİTE KONTOL EKİBİ	Kalite Müdürlüğü		
İŞ AKIŞ ADIMI	Merkezi bir Konfigürasyon Yönetimi veritabanının oluşturulması		
DENETİM AMACI/ KAPSAMI	*Konfigürasyon yönetim öğelerini kayıt altına alınacağı bir konfigürasyon deposu oluşturulmalıdır. Sistemlere, servislere, versiyon numaralarına ve lisanslama ayrıntılarına erişebilmek, bunları kullanmak ve işletmek için gerekli olan donanım, uygulama yazılımı, ara katman ekipmanı, parametreler, dokümantasyon, prosedürler depo içeriğinde bulunmalıdır.		
ÖNCEKİ DENETİM KODU/ TARİHİ	XBANK.2009.DS09.01.02 – Önceki Denetim Tarihi		
BAŞLANGIÇ TARİHİ	Denetim Başlangıç Tarihi Girilir	**BİTİŞ TARİHİ (PLANLANAN)**	Denetim Bitiş Tarihi Girilir
BİTİŞ TARİHİ (GERÇEKLEŞEN)	Denetim Bitiş Tarihi Girilir		
SÜREÇ DENETİM SONUCU			
**Konfigürasyon yönetim öğelerini kayıt altına alınacağı bir konfigürasyon deposu oluşturulduğu görülmüştür. Konfigürasyon öğeleri donanım, uygulama yazılımı, ara katman ekipmanı, parametreler, dokümantasyon, prosedürler kategorilenmiş olup konfigürasyon deposunun düzenli işleyişini sağlayabilmek adına altı aylık periyodlar ile kontrol edilmekte olduğu görülmüştür. Lisanslama ayrıntılarına ilişkin yazılım konfigürasyon yönetimi çalışmaları konusunda güncelleme yavaşlıkları bulunmakla birlikte, İlgili kontrolün Uygulama Geliştirme Departmanı Uygulama Geliştirme Uzmanları tarafından yapılmakta olduğu görülmüştür.			
HAZIRLAYAN:	Hazırlayan Bilgi Sistemleri Müfettişi	**ONAYLAYAN:**	Onaylayan Bilgi Sistemleri Baş Müfettişi

***ITAssurance Guide Using Cobit® baz alınarak oluşturulmuştur.**

****Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

DS09 KONFİGÜRASYON YÖNETİMİ SÜREÇ DENETİMİ SONUÇ RAPORU-2011.DS09.01.03			
SÜREÇ KODU	XBANK.2011.DS09		
ALT SÜREÇ KODU	XBANK.2011.DS09.01-01.03		
ALT SÜREÇ ADI	Konfigürasyon Havuzu ve Dayanak Denetimi		
SÜREÇ SAHİBİ	Operasyon Müdürlüğü		
SÜREÇ KALİTE KONTOL EKİBİ	Kalite Müdürlüğü		
İŞ AKIŞ ADIMI	Merkezi bir Konfigürasyon Yönetimi veritabanının oluşturulması		
DENETİM AMACI/ KAPSAMI	* Her bir konfigürasyon öğesine tekil bir belirleyici tanımlanmalı ve bu belirleyici kullanılarak öğenin fiziksel varlıklar ve finansal kayıtlar ile ilişkileri izlenebilmelidir.		
ÖNCEKİ DENETİM KODU/ TARİHİ	2009.DS09.01.03 – Önceki Denetim Tarihi		
BAŞLANGIÇ TARİHİ	Denetim Başlangıç Tarihi Girilir	**BİTİŞ TARİHİ (PLANLANAN)**	Denetim Bitiş Tarihi Girilir
BİTİŞ TARİHİ (GERÇEKLEŞEN)	Denetim Bitiş Tarihi Girilir		
SÜREÇ DENETİM SONUCU			
**Konfigürasyon yönetim öğelerini kayıt altına alınacağı bir konfigürasyon deposu oluşturulduğu görülmüştür. Oluşturulan konfigürasyon Deposunda Konfigürasyon Öğelerine ait tekil ayırt edici numaralar verilmiş olup versiyon numaralama işlemi yapılmaktadır. Her bir konfigürasyon öğesine tekil bir belirleyici tanımlanmış olduğu ve bu belirleyici kullanılarak öğenin fiziksel varlıklar ve finansal kayıtlar ile ilişkilerinin izlenebildiği görülmüştür.			
HAZIRLAYAN:	Hazırlayan Bilgi Sistemleri Müfettişi	**ONAYLAYAN:**	Onaylayan Bilgi Sistemleri Baş Müfettişi

***ITAssurance Guide Using Cobit® baz alınarak oluşturulmuştur.**

****Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

DS09 KONFİGÜRASYON YÖNETİMİ SÜREÇ DENETİMİ SONUÇ RAPORU-2011.DS09.01.04			
SÜREÇ KODU	XBANK.2011.DS09		
ALT SÜREÇ KODU	XBANK.2011.DS09.01-01.04		
ALT SÜREÇ ADI	Konfigürasyon Havuzu ve Dayanak Denetimi		
SÜREÇ SAHİBİ	Operasyon Müdürlüğü		
SÜREÇ KALİTE KONTOL EKİBİ	Kalite Müdürlüğü		
İŞ AKIŞ ADIMI	Merkezi bir Konfigürasyon Yönetimi veritabanının oluşturulması		
DENETİM AMACI/ KAPSAMI	*Geçmişteki, bugünkü ve planlanmış olarak gelecekteki her zaman noktasındaki konfigürasyonun bilgisinin tutulabilmesi için geliştirme ortamı, test ortamı ve gerçek ortamdaki konfigurasyon temel seviyelerinin tanımlanması ve dokümante edilmesi gerekmektedir.		
ÖNCEKİ DENETİM KODU/ TARİHİ	2009.DS09.01.04 – Önceki Denetim Tarihi		
BAŞLANGIÇ TARİHİ	Denetim Başlangıç Tarihi Girilir	**BİTİŞ TARİHİ (PLANLANAN)**	Denetim Bitiş Tarihi Girilir
BİTİŞ TARİHİ (GERÇEKLEŞEN)	Denetim Bitiş Tarihi Girilir		
SÜREÇ DENETİM SONUCU			
**Banka bünyesinde kullanılmakta olan Konfigürasyon Yönetimi Aracı tüm konfigürasyon öğelerini Geliştirme (production) test ve üretim (gerçek ortam) için farklı seviyelerde kayıtları tutabilmekte ve Konfigürasyon temel seviyelerini detaylı tanımlayabilip yöneticiler için rapor sunabilmektedir. Geçmişteki, bugünkü ve planlanmış Konfigürasyon bilgilerine raporlar aracılığı ile istendiği taktirde erişilebilmekte olduğu görülmüştür.			
HAZIRLAYAN:	Hazırlayan Bilgi Sistemleri Müfettişi	**ONAYLAYAN:**	Onaylayan Bilgi Sistemleri Baş Müfettişi

***ITAssurance Guide Using Cobit® baz alınarak oluşturulmuştur.**

****Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

DS09 KONFİGÜRASYON YÖNETİMİ SÜREÇ DENETİMİ SONUÇ RAPORU-2011.DS09.01.05			
SÜREÇ KODU	XBANK.2011.DS09		
ALT SÜREÇ KODU	XBANK.2011.DS09.01-01.05		
ALT SÜREÇ ADI	Konfigürasyon Havuzu ve Dayanak Denetimi		
SÜREÇ SAHİBİ	Operasyon Müdürlüğü		
SÜREÇ KALİTE KONTOL EKİBİ	Kalite Müdürlüğü		
İŞ AKIŞ ADIMI	Merkezi bir Konfigürasyon Yönetimi veritabanının oluşturulması		
DENETİM AMACI/ KAPSAMI	*Problem olması durumunda eski konfigürasyon temel seviyesine dönebilmek için bir süreç oluşturulmalıdır.		
ÖNCEKİ DENETİM KODU/ TARİHİ	2009.DS09.01.05 – Önceki Denetim Tarihi		
BAŞLANGIÇ TARİHİ	Denetim Başlangıç Tarihi Girilir	**BİTİŞ TARİHİ (PLANLANAN)**	Denetim Bitiş Tarihi Girilir
BİTİŞ TARİHİ (GERÇEKLEŞEN)	Denetim Bitiş Tarihi Girilir		
SÜREÇ DENETİM SONUCU			
**Banka bünyesinde kullanılmakta olan Konfigürasyon Yönetimi Aracı ile Geçmişteki, bugünkü ve planlanmış Konfigürasyon bilgilerine erişilebildiği için Problem olması durumunda eski konfigürasyon temel seviyesine dönebilmek için yeterli bilgiye sahip olunduğu görülmüştür.			
HAZIRLAYAN:	Hazırlayan Bilgi Sistemleri Müfettişi	**ONAYLAYAN:**	Onaylayan Bilgi Sistemleri Baş Müfettişi

***ITAssurance Guide Using Cobit® baz alınarak oluşturulmuştur.**

****Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

DS09 KONFİGÜRASYON YÖNETİMİ SÜREÇ DENETİMİ SONUÇ RAPORU-2011.DS09.01.06			
SÜREÇ KODU	XBANK.2011.DS09		
ALT SÜREÇ KODU	XBANK.2011.DS09.01-01.06		
ALT SÜREÇ ADI	Konfigürasyon Havuzu ve Dayanak Denetimi		
SÜREÇ SAHİBİ	Operasyon Müdürlüğü		
SÜREÇ KALİTE KONTOL EKİBİ	Kalite Müdürlüğü		
İŞ AKIŞ ADIMI	Merkezi bir Konfigürasyon Yönetimi veritabanının oluşturulması		
DENETİM AMACI/ KAPSAMI	* Tanımlanmış depo ve temel seviyeler ile değişiklikleri izleyecek ve karşılaştıracak mekanizmalar kurulmalıdır. İstisnalar, mutabakatlar ve karar verme için yönetim raporlaması yapılmalıdır.		
ÖNCEKİ DENETİM KODU/ TARİHİ	2009.DS09.01.04 – Önceki Denetim Tarihi		
BAŞLANGIÇ TARİHİ	Denetim Başlangıç Tarihi Girilir	**BİTİŞ TARİHİ (PLANLANAN)**	Denetim Bitiş Tarihi Girilir
BİTİŞ TARİHİ (GERÇEKLEŞEN)	Denetim Bitiş Tarihi Girilir		
SÜREÇ DENETİM SONUCU			
**Konfigürasyon Yönetimi Aracı ile Geçmişteki, bugünkü ve planlanmış Konfigürasyon bilgilerine erişilebildiği için gerekli mekanizmanın kurulu olduğu sonucuna ulaşılmıştır. Detaylı raporlamanın üst yönetime sunumu için program vasıtasıyla alınabilmesi düzenli raporların sistem üzerinde saklanması ve yıllık konfigürasyon denetimlerine kaynak teşkil etmektedir.			
HAZIRLAYAN:	Hazırlayan Bilgi Sistemleri Müfettişi	**ONAYLAYAN:**	Onaylayan Bilgi Sistemleri Baş Müfettişi

***ITAssurance Guide Using Cobit® baz alınarak oluşturulmuştur.**

****Örnek olarak hazırlanmıştır. Hiç bir banka ile ilişkisi yoktur.**

4.6.4.3. DS9.2 Konfigürasyon Birimleri Tanımlanması ve Korunması

Aşağıdakiler için prosedürler uygulanmalıdır:

- Konfigürasyon birimleri ve özellikleri tanımlanmalıdır
- Yeni, modifiye edilmiş ve silinmiş konfigürasyon maddeleri kaydedilmelidir.
- Konfigürasyon havuzunda konfigürasyon birimleri arasında ilişkiler tanımlanmalıdır ve korunmalıdır
- Konfigürasyon havuzundaki mevcut konfigürasyon maddeleri güncellenmelidir
- Yetkisiz yazılım kullanılması önlenmelidir

Bu prosedürler konfigürasyon havuzundaki tüm eylemlerin uygun yetkilendirilmesini ve kayıtlarını sağlamalıdır ve değişiklik yönetimi ve sorun yönetimi prosedürleri ile uygun şekilde entegre edilmelidir.

Yönetim Beyanı Kapsamında Konfigürasyon Yönetimi Denetim Çalışmaları

DS9.2.1 Konfigürasyon Birimleri Tanımlanması ve Korunması Kontrol Amaçları

Konfigürasyon Öğelerinin Tanımlanması ve Bakımı - Konfigürasyon deposundaki her değişimin denetim izlerinin tutulmasının desteklenmesi ve yönetilmesini sağlayacak konfigürasyon süreçleri kurulması.

DS9.2.2 Konfigürasyon Birimleri Tanımlanması ve Korunması Değer Unsurları

• Etkin değişim ve olay yönetimi

• Muhasebe gereksinimlerine uyum

DS9.2.3 Konfigürasyon Birimleri Tanımlanması ve Korunması Risk Unsurları

• Kritik iş bileşenlerinin belirlenememesi

• Değişim yönetiminin kontrol edilememesi ve iş kesintilerinin yaşanması

• Yanlış bilgi nedeniyle bir değişimin etkisinin değerlendirilememesi

• Varlık kayıtlarının doğru tutulamaması

DS9.2.4 Konfigürasyon Birimleri Tanımlanması ve Korunması Kontrol Uygulamaları

Konfigürasyon Yönetimi Kapsamında Konfigürasyon Birimleri Tanımlanması ve Korunması Kontrol Uygulamaları örnek çalışmaları sırasıyla yapılmıştır. Denetim raporları tüm Kontrol uygulamaları için oluşturulmuştur.

DS09.02 Konfigürasyon Birimleri Tanımlanması ve Korunması Denetim Çalışmaları Kontrol Uygulamaları		
Denetim Amacı	**Test Çalışması**	**Çalışma K.Ref. No**
1. Her bir konfigürasyon öğesinin özelliklerinin ve versiyon bilgilerinin belirlenmesi ve bilgilerinin güncelliğinin sağlanmasını gerektiren bir politika tanılanmalı ve uygulanmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
2. Fiziksel varlıklar politikaya göre etiketlenmelidir. Barkod veya benzeri bir otomatik sistem kullanılabilir.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
3. Olay, değişim ve problem yönetimi prosedürlerini konfigürasyon deposunun güncelliğinin sağlanması işleri ile entegre olarak işlemesini sağlayacak bir politika tanımlanmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
4. Yeni, modifiye edilmiş ve silinmiş konfigürasyon öğelerinin ve özellikleri ile versiyonlarının kaydedilmesini tanımlayan bir süreç oluşturulmalıdır. Konfigürasyon öğeleri ile konfigürasyon deposu arasındaki ilişkiler tanımlanmalı ve güncel tutulmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
5. Konfigürasyon öğelerinde yapılan her bir değişikliğin denetim izlerini tutacak bir süreç kurulmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
6. İş süreçlerinin sürdürülebilmesi için kritik olan konfigürasyon öğelerinin belirlenmesini sağlayacak bir süreç tanımlanmalıdır. (Bileşen arıza etki analizi)	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
7. Tüm varlıklar konfigürasyon yönetimi veri deposunda kayıt altına alınmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
8. Yazılım lisanslarının geçerliliğini doğrulayacak bir süreç tanımlanmalı ve uygulanmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	

Tablo 7: DS09 Konfigürasyon Yönetimi Bilgi Sistemleri Denetimi Konfigürasyon Birimleri Tanımlanması ve Korunması Denetim Çalışmaları Kontrol Durumu Belirleme Çalışması

	DS09 Konfigürasyon Yönetimi Bilgi Sistemleri Denetimi									
Risk Kodu	**Anahtar Kontrol**	**Kontrol Referansı**		**Kontrol**	**Etki**	**Kontrolü Yapan**	**Kontrol Sahibi Birim/**	**Kontrol Sıklığı**	**Kontrol Türü**	**Bankadaki Uygulama**
		Alt Süreç Kodu: DS09.02.Konfigürasyon Birimleri Tanımlanması ve Korunması Kontrol Durumu								
1	**Evet**	**DS09**	**DS9.2**	**Tüm konfigürasyon öğelerinin ve özelliklerinin belirlenmesini ve bilgilerinin güncelliğinin sağlanmasını sağlayan bir politikanın olduğu ve uygulanmakta olduğu sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü <Bu kısımda ilgili bankaya ait kontrol/Süreç sahibi birim belirtilir>**	**Yıllık<Bu kısımda bankada hangi sıklıkla kontrol yapıldığı bilgisi verilir>**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
2	**Evet**	**DS09**	**DS9.2**	**Fiziksel varlıkların etiketlenmesini tanımlayan bir politikasının bulunduğu sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Gerektiğinde**	**Sistemsel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
3	**Evet**	**DS09**	**DS9.2**	**Fiziksel varlıkların politikaya göre etiketlendiği doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
4	**Evet**	**DS09**	**DS9.2**	**Rol tabanlı bir erişim politikasının bulunduğu sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

5	**Evet**	**DS09**	**DS9.2**	**Politika uyarınca, konfigürasyon deposuna yalnızca yetkili kullanıcıların erişebildiği doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
6	**Evet**	**DS09**	**DS9.2**	**Değişim ve problem yönetimi prosedürlerini konfigürasyon deposunun güncelliğinin sağlanması işleri ile entegre olarak işlemesini sağlayacak bir politikanın tanımlandığı sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
7	**Evet**	**DS09**	**DS9.2**	**Yeni, modifiye edilmiş ve silinmiş konfigürasyon öğelerinin kaydedilmesini ve konfigürasyon deposundaki konfigürasyom öğeleri ile ilişkilerini belirleyerek güncelliğini sağlayan bir bir sürecin varlığı sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
8	**Evet**	**DS09**	**DS9.2**	**Sürecin dokümantasyonu, süreç adımlarının zamanlı olarak gerçekleştirilmesi ve veri bütünlüğü denetlenmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
9	**Evet**	**DS09**	**DS9.2**	**Kritik konfigürasyon öğelerinin belirlenmesine yönelik analizlerin gerçekleştirilmesini tanımlayan bir sürecin varlığı ve uygulanmakta olduğu sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

10	**Evet**	**DS09**	**DS9.2**	**Bu sürecin değişim yönetimini, gelecekteki bilgi teknolojileri gereksinimlerini ve satın almalarını desteklediği doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
11	**Evet**	**DS09**	**DS9.2**	**Tedarik süreçlerinin yeni varlıkların konfigürasyon yönetimi aracında kayıt altına alınmasını gerektirdiğini hesaba kattığı sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
12	**Evet**	**DS09**	**DS9.2**	**Konfigürasyon yönetim verileri ile satın alma kayıtlarının mutabık olduğu doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

4.6.4.4. DS9.3 Konfigürasyon Entegrite Revizyonu

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

Yönetim Beyanı Kapsamında Konfigürasyon Yönetimi Denetim Çalışmaları

DS9.3.1 Konfigürasyon Entegrite Revizyonu Kontrol Amaçları

Konfigürasyon Bütünlüğünün Gözden Geçirilmesi - Güncel ve geçmiş konfigürasyonlara ilişkin verilerin bütünlüğünü doğrulamak için konfigürasyon verileri düzenli aralıklarla gözden geçirilmeli. Yazılım lisansı sözleşmelerinin aşılmaması için yüklü yazılımlar ile yazılım kullanımı politikaları gözden geçirilmelidir. Hatalar ve saplamalar raporlanmalı, eylem alınmalı ve düzeltilmelidir.

DS9.3.2 Konfigürasyon Entegrite Revizyonu Değer Unsurları

• Temel seviyelerden sapmaların belirlenebilmesi

• Problemlerin tespit edilmesi ve çözülmesinde iyileşme

• Yetkisiz olarak kullanılan yazılımların belirlenebilmesi

DS9.3.3 Konfigürasyon Entegrite Revizyonu Risk Unsurları

DS9.2.3 Konfigürasyon Birimleri Tanımlanması ve Korunması Risk Unsurları ile aynı Risk unsurlarını barındırır. Bunlar;

• Kritik iş bileşenlerinin belirlenememesi

• Değişim yönetiminin kontrol edilememesi ve iş kesintilerinin yaşanması

• Yanlış bilgi nedeniyle bir değişimin etkisinin değerlendirilememesi

• Varlık kayıtlarının doğru tutulamaması

DS9.3.4 Konfigürasyon Entegrite Revizyonu Kontrol Uygulamaları

Konfigürasyon Yönetimi Kapsamında Konfigürasyon Entegrite Revizyonu Kontrol Uygulamaları örnek çalışmaları sırasıyla yapılmıştır. Denetim raporları tüm Kontrol uygulamaları için oluşturulmuştur.

DS09.03. Konfigürasyon Entegrite Revizyonu Denetim Çalışmaları Kontrol Uygulamaları		
Denetim Amacı	**Test Çalışması**	**Çalışma Kağıdı Referans No**
1. Konfigürasyon verilerinin bütünlüğünü denetlemek için, konfigürasyon öğelerinin izlenmesini sağlayan bir süreç yürütülmelidir. Mevcut veriler ile öğeler arasında mutabakat sağlanmalı ve hatalar ile sapmaların raporlanması ve düzeltilmesi sağlanmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
2. Yüklü yazılım ve donanımlar ile konfigürasyon veritabanındaki, lisans kayıtlarındaki ve fiziksel etiketlerdeki bilgiler arasında düzenli aralıklarla mutabakat yapılmalı, uygun olduğu durumlarda otomatik araçlardan yararlanılmalıdır.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	
3. Düzenli aralıklarla yazılım kullanım politikası ile mevcut durumda kullanılan yazılımlar karşılaştırılmalı, lisans sözleşmelerine ve mevcut politikalara aykırı durumlar raporlanmalı ve düzeltilmelidir.	Bu kısımda ilgili bankaya özel bilgiler yer alır. Yapılan test çalışması kısaca açıklanır	

Tablo 8: DS09 Konfigürasyon Yönetimi Bilgi Sistemleri Denetimi Konfigürasyon Entegrite Revizyonu Denetim Çalışmaları Kontrol Durumu Belirleme Çalışması

	DS09 Konfigürasyon Yönetimi Bilgi Sistemleri Denetimi									
Risk Kodu	**Anahtar Kontrol**	**Kontrol Referansı**		**Kontrol**	**Etki**	**Kontrolü Yapan**	**Kontrol Sahibi Birim/**	**Kontrol Sıklığı**	**Kontrol Türü**	**Bankadaki Uygulama**
		Alt Süreç Kodu: DS09.03. Konfigürasyon Entegrite Revizyonu Kontrol Durumu								
1	**Evet**	**DS09**	**DS9.3**	**Tüm konfigürasyon verilerinin bütünlüğünü sağlayan bir sürecin varlığı sorgulanmalı ve doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü <Bu kısımda ilgili bankaya ait kontrol/Süreç sahibi birim belirtilir>**	**Yıllık<Bu kısımda bankada hangi sıklıkla kontrol yapıldığı bilgisi verilir>**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
2	**Evet**	**DS09**	**DS9.3**	**Fiziksel ortam ile kayıtlı verileri karşılaştıran raporlar gözden geçirilmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Gerektiğinde**	**Sistemsel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
3	**Evet**	**DS09**	**DS9.3**	**Sapmaların raporlandığı ve düzeltildiği doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
4	**Evet**	**DS09**	**DS9.3**	**Donanımların ve yazılımların konfigürasyon veri tabanı ile mutabakatının düzenli aralıklarla yapıldığı doğrulanmalıdır.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

5	**Evet**	**DS09**	**DS9.3**	**Mutabakatlar için otomatik araçlar kullanılıyor ise, bir manüel mutabakat gerçekleştirilmelidir.**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**
6	**Evet**	**DS09**	**DS9.3**	**Düzenli aralıklarla yazılım kullanım politikası ile mevcut durumda kullanılan yazılımların karşılaştırıldığı, lisans sözleşmelerine ve mevcut politikalara aykırı durumlar var ise tespit edilmelidir. (Kişisel programlar, lisanssız programlar ve her türlü uygunsuz yazılım kullanımları)**	**Yüksek**	**Bilgi Sistemleri Müfettişi**	**Operasyon Müdürlüğü**	**Yıllık**	**Manuel**	**<Bu kısımda ilgili bankaya ait kontrolü karşılamak üzere yapılan çalışmalar açıklanır>**

Konfigürasyon Entegrite Revizyonu ve Konfigürasyon Birimleri Tanımlanması ve Korunması başlıkları altında bulunan Denetim Çalışmaları Kontrol Uygulamaları Denetim Test Çalışmaları DS09 Konfigürasyon Yönetimi Süreç Denetimi Sonuç raporu formatında test sonuçlarını içerecek şekilde müfettişler tarafından hazırlanarak Bilgi Sistemleri Baş Müfettişine sunulur.

Bulgular süreç sahipleri tarafından düzeltilmek üzere belirtilen tarihler içerisinde mutabakata varılmaya çalışılır. Şayet Bulgu kapatılmadı ise tüm sebepler Bilgi sistemleri müfettişlerine bildirilir. Müfettiş var ise açık bulguları denetim raporunu ekleyerek onaylanmış raporunu Teftiş Kurulu başkanına sunar. Teftiş Kurulu başkanlığı tarafından rapor incelenir ve her hangi bir düzenleme yok ise onaylanır.

Bu şekilde tüm süreçler yetkili müfettişlerce denetlenir ve raporlanıp onaylanır. Bir araya getirilen raporlar ve Raporların oluşturulmasına mesnet teşkil eden tüm çalışma kağıtları, Denetim kanıtları sürecin teftişini yapan müfettişince dosyalanıp arşivlenir. Bağımsız denetçinin denetimleri sırasında sunulabilmek ve daha sonraki denetim çalışmalarına kaynak temsil edebilmek üzere saklanır.

Oluşturulan Yönetim Beyanı artık Yönetim Kurulu Onayına Sunulmaya hazırdır. Teftiş Kurulu Başkanı Yönetim Kuruluna yapacağı sunum ardından Yönetim Kurulu tarafından istenen bir düzenleme yok ise Yönetim Kurulu üyelerince imzalanarak Bağımsız Denetçilere sunulmaya hazır hale gelir.

Bağımsız denetçiler, 13 Ocak 2010 tarih ve 28006 sayılı Resmî Gazete'de yayımlanan "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Tebliğ" istinaden içerik ve şekline ilişkin usul ve esaslara göre raporlarını hazırlar.

Resmi Gazete'de 26/07/2011 Sayı: 26170 ile yayınlanan "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik" de belirtildiği üzere "Banka Bilgi Sistemleri Ve Bankacılık Süreçleri Denetim Raporu" adı verilen formlardan denetçinin görüşüne göre seçeceği Olumlu Görüş, Şartlı Görüş, Olumsuz Görüş, Görüşten Kaçınma formlarından birini doldurur ve Raporla birlikte BDDK ya sunulur.

5. SONUÇ

Yönetim Beyanı bankaların bilgi sistemleri risklerine karşı güçlerini önemli bir düzeyde artırması beklenmektedir. Yönetim kurullarının bankalarının tüm bankacılık bilgi sistemleri hakkında bilgi sahibi olmaları sağlanabilecek, kontrol zayıflıkları ortaya konulabilecektir. Yönetim Kurullarının farkındalığının artması, bilhassa kendi onayladıkları bir belgenin ve denetim çalışmalarının konusu hakkında bilgi sahipleri olmaları açısından büyük önem arz etmektedir.

Yönetim Beyanı çalışmaları banka süreçleri içinde etkin kontrol noktalarının oluşumunu ve gelişimini sağlayacak kontrol eksiklikleri, zayıflıkları denetim ekiplerince ilgili süreç sahiplerine iletileceği için banka denetim ekibinin de gelişimi sağlanacak uygulanan bankacılık bilgi sistemleri konularında bilgi düzeylerini artıracaktır.

Yapılan denetim çalışmaları bilgi sistemleri ekiplerince de yaptıkları işlerin önemini ortaya koyacak daha etkin ve verimli işlerin ortaya konmasını sağlayacaktır. Süreçlerin devamlı ve düzenli bir şekilde izlendiğinin bilincinde olan süreç sahipleri birim müdürleri veya yöneticileri kendi birimlerinde etkin bir biçimde yönetimi anlayışlarına katkı sağlayacaktır.

Yönetim Beyanı her yıl tekrarlanması bankalardaki bilgi sistemleri olgunluk yapısını güçlendirecek uygulanan süreçlerdeki kontrol hatalarını zamanla ortadan kaldıracaktır. Açık kalan bulguların bir sonraki yılın denetiminde bulunmaması için aksiyonlar alınacak ve düzeltmeler yapılacaktır. Tüm bunlar banka içinde gelişimi ve ilerlemeyi sağlayabilecektir.

Bütün bu gelişme ve olumlu yönler yanında bankaların yönetim beyanı hazırlamaya yönelik iş yükleri yetkin ve deneyimli personel istihdam etmeleri ve denetlenenlerin denetim baskısı engellenemeyecek yükler oluşturacaktır. Personelin eğitim ve gelişimi süreç bazlı denetim yöntemlerinin daha fazla denetçi ve kaynak ayrılarak kullanılması gerekecektir.

Yönetim beyanı çalışmalarının Türk Bankacılık sektörüne sağlayacağı faydalarını önümüzdeki yıllarda görebileceğiz.

Tez çalışmamız sırasında Yönetim Beyanı hazırlık çalışmaları ile tüm ilgililere kullanabilecekleri bilgiler sunulmuş hazırlama süreci detaylı olarak açıklanmıştır. Yönetim Beyanı çalışmalarının başlangıcından sonuçlanmasına kadar geçecek süreç açıklanmış ve bu konuda bankaların kullanabileceği formlar ve metodlar örnek olarak hazırlanmıştır. Yönetimi beyanı bilgi sistemleri denetim süreçleri arasından Cobit 4.1 DS09 Konfigürasyon Yönetimi denetim çalışmaları Yönetim Beyanına mesnet teşkil edebilecek şekilde hazırlanmıştır.

Çalışmamız Yönetim Beyanı konusunun akademik bir yayında ilk kez ele alınması ve bundan sonraki çalışmalara kaynak sağlayabilmesi açısından önem arz etmektedir.

Yönetim Beyanı Konusu Türkiye İç Denetim Enstitüsü'nün İç Denetim Dergisinin 10.Yıl Özel Sayısında (Sonbahar 2011, Sayı 30) Aysberg konusu olarak ele alınmış başta BDDK Bilgi Yönetimi Daire Başkanı Ahmet Türkay Varlı ve İç Denetim Enstitüsü'nün değerli yöneticileri olmak üzere bir çok bankanın Denetim ve Risk ile ilgili Genel Müdürleri, Teftiş Kurulu başkanlarının görüşlerine yer verilmiştir.

Ortaya konan ortak kanaat Yönetim Beyanı'nın Bankalar için bir fırsat olduğu ve getireceği operasyon yükünün yanında, bankanın gelişimine doğrudan katkı sağlayacağı yönündedir.

Tüm bu çalışmalar neticesinde 2012 yılında Beyanlar sunulacak ve çalışmalar meyvelerini verecektir. Yönetim Beyanın sonuçlarını hep beraber göreceğiz. Umarız Türk Bankacılık Sektörü güçlü yapısına katkı sağlayarak daha fazla gelişmesi yönünde adımlar atılmasına vesile olur.

KAYNAKÇA

Alpay, B. Naci. 2008. ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması. Yüksek Lisans Tezi. Haliç Üniversitesi Fen Bilimleri Enstitüsü.

Aydoğdu, Fatih. 2010. Bankacılık Sektöründe Kurum Kimliğinin Oluşumunda Yeni İletişim Teknolojilerinin Kullanımı: Türkiye İş Bankası Örneği. Yüksek Lisans Tezi. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü

Artinyan, E. Natasa. [11.10.2011]. CobiT Çerçevesi. http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf

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

Baraçlı, Hayri. "Kriz ve Teknoloji Yönetimi", **3Gen Dergisi**, 2001.

Bddk. **Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ.**.(Sayı 27120; Tarih: 06.2010)

_____. **Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka bilgi sistemleri ve bankacılık süreçlerinin denetimine İlişkin Rapor Hakkında tebliğ.** (Sayı 27461; Tarih: 13 Ocak 2010)

_____. **Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğ.** (Sayı 26367; Tarih: 5 Aralık 2006)

_____. **Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik** (Sayı: 28006; Tarih: 26/07/2011)

_____. **Yönetim Beyanı Genelgesi**, Genelge (BSD.2010/3, 30.07.2010).

_____. **Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğine** (Sayı 26367; Tarih: 5 Aralık 2006)

_____. **Bilgi Sistemleri Denetimlerinde Tespit Edilen Bulguların Kodlanması Hakkında Genelge** (Sayı: BYD.138/1 Tarih:29 Aralık 2008)

_____. **Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik.** (Sayı : 28106; 5 Kasım 2011)

Bilişimin 10 Milyar $ Yolculuğu.[20.10.2011] **Capital Dergisi.** http://www.capital.com.tr/bilisimin-10-milyar-$-yolculugu-haberler/21297.aspx

Carnegie Mellon University. [28.11.2011] . **Konfigurasyon Yönetimi İçin CMMI Süreçleri.**http://ieee.metu.edu/iffet/blog/Konfigurasyon_Yonetimi_CMII-V1.2.pdf

Christopher M. 1991. **Information Systems**, McGraw-Hill,9.(Aktaran: Polat , Necip. [21.11.2011] .Yönetim bilgi sistemi ve Sayıştayda yürütülen çalışmalar.**Sayıştay Dergisi**, c.65, http://dergi.sayistay.gov.tr/icerik/der65m14.pdf).

CobiT 5, **Yakın Bir Zamanda Hayatımızdaki Yerini Alacak**!. [12.11.2011] http://www.pwc.com/tr/tr/service/it-services/cobit-bes/index.jhtml

Cobit 5 Taslak Dokümanları Yayınlandı. [13.11.2011]. http://blog.lostar.com/2011/07/cobit5-taslak.html

Cüneyt Sezgin, Mustafa A. Aysan, Hakan Tıraşan ve diğ. Yönetim Beyanı'ndan Neler Bekliyoruz?. **Türkiye İç Denetim Enstitüsü İç Denetim Dergisi.** 10.Yıl Özel Sayısı (2011):6-33

Çetin, R.Reha. 2007 .Yazılım Mühendisliğinde Uygulama Geliştirmede bir Çözüm: Yazılım Konfigürasyon Yönetimi. Doktora Tezi. T.C. Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Deloitte, **Yönetim Beyanı Hakkında**. İstanbul, 2010.

Demircan M. L. **Bilgiyi Yönetmek**, İstanbul: Beta Basım Yayım Dağıtım A.Ş,1997.

Durkaya , Tanıl. [10.11.2011]. Banka İç Denetimlerinde Yeni bir dönem Başlıyor. **KPMG Gündem Ekim-Aralık 2010**. http://www.kpmgvergi.com/tr-tr/SanalKutuphane/yayinlar/guncelyayinlar/Documents/kpmgundemsayi04.pdf

Erdoğan, M. **Denetim,** 2.bs, Ankara:Maliye ve Hukuk Yayınları, 2005.

Güredin, E. **Denetim ve Güvence Hizmetleri**, 11.bs, İstanbul: Arıkan Yayınları, 2007.

Hacısüleymanoğlu, Emine. 2010. Bilgi Teknolojileri Yönetişim Yöntemleri ve Cobit ile Ulusal Bir Bankada Uygulaması. Yüksek Lisans Tezi , Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü.

Intosai (IDI). **Intorduction of IT Audit e-learning Course Notes**, USA,2007. (Aktaran: Yıldız, Ö. Rıza. [24.11.2011]. Bilişim Sistemleri Denetimi ve Sayıştay, **Sayıştay Dergisi**, s.65. http://dergi.sayistay.gov.tr/default.asp?sayfa=4&id=65).

Isaca. **IT Assurance Guide Using Cobit.** USA, 2007.

____. **Control Objectives for Information and Related Technology 4.1.** USA, 2007.

____. **Control Objectives for Information and Related Technology 4.0.** USA, 2005.

Şerif, Ş. **Yönetim ve Organizasyon**, Konya: Günay Ofset, 2002.

Şenver, Bülent. **Muhasebe ve Finansman Dergisi**, s.7, 2000.

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

Karaman, Özhan. **ITIL Temelli BT Hizmet Yönetimi.** 6. Linux ve Özgür Yazılım Şenliği 2007, http://seminer.linux.org.tr/wp-content/uploads/itil_temelli_bt_hizmet_yonetimi.pdf [27.11.2011]

Kate Behan, , Holmes, Diana, **Understanding Information Technology**, 2.bs, New York:Prentice Hall Inc.,1990.

Kenneth C. Laudon, Jane P. Laudon, **Management Information Systems : Managing The Digital Firm,** 7.bs, USA:Prentice Hall, 2001.

Konfigürasyon Yönetimi. [27.11.2011]. http://www.bilgisite.com/yonetim/yonetim_06.html

Köşe Yazarları Haberleri. [21.11.2011]. Ekonometri Dergisi. http://www.ekonometri.com.tr/ index.php?page=habergoster&hbrID=670

Milli Prodüktivite Merkezi .**Türk Bankacılık Sistemine İlişkin Bir Değerlendirme (1973-1988)**. Ankara: Milli Prodüktivite Merkezi Yayınları, 1990.

Özbilgin, İ. Gökhan. Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar. **Sayıştay Dergisi,** s.49, (2003)

Polat , Necip. [21.11.2011] .Yönetim bilgi sistemi ve Sayıştayda yürütülen çalışmalar.**Sayıştay Dergisi**, c.65, http://dergi.sayistay.gov.tr/icerik/der65m14.pdf

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

Sayıştay. [26.11.2011]. Hazine Bilişim Sistemleri Denetimi Raporu http://www.sayistay.gov.tr/rapor/hazine/diger/Hazine_Bilisim_SistemleriRaporu.pdf

Topkaya, Cem. 2008.ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması. Yüksek Lisans Tezi. Haliç Üniversitesi Fen Bilimleri Enstitüsü.

Türkiye Bankalar Birliği, [18.10.2011], İnternet ve Mobil Bankacılık İstatistikleri Haziran 2011. http://www.tbb.org.tr/tr/Banka_ve_Sektor_Bilgileri/Linkler.aspx?RId=1029

Türkiye İç Denetim Enstitüsü, "Yönetim Beyanından Neler Bekliyoruz", **İç Denetim,** 10.yıl Özel Sayısı Sonbahar, (2011):21.

_____, "Bağımsız Denetim Kuruluşları Yönetim Beyanı Konusunda Neler Söylüyor?", **İç Denetim,** 10.yıl Özel Sayısı Sonbahar, (2011):33.

Uzun, A. Kamil. "Organizasyonlarda İç Denetimin Fonksiyonu ve Önemi". **Active Bankacılık ve Finans Dergisi**, s.6, (1999):2.

Uzunay, Vildan. **COBIT (Control Objectives for Information and related Technology).** Ankara: İç Kontrol Merkezi Uyumlaştırma Dairesi, 2007.

Weber, R. **Information Systems Control and Audit**. 1999.(Aktaran: Yıldız, Ö. Rıza. [24.11.2011]. Bilişim Sistemleri Denetimi ve Sayıştay, **Sayıştay Dergisi**, s.65. http://dergi.sayistay.gov.tr/default.asp?sayfa=4&id=65)

Varlı, A.Türkay, Türkiye İç Denetim Enstitüsü, XI. Türkiye **İç Denetim Kongresi Sunumu.** İstanbul, 2007.

Yıldız, Ö. Rıza. [24.11.2011]. Bilişim Sistemleri Denetimi ve Sayıştay, **Sayıştay Dergisi**, s.65. http://dergi.sayistay.gov.tr/default.asp?sayfa=4&id=65

Yılmaz, E. Aykut. [20.11.2011]. **Bankalara Yönetim Beyanı Zorunluluğu.** http://www.dunya.com/bankalara-yonetim-beyani-zorunlulugu_98522_haber.html

İnternet Kaynakları

http://www.isaca.org

http://www.ekonometri.com.tr/ index.php?page=habergoster&hbrID=670

http://www.tbb.org.tr/tr/Banka_ve_Sektor_Bilgileri/Linkler.aspx?RId=993

http://www.bddk.org.tr

http://www.tdk.gov.tr

www.itil-officialsite.com

http://en.wikipedia.org/wiki/ITIL

http://en.wikipedia.org/wiki/Risk_management

http://www.slideshare.net/ISACA-Istanbul/isacaistanbul-ynetim-beyan-sunumu-29032011

EKLER

Ek 1. İnternet bankacılığı istatistikleri gönderen bankalar

1 Akbank T.A.Ş.

2 Aktif Yatırım Bankası A.Ş.

3 Alternatif Bank A.Ş.

4 Anadolubank A.Ş.

5 BankPozitif Kredi ve Kalkınma Bankası A.Ş.

6 Citibank A.Ş.

7 Denizbank A.Ş.

8 Eurobank Tekfen A.Ş.

9 Fibabanka A.Ş.

10 Finans Bank A.Ş.

11 HSBC Bank A.Ş.

12 ING Bank A.Ş.

13 Şekerbank T.A.Ş.

14 Tekstil Bankası A.Ş.

15 The Royal Bank of Scotland N.V.

16 Turkish Bank A.Ş.

17 Turkland Bank A.Ş.

18 Türk Ekonomi Bankası A.Ş.

19 Türkiye Cumhuriyeti Ziraat Bankası A.Ş.

20 Türkiye Garanti Bankası A.Ş.

21 Türkiye Halk Bankası A.Ş.

22 Türkiye İş Bankası A.Ş.

23 Türkiye Sınai Kalkınma Bankası A.Ş.

24 Türkiye Vakıflar Bankası A.Ş.

25 Yapı ve Kredi Bankası A.Ş.

Mobil bankacılık istatistikleri gönderen bankalar

1 Akbank T.A.Ş.

2 Aktif Yatırım Bankası A.Ş.

3 Denizbank A.Ş.

4 Finans Bank A.Ş.

5 ING Bank A.Ş.

6 Şekerbank T.A.Ş.

7 Türk Ekonomi Bankası A.Ş.

8 Türkiye Cumhuriyeti Ziraat Bankası A.Ş.

9 Türkiye Garanti Bankası A.Ş.

10 Türkiye İş Bankası A.Ş.

11 Yapı ve Kredi Bankası A.Ş.

Ek 2. Yönetim Beyanı Yetkilendirme Bildirimi

XBANK TEFTİŞ KURULU BAŞKANLIĞINA

Sayı : XBNK.2011.12.YB.1
Konu: Yönetim Beyanı Yetkilendirme Bildirimi

Bankacılık Düzenleme ve Denetleme Kurulu Bilgi Yönetimi Dairesi tarafından 30.07.2010 tarihinde yayınlanan genelge ile bankaların …… yılı denetim döneminde hazırlanacak Yönetim Beyanı ve uygulaması hakkında tüm çalışma ve denetimlerin sorumluluğunu Teftiş Kurulu başkanlığımıza verilmiştir.

Denetimin başarıyla sonuçlanması için gerekli çalışmaların yapılmasını ve süreç sonunda Yönetim Beyanı'nın tarafımıza sunulmasını rica ederiz.

Yönetim Kurulu Başkanı

Yönetim Kurulu Üyesi	**Yönetim Kurulu Üyesi**	**Yönetim Kurulu Üyesi**
(imza)	(imza)	(imza)

Ek 3. Yönetim Beyanı Süreç Denetimi Süre Planı

XBANK TEFTİŞ KURULU BAŞKANLIĞI YÖNETİM BEYANI SÜREÇ DENETİMİ SÜRE PLANI FORMU

Denetim Numarası:

	Planlanan Tarih ve Süre	Revize Edilen Tarih ve Süre	Gerçekleşen Tarih ve Süre	Planlananın Üzerinde/Altında Gerçekleşen Süre
Denetlenecek 1. Süreç				
Denetlenecek 2. Süreç				
Denetlenecek 3. Süreç				
Denetlenecek 4. Süreç				
Denetlenecek 5. Süreç				
Denetlenecek 6. Süreç				
Denetlenecek 7. Süreç				
Yapılacak N. Süreç				
TOPLAM SÜRE				

*Planlanan denetim süresi revizyonları, Denetim Süresi Revizyon Formu ile desteklenecektir.

Ek 4. Yönetim Beyanı Denetim Süresi ve Kaynağı Revizyon Formu

XBANK YÖNETİM BEYANI DENETİM SÜRESİ
VE KAYNAĞI REVİZYON FORMU

Süreç Adı :	
Denetim Numarası:	

Toplam Planlanmış Denetim Süresi:	
İstenen Değişiklik:	
Revize Edilmiş Planlanan Denetim Süresi:	
Revizyon İstenmesinin Nedeni:	

Toplam Planlanmış Denetim Kaynağı:	
İstenen Değişiklik:	
Revize Edilmiş Planlanan Denetim Kaynağı:	
Revizyon İstenmesinin Nedeni:	

Önerilen Revizyon Uygundur

…../…./…..
TEFTİŞ KURULU BAŞKANLIĞI
(imza)

Ek 5. Yönetim Beyanı Bireysel Süreç Denetimi Süre Planı

XBANK YÖNETİM BEYANI
BİREYSEL SÜREÇ DENETİMİ SÜRE PLANI FORMU

Denetlenen Süreç Adı:
Denetim Numarası:

	Planlanan Tarih ve Süre	Revize Edilen Tarih ve Süre	Gerçekleşen Tarih ve Süre	Planlananın Üzerinde/Altında Gerçekleşen Süre
Yapılacak 1. Denetim Adımı				
Yapılacak 2. Denetim Adımı				
Yapılacak 3. Denetim Adımı				
Yapılacak 4. Denetim Adımı				
Yapılacak 5. Denetim Adımı				
Yapılacak 6. Denetim Adımı				
Yapılacak 7. Denetim Adımı				
Yapılacak N. Denetim Adımı				
TOPLAM SÜRE				

*Planlanan denetim süresi revizyonları, Denetim Süresi Revizyon Formu ile desteklenecektir.

Ek 6. Yönetim Beyanı Süreç Sahipleri İle Yapılan Açılış Toplantısı Tutanağı

YÖNETİM BEYANI SÜREÇ SAHİPLERİ
AÇILIŞ TOPLANTISI TUTANAĞI

Süreç Adı :……

Denetimin Numarası :……

Toplantı Tarihi :……

Toplantıya Katılan Müfettişler :……

Denetlenen Birim :……
……

Denetlenen Birim Yöneticisinin Adı ve Unvanı:
……

Toplantıya Katılan Birim Personeli :……
……
……

- Gündeme Getirilen Önemli Konular: :

……

……

……

(imza) (imza) (imza)

Ek 7. Yönetim Beyanı Süreç Sahipleri İle Yapılan Kapanış Toplantısı Tutanağı

YÖNETİM BEYANI SÜREÇ SAHİPLERİ
KAPANIŞ TOPLANTISI TUTANAĞI

Süreç Adı :……

Denetimin Numarası :……

Toplantı Tarihi :……

Toplantıya Katılan Müfettişler :……

Denetlenen Birim :……
……

Denetlenen Birim Yöneticisinin Adı ve Unvanı:
……

Toplantıya Katılan Birim Personeli :……
……
……

- Bulgu Numaraları :……
- ……

- Denetlenen Birim Yönetiminin Mütalaası :

……

……

……

(imza) (imza) (imza)

Ek 8. Yönetim Beyanı Müfettiş Örnek Çalışma Kağıdı

ÖRNEK ÇALIŞMA KAĞIDI

XBANK TEFTİŞ KURULU **(Hazırlanma Tarihi)**
DENETLENEN BİRİM
DENETLENEN SÜREÇ

TEST	
AMAÇ	
YÖNTEM	
EDİNİLEN BİLGİ	
SONUÇ	
HAZIRLAYAN **(Ad Soyad, Unvan, Tarih, İmza)**	**GÖZDEN GEÇİREN** **(Ad Soyad, Unvan, Tarih, İmza)**

Ek 9. Yönetim Beyanı İş Akışı ve Risk Kontrol matrisleri Süreç Sahibi Onay Tutanağı

XBANK TEFTİŞ KURULU BAŞKANLIĞINA

Sayı : XBNK.2011.12.YB.BT.01
Konu: İş Akışı ve Risk Kontrol matrisleri Onayı

Yönetim Beyanı kapsamında gerçekleştireceğiniz denetimlere konu olan.....
.....
.....sürecinin risk kontrol matrisleri ve iş akışları güncel olup birimimiz tarafından işletilmektedir.

Birim Yöneticisi/Müdürü

(Tarih/ imza)

Ek 10. Yönetim Beyanı Genelgesi

BANKACILIK DÜZENLEME VE DENETLEME KURUMU
(Bilgi Yönetimi Dairesi)

Sayı: B.02.1.BDK.0.77.00.00.010.06.02/3 30.07.2010

Konu: Yönetim Beyanı

GENELGE
BSD.2010/3

Bankalarda bağımsız denetim kuruluşlarınca gerçekleştirilecek bilgi sistemleri ve bankacılık süreçleri denetimine (BSD) ilişkin usul ve esaslar, 13.01.2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren "Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik" (Yönetmelik) ile düzenlenmektedir.

Yönetmeliğin 19 uncu maddesinin yedinci fıkrası ile 33 üncü maddesinin birinci fıkrası uyarınca bankalar, bilgi sistemleri ve bankacılık süreçleri üzerindeki iç kontrolleri hakkında denetim dönemi itibariyle yönetim kurullarınca düzenlenecek Yönetim Beyanını bağımsız denetçiye sunmakla yükümlüdür.

Yönetmeliğin 44 üncü maddesi uyarınca, 2011 yılı denetim döneminden itibaren hazırlanacak olan Yönetim Beyanı ve uygulamasında işbu Genelge ile çerçevesi çizilen usul ve esaslar dikkate alınır.

1) Amaç

Yönetim Beyanının amacı, banka yönetim kurulunun, bankanın bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontrollerinin BSD dönemi açısından etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, bu çerçevedeki mevcut durum ve yürütülen çalışmalara ilişkin güvence sunmasıdır.

2) Kapsam

Banka, Yönetim Beyanı çerçevesinde bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin kanaat oluştururken, Yönetmeliğin 24 üncü maddesinde yer verilen bilgi sistemleri denetimi ve 25 inci maddesinde yer verilen bankacılık süreçleri denetimi kapsamını dikkate alır.

Bilgi sistemleri ve bankacılık süreçleri dâhilinde değerlendirilecek alanlar, risk odaklı bir bakış açısıyla ve Yönetmeliğin 5 inci maddesinde yer verilen önemlilik kriteri esas alınarak belirlenir. Bu değerlendirme kapsamı, Yönetim Beyanında bilgi sistemleri ve bankacılık süreçlerinin bütünü için verilecek görüşe makul güvence sunacak ölçüde yeterli denetim kanıtının temin edilmesine imkân sağlayacak şekilde belirlenir.

Yönetim Beyanı sadece banka bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontroller hakkında düzenlenir. Yönetim Beyanı oluşturulurken alınan destek hizmetleri de göz önünde bulundurulur.

Yönetim Beyanı kapsamında, Yönetmeliğin 22 nci maddesinin dördüncü fıkrasında ifade edilen BSD periyodundan bağımsız olarak, her dönem için hem bilgi sistemleri hem de bankacılık süreçlerine ilişkin iç kontroller hakkında değerlendirmelerde bulunulur.

3) Dönem

Banka yönetim kurulu, Yönetim Beyanını, cari BSD dönemine ilişkin yürütülen çalışmalar ve değerlendirmeler neticesinde oluşturur. Bu bağlamda esas alınacak dönem 1 Ocak -31 Aralık dönemi olup, banka yönetim kurulu bu dönemin sonu itibariyle, BSD raporu tarihi ile uyumlu olarak beyanda bulunur.

4) İçerik

Yönetim Beyanında; açık ve kesin ifadelerle, asgari olarak:

a) Banka yönetim kurulunun 5411 sayılı Bankacılık Kanununun 29 ve 30 uncu maddeleri ve 1 Kasım 2006 tarihli ve 26333 sayılı Resmi Gazete'de yayımlanan Bankaların İç Sistemleri Hakkında Yönetmelik'in 4 üncü maddesinin birinci fıkrasına istinaden etkin, yeterli ve uyumlu bir iç kontrol sistemi kurma ve işletme yükümlülüğünün bulunduğu,

b) İlgili banka birimlerince, iç kontrol sisteminin incelenmiş ve bu sistem hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılmış olduğu,

c) İlgili banka birimlerince iç kontrol sistemi hakkında yapılan değerlendirmede bağımsız denetim kuruluşu tarafından gerçekleştirilen çalışmaların kullanılmadığının taahhüt edildiği,

ç) İç kontrol sistemi üzerinde -varsa- tespit edilen önemli kontrol eksiklikleri,

d) İç kontrol sisteminin, Bankaların İç Sistemleri Hakkında Yönetmelik'in "İç Kontrol Sistemi" başlıklı İkinci Kısmı ile 14 Eylül 2007 tarihli ve 26643 sayılı Resmi Gazete'de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'de belirtilen usul ve esaslar açısından etkinliği, yeterliliği veya uyumluluğuna engel teşkil edecek ve (ç) fıkrası çerçevesinde beyan edilenlerin haricinde herhangi bir önemli kontrol eksikliğinin olmadığı,

e) İç kontrol sistemi üzerinde yapılan değerlendirmelerde -dönem sonu itibariyle düzeltilmiş olsa dahi- tespit edilen iç kontrol sistemine ilişkin tüm kontrol zayıflıklarının, kayda değer ve önemli kontrol eksikliklerinin sınıflandırılarak bağımsız denetçiye sunulduğu,

f) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere banka açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen ya

da önemli seviyede olmasa da yöneticilerin veya iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu tüm suistimal veya yolsuzluklar, z

g) Daha önceki bağımsız bilgi sistemleri ve bankacılık süreçleri denetimlerinde tespit edilip bankaya sunulmuş ve bağımsız denetim kuruluşu tarafından çözüldüğü onaylanmamış olan bulguların çözülüp çözülmediğine ilişkin mevcut durumuna Yönetim Beyanı ekinde yer verildiği,

h) İç kontrol sisteminde gerçekleştirilen incelemeleri takiben, önemli ve kayda değer kontrol eksiklikleri konularında banka tarafından alınmış olan düzeltici önlemleri de içerecek şekilde, iç kontrol sisteminde veya iç kontrol sistemini önemli derecede etkileyebilecek diğer hususlarda meydana gelmiş olan değişiklikler

beyan edilir.

5) Yürütülecek Çalışmalar ve Beyanın Oluşturulması

Bilgi sistemleri ve bankacılık süreçlerine ilişkin iç kontroller hakkındaki Yönetim Beyanına mesnet teşkil edecek çalışmalar, banka iç sistemler birimlerince Yönetmeliğin "Bilgi Sistemleri ve Bankacılık Süreçleri Denetimine İlişkin Esaslar" başlıklı Beşinci Bölümü ile "Bilgi Sistemleri ve Bankacılık Süreçleri Denetimi Metodolojisi" başlıklı Altıncı Bölümü çerçevesindeki usul ve esaslar dikkate alınarak gerçekleştirilir.

6) Raporlama

Yönetim Beyanı banka yönetim kurulunca düzenlenir ve denetim dönemini takip eden Ocak ayı sonuna kadar bağımsız denetim kuruluşuna iletilir.

Banka, Yönetim Beyanı sunulmadan önce bağımsız denetim kuruluşunun, yapılan çalışmalar ve sonuçlarına ilişkin her türlü bilgi ve belge talebini zamanında karşılar.

7) Yönetim Beyanının ve İlgili Çalışmaların Değerlendirilmesi

Bağımsız denetim kuruluşu, Yönetim Beyanını ve bu beyana mesnet teşkil eden çalışmaların yeterliliğini inceler. Bağımsız denetçi beyanda, içerik açısından eksiklik veya bağımsız denetim çalışması sonuçları itibariyle uyumsuzluk tespit ederse denetim raporunda ayrı bir bölüm halinde bu tespitlere yer verir.

Tebliğ olunur.

Tevfik BİLGİN
Başkan

ÖZGEÇMİŞ

Doğum Tarihi: 07.11.1987

Doğum Yeri: Elbistan

Lise: Karşıyaka Lisesi

Lisans: 2005–2009 Yıldız Teknik Üniversitesi Elektrik Elektronik Fakültesi Bilgisayar Mühendisliği

Yüksek Lisans: 2009- Yıldız Teknik Üniversitesi Sosyal Bilimleri Enstitüsü İşletme Yönetimi Tezli Yüksek Lisans Programı

Çalıştığı Kurumlar:

2008-2009 Deloitte Technology Services

2009- 2011 Garanti Teknoloji

2011- Devam KuveytTurk Teftiş Kurulu