BİLGİ KRİTERLERİ ÇERÇEVESİNDE BİLİŞİM TEKNOLOJİLERİ DENETİMİ

Musa KAYRAK*

ÖZET

Bilginin en değerli varlık olarak kabul edildiği bugünün dünyasında, verilerin bilgiye ve sonrasında bilgi birikimine dönüşmesi bilişim teknolojisi araçlarıyla sağlanmaktadır. Hayatımızın vazgeçilmez bir unsuru haline gelen bilişim teknolojileri (BT), karar alma süreçlerinde belirleyici bir rol oynarken; eski kurumsal yapılar ve yönetim yaklaşımları ile bilgiden optimum düzeyde fayda sağlamak artık mümkün değildir. Halen yaşanmakta olan bilişim teknolojileri dönüşüm süreci, yönetim araçlarını değiştirdiği kadar, bilginin yaşam döngüsündeki risk ve kontrollerin doğasını da değiştirmiş ve dolayısıyla yeni denetim anlayışlarının ve prosedürlerinin ortaya çıkmasına neden olmuştur. Bu gelişmelerin paralelinde, standartlara uygun olarak ve risk odaklı bir denetim yaklaşımıyla yürütülen BT denetimi, yirminci yüzyılın son çeyreğinden itibaren denetim mesleğine yeni bir boyut kazandırmıştır.

Bütünlük, güvenilirlik, gizlilik, uygunluk, süreklilik, verimlilik ve etkinlik gibi bilgi kriterleri çerçevesinde tespit edilen riskler ve kontrol hedefleri, hem kurum yöneticileri hem de denetçiler için yol göstericidir. Söz konusu bilgi kriterlerinden hareketle, BT denetiminin türü ve hedefleri doğrultusunda farklı denetim programları oluşturmak mümkündür. Aynı şekilde, BT yönetişimi, bilgi güvenliği ve verinin güvenilirliği gibi BT denetiminin önemli konularına ilişkin kontrol testlerinin ve maddi doğrulama testlerinin kapsamı, bilgi kriterlerinden yola çıkılarak belirlenebilir. Bu noktada, ulusal mevzuatta yer alan zorlayıcı hükümler ile ulusal ve uluslararası standartlar, başvurulması gereken en temel kaynaklardır.

Anahtar Kelimeler: Bilişim Teknolojisi (BT), BT Denetimi, Bilgi Kriterleri, BT Yönetişimi, Bilgi Güvenliği.

INFORMATION TECHNOLOGY AUDIT IN THE CONTEXT OF INFORMATION CRITERIA

ABSTRACT

In today's world where information is considered the most valuable asset, transformation of data into information and afterwards knowledge is realized by means of information technology instruments. While information technologies (IT) which have turned out to be the most indispensable fact in our lives play a decisive role in decision-making processes, it is not feasible to benefit from information at the optimum level with archaic organizational structures and management approaches. Currently ongoing process

* Sayıştay Başdenetçisi, CISA (Sertifikalı Bilişim Sistemleri Denetçisi)

of information technology transformation has altered the nature of the risks and controls in the lifecycle of information as well as management tools and thereby caused to the rise of new understandings in auditing and audit procedures. In parallel with these developments, IT audit carried out in accordance with standards and a risk-based approach has provided a new dimension to the audit profession since the last quarter of the twentieth century.

Risks and control objectives determined within the framework of information criteria such as integrity, reliability, confidentiality, compliance, availability, effectiveness and efficiency provide guidance to both managers and auditors. It is likely to form different audit programs in line with IT audit type and objectives by relying on those information criteria. By the same token, the scope of control tests and substantive tests relating to the crucial topics in IT audit such as IT governance, information security and reliability of data can be determined by referring to information criteria. At this point, compelling provisions of national regulations and national and international standards are the most essential resources to be applied.

Keywords: Information Technology (IT), IT Audit, Information Criteria, IT Governance, Information Security.

GİRİŞ

Günümüzde stratejik karar verme mekanizmalarını en etkin düzeyde işletebilmek için ihtiyaç duyulan kurumsal bilgiler, karmaşıklık düzeyi yüksek bilişim sistemleri (BS) yardımıyla üretilmekte ve yönetilmektedir. Özel sektör organizasyonları, bilişim dünyasında yaşanan ilerlemelerden en üst düzeyde fayda sağlayarak faaliyet gösterdikleri alanda rekabetçi kalabilmek; kamu kurum ve kuruluşları ise vatandaşlara sağladıkları hizmetleri daha hızlı, kolay ve şeffaf bir biçimde sunabilmek amacıyla yüksek maliyetli bilişim teknolojileri (BT) yatırımları yapmaktadır. Bilişimin iş süreçlerinin ayrılmaz bir parçası haline gelmesiyle birlikte, organizasyonların en değerli varlığı olan veri, bilgi ve bilgi birikiminin geleneksel risk ve kontrol anlayışı ile yönetilmesi imkânsız hale gelmiştir. Bu nedenle, kurumsal risklerin BT ortamının koşullarına uygun bir yaklaşım ile yönetilmesi, BT yatırımlarından beklenen değerin, doğru maliyetlerle ve kabul edilebilir risk düzeyinde elde edilebilmesi için önemli bir rol oynamaktadır.

Yaşanan teknolojik dönüşümle birlikte, değişik kademelerdeki yönetici ve kurum çalışanları için yeni görev tanımları ve sorumluluklar ortaya çıkmıştır. Aynı şekilde, uluslararası standartlarda yönetim süreçlerinin bir parçası olarak kabul edilen denetim mesleğinin de söz konusu koşullar çerçevesinde kendisini yenileme çabası, BT denetiminin giderek popüler bir çalışma alanı olmasına neden olmuştur. BT denetimlerini icra eden özel sektör kuruluşları, iç ve dış denetim birimleri ile uluslararası organizasyonlar açısından standartlar, metodoloji, risk ve kontroller konusunda ortak bir çerçeve mevcut iken; BT denetimlerinin hangi hedefler

doğrultusunda ve nasıl yürütülmesi gerektiği konusunda sektör, denetim anlayışı, yasal zorunluluklardan kaynaklanan yetki, yaklaşım ve uygulama farklılıkları mevcuttur.

Bu çalışmada BT denetiminin, diğer denetim türleri ile ilişkisi, standartlar, metodoloji, risk ve kontroller çerçevesinde genel bir değerlendirmesi yapılmış ve COBIT 4.1 çerçevesinde Avrupa Birliği Sayıştayı (ECA) tarafından uygulanan BT denetim yaklaşımına yer verilmiştir. Bu yaklaşım, bilgi kriterlerinin birincil ve ikincil düzeyde ilişkili olduğu BT süreçleri ve bunlara ilişkin kontrollerle eşleştirilmesi suretiyle BT denetim programlarının hazırlanmasına dayanır[1]. Diğer bir ifade ile yürütülecek denetimin hedeflerini destekleyen etkililik, verimlilik, gizlilik, bütünlük, süreklilik, güvenilirlik ve mevzuata uyum kriterlerinden bir ya da daha fazlası seçilerek, BT kontrolleri, BT süreçleri ve denetimin amaçları arasında ilişki kurulur. Ayrıca, BT denetiminin kamuda ve özel sektörde uygulanması ve sonuçlarının kabul edilirliği için, standart ve ilgili mevzuata referans verilmesi olmazsa olmaz bir ön koşuldur. Bu bağlamda, BT denetimlerinde karşılaşılan en temel sorunlardan veri güvenilirliği, BT yönetişimi ve bilgi güvenliği konuları, anılan denetim metodolojisi çerçevesinde bilgi kriterleri ve BT süreçleriyle ilişkilendirilmiş ve hangi genel kontroller ve uygulama kontrollerinin değerlendirilmesi gerektiği, standart ve mevzuat hükümleri de dikkate alınarak tespit edilmiştir.

1. TEKNOLOJİ VE TEMEL KAVRAMLAR

Literatürde derinlemesine tartışmaları yapılan ve farklı tanımlamaları olan veri, enformasyon ve bilgi kavramları çoğu kez birbirleriyle karıştırılmaktadır. Kısaca açıklamak gerekirse veriler, olaylar ve olgular hakkında işlenmemiş nesnel gerçekliklerdir ve genellikle kendi başlarına anlam ifade etmezler (Demirel ve Durna, 2008:133). Veri, bir ses veya video kaydı olabileceği gibi, bir grafik yahut sayısal bir anlatım şeklinde de olabilir. Enformasyon, organize edilmiş ve özetlenmiş verileri ifade etse de insan beyni tarafından işlenmediği sürece bilgiye dönüşmez (Demirel ve Durna, 2008:139). Bilgi ise verilerin, çeşitli dönüştürme süreçlerinden geçirilerek bir kişi ya da kurum için anlamlı hale gelmesiyle elde edilir (Akolaş, 2004:30). Bilgi, kullanıcısı için anlamlı olduğu sürece bu niteliğini taşırken; başka kullanıcılar için anlam ifade etmediği sürece veri olarak kabul edilecektir.

Bilişim, bilginin teknoloji yardımıyla düzenli ve akılcı bir biçimde üretilmesi olarak tanımlanabilir (TBD, 2010). Verinin bilgiye dönüşmesi sürecinde rol alan bilişim, bu bilginin elde edilmesi, yeniden kullanılması, dönüştürülmesi, iletilmesi ve yok edilmesi süreçlerinde farklı formlarda yer alır. Diğer yandan, bilişim teknolojileri

1 Ayrıntılı bilgi için bkz. http://www.cobitonline4.info/Pages/Public/Home.aspx (Erişim Tarihi: 29.01.2013); ve Guideline for Audit of IT Environment, ECA (2011), Lüksemburg.

ve bilişim sistemleri kavramları birbirlerinin yerine geçecek şekilde kullanılsalar da farklı anlamlar içermektedir. Şöyle ki bilişim teknolojileri, veri ya da bilgileri iletir, işler ve depolar. Sistem olgusu ise manuel veya sayısal ortamda, önceden belirlenmiş bir veya birden fazla amaca yönelik olarak, girdileri alıp belirli kurallar çerçevesinde çıktılara çevirmeyi ifade eder ve bu açıdan değerlendirildiğinde bilişim sistemleri terimi, bireysel ya da kurumsal hedeflere ulaşmak amacıyla hazırlanmış ve birlikte çalışan entegre yazılımlar tarafından yönetilen bilişim teknolojileri olarak ifade edilebilir (Watson, 2007:8).

2. BİLİŞİM TEKNOLOJİLERİ DÖNÜŞÜMÜ VE DENETİME YANSIMALARI

Bilişim teknolojileri (BT) devrimi olarak da adlandırılan dönüşüm süreci, İkinci Dünya Savaşı sonrasında teknolojideki ilerlemeler ile hız kazanmıştır. 1983 yılında, bilgisayarın Time Dergisi tarafından "yılın adamı" olarak seçilmesi (Time, 2012) ise yaşanan sürecin insanlık tarihinde bıraktığı ve bırakacağı izlerin boyutlarını gözler önüne sermiştir. Bilgisayarlar, 90'lı yıllar ile birlikte kurumsal iş süreçlerinin yürütülmesinde kullanılmaya başlanmıştır (Hinnsen, 2009:10) ve Amerika Birleşik Devletleri başta olmak üzere birçok ülkede teknolojinin, ekonomik büyümenin temel unsuru haline gelmesi de aynı döneme rastlamıştır (ITIF, 2007). Bu gelişmelere paralel olarak, üçüncü dünya ülkelerinde politik ve ekonomik geri kalmışlığa, teknoloji kullanımı üzerinden açıklamalar getirilmiştir.

BT kullanımındaki temel saik, bilgisayarlar yardımı ile iş ve işlemlerin otomasyonunun sağlanarak, maliyetlerin azaltılması ve üretkenliğin artırılması olmuştur (Menkus ve Galleos, 2001:01). Kurumsal faaliyetlerini daha etkin bir biçimde yürütmek isteyen organizasyonlar, öncelikli olarak muhasebe birimlerinde bilişim sistemleri kullanmıştır. Günümüz dünyasının gelişmiş toplumlarındaki özel ya da kamu kuruluşlarının tümünde, iş süreçlerinin büyük çoğunluğu bilişim ortamında yürütülmekte ve bilginin doğuşundan yok edilmesine kadar olan yaşam döngüsü bilişim sistemleri vasıtasıyla gerçekleştirilmektedir. Teknolojideki ilerleme hızının her yıl katlanarak artması ise organizasyonları, eski bilişim teknolojilerini bir kenara bırakarak, bilgi, zekâ, entegrasyon ve inovasyon odaklı çözümler üretmeye zorlamaktadır (Hinnsen, 2010:17-21).

Karar vericiler, muhtelif kaynaklardan sağladıkları çıktıları (bilgi ve raporlar) kullanarak çeşitli değerlendirmeler yapar ve kurum kaynaklarının nasıl kullanılacağına ilişkin kararlar alırlar (Sayıştay, 2007:6). Bu noktada, stratejik kararların sağlıklı olarak alınabilmesi için, iş süreçlerini ideal düzeyde destekleyen bilişim sistemlerinin yanı sıra karar verme süreçlerine doğru, tutarlı ve uygun bilgiyi zamanında sunabilen yönetim bilgi sistemlerine ihtiyaç duyulmaktadır. Organizasyonların rekabetçi

olabilmeleri için kritik başarı faktörü olarak düşünülen yönetim bilgi sistemlerine ilişkin hizmetlerin çerçevesi ile bu hizmetlerle ilgili görev ve sorumluluklar, birçok ülkede yasal düzenlemelerle belirlenmektedir[2].

Diğer taraftan, BT kullanımı, yeni yolsuzluk metotları, hak ihlalleri, usulsüzlükler, suç tanımları ile birlikte yeni kontrol gereksinimleri ortaya çıkarmıştır. Gelişmiş ülkelerde, kişisel verilerin korunması, kurumsal veri güvenliği, e-ticaret, telif hakları, BT kontrol ortamı, bilişim suçları, internet erişimi gibi konularda çeşitli yaptırım düzeylerine sahip yasal düzenlemeler hayata geçirilmiştir. Ayrıca, iyi uygulama örneklerinden yola çıkılarak uluslararası ve ulusal standartlar geliştirilmiştir. Bu gelişmelere paralel olarak, mevzuattan kaynaklanan yasal yükümlülüklere ve standartlara uyum, yapılan denetimin türü ve kapsamına göre denetçiler tarafından dikkate alınmaya başlanmıştır.

Ayrıca, teknolojik dönüşüm süreci, risk algısının da BT risklerini içerecek şekilde değişmesine yol açmıştır. Çünkü bireysel hataların sistematikleşmesi, işlemi gerçekleştiren kişinin tespit edilememesi, yetkisiz kişilerin verileri değiştirmesi, veri kaybı ve gizli veya kişisel bilgilerin ifşa edilmesi gibi BT kaynaklı risklerin (ECA, 2011:3) değerlendirilmesi ve denetim sonuçlarına olası etkilerinin doğru analiz edilmesi gerekliliği ortaya çıkmıştır. Bu nedenle, iş süreçlerinin BT ortamında yürütülmesi, denetim kanıtını ve denetim izini değiştirerek, yeni denetim prosedürlerinin oluşmasına neden olmuştur (INTOSAI, 1996:5).

Teknolojik dönüşümün denetim üzerindeki yansımaları, 1950'den itibaren üç ayrı kavramı ortaya çıkarmıştır: bilgisayar çevresinde denetim, bilgisayarlı denetim ve bilgisayarın içinde denetim. Bilgisayar çevresinde denetim, denetçilerin bilgisayara girilen kaynak veriler ve çıktısı alınan dokümanlar ile ilgilenerek denetim izini aradığı ancak bilgisayarın kendisiyle ilgilenmediği ilk dönemlerdir. Daha sonraları ortaya çıkan bilgisayarlı denetim, bilişim sistemleri kullanımının artmasıyla birlikte, denetçilerin veriler üzerinde genel denetim yazılımları ve diğer programları kullanarak analiz yaptıkları ve istatistiki yöntemleri uyguladıkları dönemdir. Son aşamada ise otomasyon düzeyinin artması ve büyük bilişim sistemlerinin yaygın olarak kullanılması, bilgisayar içinde denetim kavramını ön plana çıkarmış ve denetçiler, sistemleri üzerindeki genel kontroller ve uygulama kontrolleri ile ilgilenerek günümüzdeki anlamıyla BT denetimini icra etmeye başlamıştır (Yıldız, 2007:176).

3. BİLİŞİM TEKNOLOJİLERİ DENETİMİ

Bilişim teknolojileri (BT) denetimi**,** farklı şekillerde adlandırılmış ve denetimi yapan kurumun özelliğine göre de değişik anlamlar içerecek şekilde tanımlanmıştır.

2 Ülkemizde 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ve söz konusu Kanun'un ikincil mevzuatlarından olan Strateji Geliştirme Birimlerinin Çalışma Usul ve Esasları Hakkında Yönetmelik bu konudaki düzenlemelerdir.

2000'li yıllara kadar bilişim teknolojilerinin amacı elektronik veri işlemeyken, daha sonra bilgiyi yönetmek olgusu ön plana çıkmış (Schroeder, 2009:1) ve bu nedenle elektronik veri işleme denetimi terimi de yerini bilişim sistemleri denetimi ya da BT denetimi kavramlarına bırakmıştır (ASOSAI, 2001:1).

Weber'e göre BT denetimi, bilgisayar sistemlerinin bilgi varlıklarını koruması, veri bütünlüğünü sağlaması ve bir organizasyonun hedeflerine verimli ve etkin bir şekilde ulaşmasına yardım etmesi gibi hususlara ilişkin yapılan bir incelemedir (Sayana, 2002:1). Diğer bir ifadeyle, önceden belirlenmiş denetim hedefleri doğrultusunda, bilişim ortamında kanıt toplama ve değerlendirme sürecidir (INTOSAI, 2007a:1). 16 Mayıs 2006 tarih ve 26170 sayılı Resmi Gazete'de yayımlanan 'Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik'in 4 üncü maddesinde bilgi sistemleri denetimi, denetlenenlerin faaliyetlerini gerçekleştirmekte kullandıkları yazılım ve donanım gibi tüm bilgi sistemi unsurlarının, bilgi sistemi süreçlerinin, finansal veri üretiminde kullanılan bilgi sistemi ve süreçlerinin ve bunlarla ilgili olarak tesis edilen iç kontrollerin nitelik, işleyiş, yeterlilik, bütünlük, güvenlik ve güvenilirliklerinin değerlendirilmesi ve rapora bağlanması olarak tanımlanmaktadır.

Literatürde bağımsız bir denetim türü olarak kabul edilen ve risk odaklı bir yaklaşıma sahip olan BT denetimi, uluslararası BT denetim standartları ve rehberleri ile belirlenmiş olan metodoloji çerçevesinde planlanma, uygulama ve raporlama aşamalarından oluşur. Diğer denetim türlerinden bağımsız bir şekilde icra edilebileceği gibi mali denetim, uygunluk denetimi ve performans denetiminin parçası olarak da yürütülebilir.

Mali denetim ile birlikte yürütülen BT denetimi kapsamında; denetçilerin görüş verdiği mali tablolar bilişim sistemlerinin ürettiği verilerle oluşturuluyor ise denetlenen kurumda BT kullanımının, mali tablolara ve mali süreçlere yaptığı etki ile ortaya çıkardığı riskler incelenir. Bu tür bir denetimde, mali verilerin BT kullanılarak işlenmesi, saklanması ve iletilmesinin, iç kontrol sistemlerine olan etkisi ile yapısal risklere veya kontrol risklerine ilişkin denetçi kanaatine ne ölçüde tesir ettiği değerlendirilir. Sonuç olarak ise mali bilgiler üzerinde doğrudan ve önemli etkiye sahip bilişim sistemlerine ait BT kontrolleri hakkında bir görüş oluşturulur (ASOSAI, 2003:4).

Performans denetimi ile birlikte yürütülen BT denetimi kapsamında; denetim konusu iş süreçlerinin bilişim sistemleri ile yürütülen kısımları belirlenir ve BT'nin bu iş süreçlerini verimli ve etkin bir şekilde destekleyip desteklemediği hususu değerlendirilir (ASOSAI, 2003:4).

Uygunluk denetimi ile birlikte yürütülen BT denetimi kapsamında; iş süreçlerine ilişkin mevzuatın öngördüğü hususlar bilişim sistemleri uygulamaları vasıtasıyla hayata geçiriliyor ise bunların öngörüldüğü biçimde uygulanıp uygulanmadığı ve gerekli iç kontrol mekanizmalarının oluşturulup oluşturulmadığı tespit edilir.

3.1. BT Denetimi Metodolojisi

BT denetimi, kendine özgü denetim adımları çerçevesinde planlanır, yürütülür ve sonuçlandırılır. Ancak, denetim yetkisi, sektörel farklılıklar ve denetim ihtiyaçlarının kapsamı gibi çeşitli nedenlerle BT denetim metodolojileri farklılaşabilmektedir. Birleşik Krallık, Türkiye, Amerika Birleşik Devletleri ve Hindistan gibi ülke Sayıştayları ile Avrupa Birliği Sayıştayı tarafından yayımlanan rehberlerin öngördüğü BT denetim metodolojilerinin benzer yaklaşımlarını şu şekilde özetlemek mümkündür:

1. BT denetiminin planlaması
    a. Denetim hedeflerinin ve kapsamın belirlenmesi,
    b. Denetlenen kurumun ve kritik iş süreçlerinin anlaşılması,
    c. Denetlenen kurumun BT altyapısı hakkında genel bilgi edinilmesi,
    d. BT denetimi için önemli olabilecek alanların ve konuların belirlenmesi,
    e. Sistem risklerinin tespit edilmesi,
    f. Kritik kontrol noktalarının belirlenmesi,
    g. Denetimin planlamasına ilişkin diğer prosedürlerin uygulanması,
        i. İlgili yasal düzenlemelerin incelenmesi,
        ii. Sahtecilik risklerinin değerlendirilmesi,
        iii. Önceki denetim sonuçlarının gözden geçirilmesi,
        iv. Denetim kaynaklarının planlaması,
        v. Denetlenen kurum ile denetimin icra edilmesine ilişkin konularda iletişim,
        vi. Uzman çalıştırma gerekliliği konusunda değerlendirme yapılması,
        vii. Denetim planının oluşturulması,
2. Denetim testlerinin uygulanması,
    a. Denetim hedefleriyle ilgili bilişim sistemlerinin anlaşılması,
    b. Uygulanacak kontrol teknikleri hakkında karar verilmesi,
    c. Kontrollerin doğru tasarlanıp tasarlanmadığının incelenmesi,
    d. Kontrollerin etkin bir şekilde işleyip işlemediğinin incelenmesi,
    e. Kontrol zayıflıklarının tespit edilmesi,
    f. Telafi edici kontrollerin değerlendirilmesi,
3. Raporlama

Tespit edilen kontrol zayıflıklarının etkilerinin değerlendirilmesi (mali tablolara, performans denetimi konusu bilgilere vb. olan etki) (GAO, 2009:14-15).

BT denetçisi, denetimin raporlama aşamasında denetlenen kurumdaki BT kontrollerine ilişkin bir denetim görüşü oluşturur ve denetim bulguları ile ilgili kanıtlara, bu görüşe destek verecek şekilde BT denetim raporunda yer verir. Denetim görüşü üç ayrı şekilde belirlenebilir (ECA, 2011:13):

1. Denetimin yapıldığı dönemde BT kontrolleri, etkinlik ve süreklilik arz edecek bir şekilde işlemektedir ve BT kontrol ortamı genel olarak güvenilirdir.

2. Denetimin yapıldığı dönemde BT kontrollerinin etkinliğine ve sürekliliğine ilişkin zayıflıklar mevcuttur ancak BT kontrol ortamı genel olarak güvenilirdir.

3. BT kontrol ortamı güvenilir değildir. Denetimin yapıldığı dönemde BT kontrolleri, etkinlik ve süreklilik arz edecek şekilde kurgulanmamıştır ve/veya işlememektedir.

3.2. BT Kontrolleri ve BT Denetimi Açısından Tasnifi

BT kontrolleri, bir kurumun BT ortamındaki donanım, yazılım, insan kaynağı ve fiziki mekân gibi unsurlara ilişkin olarak, belirli bilgi kriterleri çerçevesinde ve farklı detaylarda tesis edilmiş kontrollerdir.

BT kontrolleri fonksiyonlarına göre, önleyici, tespit edici ve düzeltici kontroller olarak üç kategoriye ayrılır. Önleyici kontroller, bir riskin gerçekleşmesini engelleyen ve diğer kontrollere göre daha önemli kabul edilen kontrollerdir (Champlain, 2003:413). Saldırı engelleme sistemleri, güvenlik duvarları, alfabetik karakterlerin sayısal alanlara girilmesini engelleyen basit veri giriş kuralları, muhasebe uygulamasında bir hesabın negatif bakiye vermesinin engellenmesi, şifreleme ve giriş çıkışlarda güvenlik görevlilerinin çalıştırılması gibi kontroller önleyici kontrollere örnek olarak verilebilir. Öte yandan tespit edici kontroller, bir hata, iptal ya da zararlı bir hareketin ortaya çıkarılması ve raporlanması ile ilgilidir (Hindistan Sayıştayı, 2006:19). Saldırı tespit sistemleri, saldırıların tespit edilmesi için kurulmuş tuzak uygulama olan bal çanağı veya bal küpü, farklı kaynaklardan alınan verilerin karşılaştırılması, ağ tarayıcıları, kayıtların tutulması ve incelenmesi, fiziki sayım ve alarm sistemleri tespit edici kontrollerdendir. Düzeltici kontroller ise ortaya çıkarılan bir hata, iptal, müdahale veya yetkisiz kullanımın düzeltilmesine hizmet eden BT kontrolleridir (ISACA, 2012b:9). Yedeklenen veriler kullanılarak iş sürekliliğinin sağlanması, felaket kurtarma planları, elektrik akım regülatörü kullanımı ve sigorta yaptırılması düzeltici kontroller arasında yer alır.

BT kontrolleri uygulama şekillerine göre ise yönetimsel, operasyonel ve teknik kontroller olarak üç kısımdır. Yönetimsel kontroller, doğrudan üst yönetimi ilgilendiren ve politika ve prosedür seviyesinde olan kontrollerdir. Operasyonel kontroller, sorumlu çalışanların var olan politika ve prosedürleri uygulamasını; teknik kontroller ise söz konusu çerçevenin kişiler yerine bilişim sistemleri tarafından otomatik olarak yürütülmesini ifade eder (Gutman ve Roback, 1995:4). Diğer bir ifadeyle, logların sistem yöneticileri tarafından manuel olarak gözden geçirilmesi operasyonel bir kontrol iken, bu işin otomatik kayıt analiz aracı tarafından yapılması teknik bir kontroldür.

BT denetimi açısından değerlendirilecek olursa, BT kontrolleri, genel kontroller ve uygulama kontrolleri olarak iki grupta incelenmektedir.

Genel kontroller, BT ortamındaki tüm unsurlara ilişkin politika ve prosedürlerle ilgili genel amaçlı kontrollerdir (INTOSAI, 2007b:431). Diğer bir ifadeyle, uygulama programlarının geliştirildiği ve işletildiği bilişim ortamını ilgilendiren politika, prosedür ve uygulamaları kapsar ve bilişim sistemlerine, BT altyapısına ve uygulama programlarına yönelik risklerin minimize edilmesini sağlar (ECA, 2011:9). Genel kontrolleri şu şekilde kategorize etmek mümkündür (Hindistan Sayıştayı, 2006:42):

1. BT yönetimi kontrolleri,
2. Fiziki ve çevresel güvenlik kontrolleri,
3. BT işletim kontrolleri,
4. Mantıksal erişim kontrolleri,
5. Uygulama satın alınması ve değişim kontrolleri,
6. İş sürekliliği ve felaket kurtarma kontrolleri,

Genel kontrollerdeki zayıflıkların neden olabileceği riskler şu şekilde özetlenebilir (Sayıştay, 2008:92-100):

- Kurumun karşı karşıya kalacağı tehlikelerin belirlenememesi, etkilerinin ölçülememesi ve riskin yönetilememesi,
- Sorumluluklarda karmaşa, aşırı yetki verme veya açıkların oluşması,
- Uygun olmayan görev ayrımlarının yapılması,
- Yetersiz personel istihdamı,
- İşten ayrılan veya işine son verilen personelin sisteme yetkisiz erişebilmesi,
- Sistemi kötü amaçlarla kullanan personelin tespit edilememesi,
- Maddi zararların meydana gelmesi,
- Bilgisayar donanımının veya üzerinde yazılım ve bilgi bulunduran parçaların çalınması veya bozulması,
- Kritik veya gizli bilginin görülmesi, kopyalanması veya kaybedilmesi,
- Yetersiz şifre uygulamalarının, sisteme ve uygulama programlarına yetkisiz erişimi kolaylaştırması,
- Kullanıcıların kim olduklarının ve erişim seviyelerinin belirlenememesi, ayrıcalıklı kullanıcıların izlenememesi, yetki ve sorumlulukların işin gereğine uygun tespit edilememesi (yetersiz veya aşırı yetkilendirme),
- Veri kaybı, verilerin değiştirilmesi veya bozulması,
- Fikri mülkiyet haklarının ihlali ve bilişim suçları gibi yürürlükteki yasal mevzuata aykırılıkların gözden kaçırılması,
- Bir felaket durumunda iletişim imkânları, bilgi işleme kapasitesi, eğitimli insan kaynağı ve tüm varlıklar yitirilebileceğinden kurumun faaliyetlerini sürdürmesinde devamlılığın sağlanamaması.

Uygulama kontrolleri, uygulama programları düzeyinde tesis edilen manuel ya da otomatik kontrollerdir ve uygulamaların içerisine gömülüdür (ISACA, 2009:25). Bu kontrollerin amacı, bilginin uygulama programına tam olarak, zamanında ve sadece bir kere girilmesi; bilgi-işlem ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleştirilmesi ve raporların tam ve güvenilir olarak üretilmesi, yetkili kişilere ulaştırılması ve uygun şekilde saklanmasıdır (Sayıştay, 2008:100).

Manuel uygulama kontrolleri, işlemin bilişim ortamında her bir tekrarı sırasında kullanıcı tarafından uygulanır ve bu nedenle hatalara veya kötü niyetli değişikliklere daha fazla açıktır. Diğer yandan, otomatik uygulama kontrolleri, program içinde bir defa tanımlanır ve o kontrole ilişkin tüm işlemlerde sistem tarafından otomatik olarak uygulanır. Bu sebeple, kullanıcıların verileri manipüle etme riski ya da hata ve kötü niyetle yanlış işlem yapma olasılığı ortadan kalkacaktır. Ancak, otomatik uygulama kontrolleri programa hatalı olarak tanımlanırsa sistematik hatalar ortaya çıkacaktır (ECA, 2011:12). BT ortamında doğru tasarlanmış otomatik uygulama kontrolleri, sistemde üretilen verilerin güvenilirliğini artıracaktır.

Uygulama kontrolleri; girdi kontrolleri, veri transfer kontrolleri, işlem kontrolleri ve çıktı kontrolleri başlıkları altında incelenebilir. Uygulama kontrollerinin doğru kurgulanmaması ya da etkin bir şekilde işletilememesi durumunda aşağıdaki riskler söz konusu olacaktır (Sayıştay, 2008:100):

- Yetkili olmayan kişilerce veri girişi yapılması,
- Eksik veya hatalı veri girilmesi,
- Sistematik hataların oluşması,
- Hatalı veri girişlerinin tespit edilememesi ve düzetilememesi,
- Mükerrer kayıtların sistem tarafından kabul edilmesi,
- Transfer edilen verinin bozulması, kaybolması, çalınması veya değiştirilmesi,
- Denetim izinin kaybolması ve işlem sahibine başvurulamaması,
- İşlemlerin doğrulanamaması,
- Çıktıların tam ve doğru olmaması,
- Çıktıların yetkisiz kişilerin eline geçmesi.

Genel kontroller ile uygulama kontrolleri birbirleriyle ilişkili kontrollerdir. Kurumdaki BT kontrollerinin etkinliği, genel kontrollerin iyi işlemesine bağlıdır. Genel kontrollerin etkin olmadığı bir BT ortamında, uygulama kontrolleri etkin olmayacak yahut bunların etkinliği olumsuz yönde ciddi oranda azalacaktır. Örneğin, fiziksel erişim kontrollerinin veya mantıksal erişim kontrollerinin tesis edilmediği ya da bu hususlarda ciddi kontrol zayıflıklarının olduğu bir BT ortamında, uygulama kontrollerinin etkinliğinden bahsetmek mümkün değildir (ECA, 2011:9).

3.3. BT Denetimi ve Standartlar

BT denetçisi, bilişim teknolojilerine ilişkin standartlara referans vererek denetimlerini icra edebildiği ölçüde, objektif ve kabul edilebilirliği yüksek bulgu ve öneriler içeren raporlar ortaya koyabilir. BT standartları, kurum yöneticilerine ve BT birimlerinde çalışanlara yol gösterirken; BT denetçilerinin, denetim hedefleriyle uyumlu denetim programları hazırlayabilmelerine yardımcı olur. Günümüzde bilişim teknolojileri kullanımına ilişkin genel standartlar olduğu gibi, bilgi güvenliği veya hizmet sunumu gibi sadece belli konulara odaklanan detay standartlar da mevcuttur. BT standartlarının, BT denetçileri tarafından en yaygın olarak kullanılanları şunlardır: COBIT, COBIT Denetim Güvence Rehberi, Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri, ISO/IEC 27000 Standart Serisi, ISO/IEC 15408, ISO/IEC 38500, NIST SP 800 Serisi, ITIL, TOGAF, PMBOK ve PRINCE2.

COBIT 5, ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği) tarafından 2012 yılında yayımlanmış Bilgi Teknolojileri Kontrol Hedefleri adlı standardın en güncel sürümüdür. BT alanında en geniş kapsamlı çerçeveyi sunan COBIT 5, beş farklı alandaki 37 BT sürecinin her birine ilişkin BT hedeflerini, göstergeleri, girdileri, çıktıları, atılması gereken adımları ve diğer standartlarla olan ilişkileri ortaya koyarken; kurum üst yönetiminden teknik alanda çalışan personele kadar herkes için görev ve sorumlulukları belirler. BT denetçisi ise COBIT 5'i kullanarak farklı amaçlara yönelik denetim programları oluşturabilecektir[3].

COBIT Denetim Güvence Rehberi, 2007 yılında ISACA tarafından yayımlanmıştır ve BT denetimi ile uğraşan profesyonellerin, denetimlerini etkin bir biçimde planlamasına ve uygulamasına yardım etmeyi amaçlar. COBIT çerçevesinde yer alan kontrol hedeflerinden yola çıkılarak hazırlanmış olan ve BT kaynaklı riskleri ve iyi uygulamaları da içeren rehber, 2013 yılında COBIT 5'in kapsamına göre güncellenecektir[4].

Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri, ISACA tarafından 2009 yılında yayımlanmıştır ve BT denetimi mesleğinde çalışanların uyması gereken ahlaki ilkeleri, kabul edilebilir bir BT denetiminin icra edilebilmesi için asgari düzeyde zorunlu standartları, BT denetimlerinde kullanılacak araçları ve iyi uygulama örneklerini içermektedir. ISACA, bu dokümana ilişkin olarak, güncelleme çalışmaları yürütmektedir[5].

ISO/IEC 27000 Standart Serisi (ISO27k), Uluslararası Standardizasyon Örgütü (ISO) ile Uluslararası Elektroteknik Komisyonu (IEC) tarafından birlikte hazırlanan

3 Ayrıntılı bilgi için bkz. http://www.isaca.org/COBIT/Pages/default.aspx, (Erişim Tarihi: 13.11.2012).

4 Ayrıntılı bilgi için bkz. http://www.isaca.org/Knowledge-Center/Research/Research/Deliverables/Pages/IT-Assurance-Guide-Using-COBIT.aspx, (Erişim Tarihi: 13.11.2012).

5 Ayrıntılı bilgi için bkz. http://www.isaca.org/Knowledge-Center/Standards/Documents/Standards-for-IS-Auditing-Turkish.pdf, (Erişim Tarihi: 13.11.2012).

ve bilgi güvenliğinin farklı boyutlarını ele alan standart ailesine verilen addır. Bu standartlar, bilgi güvenliği riskleri, kontrolleri ve yönetimine ilişkin iyi uygulama örnekleri ortaya koymaktadır. Farklı ayrıntı düzeylerine sahip bu standartlara ilişkin sertifikasyon imkânları da bulunmaktadır[6].

ISO/IEC 15408 (Ortak Kriterler), BT ürünlerinin ve bilişim sistemlerinin güvenlik seviyelerinin tespit edilmesi ve test edilebilmesi için geliştirilmiş olan ortak kriterlerin bütünüdür ve sertifikasyon imkânı sunar[7].

ISO/IEC 38500, Uluslararası Standardizasyon Örgütü (ISO) ile Uluslararası Elektroteknik Komisyonu (IEC) tarafından birlikte hazırlanan ve BT yönetişimini konu alan uluslararası standarttır. Kurumun yöneticilerine, diğer iç paydaşlar ve ayrıca BT denetçilerine, bilişim teknolojilerinin verimli, etkin ve kabul edilebilir düzeyde kullanımının nasıl olması gerektiği hususunda yol gösterir[8].

NIST SP 800 Serisi, Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü tarafından yayımlanmıştır ve bilgi güvenliğine ilişkin standart, politika, prosedür ve rehberleri içeren dokümanlardır[9].

ITILv3 (Bilişim Teknolojileri Altyapı Kütüphanesi), BT hizmet yönetiminin kurumsal ihtiyaçlara cevap verecek şekilde planlanması, yürütülmesi, ölçülmesine ilişkin standartları ve iyi uygulama örneklerini ortaya koyar. Dünyada ileri gelen birçok özel şirket ve kamu kurumunca kullanılan ITILv3, BT hizmetlerinin verimliliğini artırmak, maliyetleri düşürmek, üçüncü taraflardan hizmet alımından optimum düzeyde fayda elde etmek ve kullanıcıların beklentilerini daha iyi karşılamak gibi katkılar sağlamaktadır. BT denetçileri, hizmet sunum ve desteği ile BT yönetişimi konularında denetim programları hazırlarken ITILv3 çerçevesine başvurabilir[10].

TOGAFv9.1 (Açık Grup Mimari Çerçevesi), bilgi mimarisinin doğru tasarlanması ve uygulanması konularında organizasyonlara yardımcı olmaktadır. İş ihtiyaçlarının daha kolay tespiti, doğru teknolojilerin seçimi, hızlı entegrasyonun sağlanması ve ürün geliştirme süreçlerinin etkinliğinin artırılması konularında kullanıcılarına katkı sağlar. TOGAFv9.1, bilgi mimarisini, iş, uygulama, veri ve teknoloji ile bu bileşenlerin etkileşimi üzerine kurgulamakta ve bu alanda çalışan profesyonellere sertifikasyon imkânı sağlamaktadır[11].

6 Ayrıntılı bilgi için bkz. http://www.iso27001security.com/, (Erişim Tarihi: 13.11.2012).

7 Ayrıntılı bilgi için bkz. https://www.bilgiguvenligi.gov.tr/ortak_kriterler/index.php , (Erişim Tarihi: 13.11.2012).

8 Ayrıntılı bilgi için bkz. http://www.iso.org/iso/catalogue_detail?csnumber=51639, (Erişim Tarihi: 13.11.2012).

9 Ayrıntılı bilgi için bkz. http://csrc.nist.gov/publications/PubsSPs.html , (Erişim Tarihi: 13.11.2012).

10 Ayrıntılı bilgi için bkz. http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx , (Erişim Tarihi: 13.11.2012).

11 Ayrıntılı bilgi için bkz. http://www.togaf.info/, (Erişim Tarihi: 13.11.2012).

PMBOK ve PRINCE2 gibi proje yönetimi metodolojileri ise BT proje yönetimi konusunda yöneticilere, uygulayıcılara ve denetçilere yol göstericidir.

4. BİLGİ KRİTERLERİ ÇERÇEVESİNDE BT DENETİMİ

Bilişim ortamındaki iş süreçlerinde üretilen verinin bilgiye ve sonrasında bilgi birikimine dönüşerek, kuruma değer katması ve bu durumun döngüsel olarak tekrar edilmesi önemlidir (ISACA, 2012a:81). Bu nedenle, bilginin belirli kontrol kriterleriyle uyumlu olması, kurumların stratejik hedeflerine ulaşmalarına yardımcı olacaktır.. Güvenlik, mali yükümlülükler ve kalite çerçevesinde belirlenen yedi bilgi kriteri; etkililik, verimlilik, gizlilik, bütünlük, süreklilik, güvenilirlik ve mevzuata uyumdur (ISACA, 2007:10).

1. *Etkililik*; iş süreçlerinin ihtiyaçlarına cevap verecek nitelikteki bilginin, zamanında, düzenli ve uygun nitelikte üretilmesini,

2. *Verimlilik*; bilginin, kaynakların üretken ve ekonomik kullanımı ile elde edilmesini,

3. *Gizlilik*; hassas bilginin yetkisiz erişime karşı korunmasını,

4. *Bütünlük*; bilginin, tam, doğru ve kurumsal değerler ve beklentiler çerçevesinde geçerli olmasını,

5. *Süreklilik*; bilginin, şimdi veya gelecekte ihtiyaç duyulduğu zaman mevcut ve erişilebilir olması ile bunu sağlayacak araç ve kaynakların korunmasını,

6. *Uygunluk*; kurumun tabi olduğu yasal düzenlemelere ve sözleşmelere uyumun sağlanmasını,

7. *Güvenilirlik*; bilginin, yöneticilerin kurumsal yönetişim görevlerini ifa edebilmeleri için uygun ve güvenilir olmasını ifade etmektedir (ISACA, 2007:10-11).

Bilgi kriterleri, yöneticileri ilgilendirdiği kadar, BT denetçisinin, denetimini nasıl şekillendireceği noktasında da belirleyicidir. BT kriterlerinden yola çıkılarak icra edilecek bir BT denetimi süreci şu şekildedir:

1. Denetim hedefleri doğrultusunda değerlendirilecek bilgi kriterlerinin belirlenmesi,

2. Kurumun BT ortamının ve bilişim sistemlerinin tanınması ve BT risklerinin belirlenmesi,

3. Bilgi kriterleriyle birincil düzeyde ilgili olan BT kontrollerinin tespiti ve denetim programının hazırlanması,

4. Kontrollerin varlığının ve etkinliğinin, kontrol testleri ve maddi doğrulama testleri uygulanarak incelenmesi,

5. Bilgi kriterleri çerçevesinde bulguların raporlanması ve BT kontrollerine ilişkin denetim görüşünün oluşturulması.

Örneğin, BT projelerine ilişkin sistem geliştirme yaşam döngüsü süreçlerinin denetim konusu olarak seçilmesi durumunda, verimlilik ve etkinlik kriterleri birincil düzeyde dikkate alınacaktır. Dolayısıyla, BT proje yönetimi, kalite yönetimi, otomasyon çözümlerinin tanımlanması, uygulama yazılımının ve/veya teknoloji altyapısının satın alınması, yasal yükümlülüklerin yerine getirilmesi, politika ve diğer düzenlemelerin hazırlanması, sistemin kurulması ve akredite edilmesi, değişimlerin yönetilmesi, sistem güvenliği ile sürekliliğinin sağlanması ve kullanıcıların eğitilmesi gibi süreçlere ilişkin kontroller değerlendirilecektir (ISACA, 2009:105-106).

Hem bağımsız BT denetimleri hem de diğer denetim türleriyle birlikte yürütülen BT denetimleri açısından önem arz eden BT alanları, süreçleri ve kontrolleri bulunmaktadır. Verilerin denetim sonuçlarına sağlıklı katkı vermesini sağlayacak düzeyde güvenilir olması, bilgi güvenliğinin kabul edilebilir riskler seviyesinde yönetilmesi ve giderek artan BT kullanımı karşısında etkin yönetişim mekanizmalarının kurulması konularında, ülkelerin mali mevzuatlarında, iç kontrol standartlarında, bilişime ilişkin diğer düzenlemelerde ve uluslararası standartlarda ayrıntılı hükümler ve kontrol gereksinimleri belirlenmiştir. Söz konusu üç alana ilişkin BT denetim programlarının, bilgi kriterlerinden yola çıkılarak hazırlanması mümkündür. Bu çerçevede;

- Güvenilirlik ve bütünlük kriterleri çerçevesinde veri bütünlüğü ve güvenilirliği,
- Verimlilik, etkinlik, güvenilirlik ve uygunluk kriterleri çerçevesinde BT yönetişimi,
- Gizlilik, bütünlük ve süreklilik kriterleri çerçevesinde bilgi güvenliği alanları incelenebilir.

4.1. Veri Bütünlüğü ve Güvenilirliği Sorunu

Gerek BT denetimi gerekse diğer denetim türlerinde, denetçinin, denetim görüşünü oluşturmak ve bulgularını desteklemek amacıyla ortaya koyduğu kanıtlara esas teşkil eden her türlü bilginin veya verinin bütünlüğü (tamlık ve doğruluk) ve güvenilirliği, yapılan denetimin kabul edilebilirliği noktasında olmazsa olmaz bir önkoşuldur. 'Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Tekniklerine' göre; BT denetçisi, veri analizi yöntemi ile bilgi veya kanıt elde etmek amacıyla bilgisayar destekli denetim tekniklerini kullanırsa, bu bilgilerin üretildiği bilişim sistemi ve ortamının bütünlüğü hakkında güvence almakla yükümlüdür (ISACA, 2009: 33). Aksi takdirde, denetlenen kurumun bilişim sistemlerine yetkisiz erişim, hatalı veri girişleri veya kasıtlı olarak mevcut verilerin bozulması gibi tehditler nedeniyle verinin güvenilirliğine ilişkin sorunların var olup olmadığı tespit edilemeyecektir ve dolayısıyla denetçinin mali analiz ya da farklı istatistiki yöntemlerle elde edeceği kanıtların geçerliliği de olumsuz etkilenecektir.

Denetlenen birimden alınan verinin sistemdeki canlı veri ile aynı olmaması durumunda veri bütünlüğü sorunları ortaya çıkacaktır. Verilerin güvenilirlik açısından kalite düzeyi, denetim hedeflerinin gerçekleştirilmesini doğrudan etkileyecektir. Verilerin tamlığı konusunda güvence, diğer kaynaklardan gelen veriler ile karşılaştırmak suretiyle veya genel kontroller ve uygulama kontrolleri test edilerek sağlanabilir (ECA, 2011:4). Buna karşılık, verilerin güvenilirliği ve doğruluğu konusunda güvence elde etmek için, BT kontrollerinin varlığının ve etkinliğinin mutlaka sorgulanması gerekmektedir. Unutulmaması gereken nokta, veri analizi için kullanılacak verinin sistemdeki veri ile aynı olmasının, o verinin doğru veri olduğu anlamına gelemeyeceğidir. Diğer bir deyişle, bilgilerin manuel ortamdan bilişim ortamına aktarımı sürecinde hata yapılması, yetkisiz erişim nedeniyle bir kısım verilerin sistemde değiştirilmesi, silinmesi veya sistemin iş akışlarına uygun olarak bilgi üretememesi gibi sebeplerle güvenilir olmayan veriler üzerinde analiz yapmak, denetçiyi yanlış sonuçlara götürecektir.

Uluslararası Yüksek Denetim Kurumları Standartlarının (ISSAI), üçüncü düzey denetim standartlarında (Temel Denetim İlkeleri), düzenlilik denetimleri ve performans denetimlerinin uygulanması esnasında karşılaşılan bilişim teknolojileri unsurlarının, denetçi tarafından dikkate alınması gerektiği ifade edilmektedir. ISSAI 300'e göre, bilgisayar temelli sistem verilerinin, denetimin önemli bir parçasını oluşturması ve veri güvenilirliğinin denetim hedefini gerçekleştirmede hayati bir rol oynaması halinde, denetçilerin, verilerin güvenilir ve güncel olduğu konusunda tatmin olmaları gerekmektedir. Daha farklı bir ifadeyle, muhasebe ve diğer bilgi sistemlerinin bilgisayarla yürütüldüğü ortamlarda denetçi, denetlenen kurumdaki iç kontrollerin; verilerin doğruluk, tamlık ve güvenilirliğini sağlayacak şekilde tasarlanıp tasarlanmadığı konusunu incelemelidir (INTOSAI, 2001).

Diğer yandan, Uluslararası İç Denetim Standartlarına göre (2120.A1); iç denetim faaliyeti sürecinde, kurumun yönetişim süreçlerinin, faaliyetlerinin ve bilgi sistemlerinin maruz kaldığı risklerin değerlendirilmesi zorunludur ve bunu yaparken mali ve operasyonel bilgilerin güvenilirliği ve doğruluğu konusu mutlaka dikkate alınmalıdır (IIA, 2009:14).

Ülkemizde, kamu kurum ve kuruluşları, yaşam döngüsünü BT ortamında gerçekleştiren bilgi ve verilerin güvenilirliğinin ve bütünlüğünün sağlanmasından sorumludurlar. 5018 sayılı Kanun'un 55 inci maddesinde iç kontrol, "idarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, *muhasebe kayıtlarının doğru ve tam olarak tutulmasını*, malî bilgi ve yönetim bilgisinin zamanında ve *güvenilir olarak üretilmesini* sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünü" olarak tanımlanmıştır.

5018 sayılı Kanun'un 55 inci maddesi uyarınca hazırlanan İç Kontrol ve Ön Mali Kontrole İlişkin Usul ve Esaslar'ın 5 inci maddesine dayanarak Kamu İç Kontrol Standartları Tebliği çıkarılmıştır. İdareler, malî ve malî olmayan tüm işlemlerinde bu standartlara uymakla ve gereğini yerine getirmekle sorumlu tutulmuşlardır. Tebliğin 12 no'lu standardında; "idareler bilgi sistemlerinin *sürekliliğini* ve *güvenilirliğini* sağlamak için gerekli kontrol mekanizmaları geliştirmelidir" denilmiş ve bunun gerçekleştirilmesi için güvenilirliğe ilişkin aşağıdaki şartlar belirtilmiştir:

1. Bilgi sistemlerinin sürekliliğini ve güvenilirliğini sağlayacak kontroller yazılı olarak belirlenmeli ve uygulanmalıdır.

2. Bilgi sistemine veri ve bilgi girişi ile bunlara erişim konusunda yetkilendirmeler yapılmalı, hata ve usulsüzlüklerin önlenmesi, tespit edilmesi ve düzeltilmesini sağlayacak mekanizmalar oluşturulmalıdır.

Tebliğin 13 no'lu bilgi ve iletişime ilişkin standardında ise bilgilerin doğru, güvenilir, tam, kullanışlı ve anlaşılabilir olması gerektiği ifade edilmektedir.

Veri güvenilirliği ve bütünlüğünü teyit etmek amacıyla bazı genel kontrollerin ve uygulama kontrollerinin incelenmesi ve bu amaca yönelik denetim prosedürlerinin uygulanması gerekir. Söz konusu amaca yönelik bir BT denetimi için, ilgili bilgi kriterlerinden hareketle hazırlanacak bir denetim programı şu kontrolleri içerebilir:

Genel kontroller verinin tutulduğu bilişim ortamını ilgilendiren yönüyle şu süreçleri kapsar (ECA, 2011:9-10):

- Veri yönetim kontrolleri,
- İş sürekliliği kontrolleri,
- Bilgi güvenliği kontrolleri,
- Değişim yönetimi kontrolleri,
- Hizmet satın alınmasına ilişkin kontroller.

Uygulama kontrolleri temel olarak şu hususları kapsar (Sayıştay, 2008:113):

- Tüm veri hazırlama ve veri giriş işlemleriyle ana dosyalardaki değişikliklerin yetki dahilinde yapılması (girdi kontrolleri),
- Hatalı veri girişlerini engelleyecek otomatik kontrol mekanizmalarının oluşturulması (girdi kontrolleri),
- Verinin, uygulama programı içerisinde, iş sürecinin gerektirdiği işleme tam ve doğru olarak tabi tutulması (veri işleme kontrolleri),
- Bilgisayar işlemlerinin, doğru zamanda ve doğru bir silsile ile işletilmesi (veri işleme kontrolleri),

- Sistemler arasında yapılan veri transferlerinin tam ve doğru olarak yapılmasını sağlayacak manuel veya otomatik kontrollerin tesis edilmesi (veri transferi kontrolleri),
- Çıktıların, tam, doğru ve zamanında üretilmesi; doğru yere/kişilere dağıtılması ve gizliliklerinin korunması (çıktı kontrolleri),
- İlgili personel tarafından çıktı raporlarının doğruluğunun gözden geçirilmesi ve hataların düzeltilmesi (çıktı kontrolleri).

4.2. BT Yönetişimi Sorunu

Bilişim dünyasındaki baş döndürücü gelişmeler, bilgi ve iletişim teknolojileri yatırımlarının hem kamuda hem de özel sektörde ciddi oranlarda artmasına neden olmuştur. Bu yatırımların kurumsal hedeflere ulaşma açısından verimliliği ve etkinliği, yöneticiler için hayati olduğu kadar, BT denetçileri açısından da önemli bir inceleme konusudur.

75'den fazla ülkede, 21 ayrı sektörde faaliyet gösteren 2252 kamu kuruluşu ve özel şirketten alınan BT yatırımları ve insan kaynağı verileri esas alınarak Gartner tarafından yapılan bir araştırmaya göre, personel başına yapılan BT harcaması rakamları 2010 yılı itibariyle ortalama 12.000 $ civarındadır. Personel başına düşen BT harcaması miktarı, özellikle, çok hassas verilerin yönetildiği sigortacılık, bankacılık, mali hizmetler ve kamu sektöründe dikkat çekmektedir (Gartner, 2011:27). Gartner tarafından periyodik olarak yapılan diğer bir araştırmaya göre dünya genelinde BT yatırımları 2012 yılı tahminleri şu şekildedir:

Tablo 1: 2012 Yılsonu İtibariyle Dünyada BT Yatırımlarına İlişkin Tahminler

Yatırım kalemi	2012 Yatırım (milyar dolar)	2012 Artış (%)
Donanım	420	3.4
Kurumsal yazılım	281	4.3
BT hizmetleri	864	2.3
Telekom araçları	377	10.8
Telekom hizmetleri	1,686	1.4
Toplam	**3,628**	**3.0**

Kaynak: Gartner, 2012.

Ülkemizde ise BT yatırımlarına ilişkin Türkiye İstatistik Kurumu verileri şu şekildedir:

Tablo 2: 2012 Yılı Türkiye Kamu Bilgi ve İletişim Teknolojileri Yatırımları Özet Tablosu

Sektör	Proje Sayısı	Proje Tutarı (Bin TL)	2012 Yılı Yatırımı (Bin TL)
Tarım	16	246,559	63,458
Madencilik	9	28,265	26,566
İmalat	6	16,007	15,007
Enerji	15	191,459	61,4
Ulaştırma ve Haberleşme	24	932,425	139,496
Turizm	1	882	882
Eğitim	20	2.406.167	1.152.521
Sağlık	2	164,841	43,288
Diğer Kamu Hizmetleri	119	2.940.619	981,71
Genel Toplam	**212**	**6.927.224**	**2.484.328**

Kaynak: Kalkınma Bakanlığı, 2012:5.

BT yatırımlarının gerek ülkemizde gerekse dünyada ulaşmış olduğu boyutlar, yukarıdaki istatistiklerde gözler önüne serilmiştir. BT sektörünün kurumsal iş süreçlerinin yürütülmesi, izlenmesi ve stratejik kararların alınması noktasında oynamakta olduğu rol, BT ile iş süreçleri arasındaki ilişkinin önemini artırmaktadır. Buna karşın, birçok organizasyon, BT kaynaklı sorunlarla karşılaşmaktadır. Bu sorunlar şu şekilde özetlenebilir (ITGI, 2003:8):

- Mali zararlar, rekabet gücünün kaybı ve itibar erozyonu,
- BT yatırımlarından beklenen faydanın elde edilememesi,
- BT yatırımlarının kuruma inovasyon anlamında beklenen katkıları sağlayamaması,
- Yetersiz veya eski teknoloji satın alınması,
- Yeni teknolojilere ayak uydurulamaması,
- Maliyet aşımları ve işlerin zamanında tamamlanamaması.

Kurumsal stratejileri üreten ve iş risklerini karar süreçlerinde dikkate alan yöneticiler, büyük maliyetler ve insan kaynağı gerektirebilecek ve çok ciddi riskleri beraberinde getirebilecek BT konusunda yeterli hassasiyeti gösterememektedir. Bunun temel nedenleri şu şekilde açıklanabilir (ITGI, 2003:8):

- BT'nin ortaya çıkaracağı riskleri veya fırsatları anlamanın, diğer iş kolları veya disiplinlere göre çok daha fazla teknik bilgi gerektirmesi,
- BT'nin, kurumun içinde kurumdan ayrı bağımsız bir alanının olması,
- Özellikle büyük ölçekli organizasyonlarda BT'nin çok fazla karmaşık olması.

Bu sorunların çözülmesi ve risklerin etkin biçimde yönetilmesi açısından BT yönetişimi büyük önem arz eder. Yönetim kurullarının ve üst yönetimin görevi olan BT yönetişimi, kurumsal yönetişimin ayrılmaz bir parçasıdır ve kurumun strateji ve hedeflerine ulaşmasını sağlayacak bir BT yönetişimi organizasyon, süreç ve liderlik unsurlarının etkin şekilde kullanılmasını gerektirir (ITGI, 2003:8). Kurumlar, BT yönetişimi sayesinde aşağıda sayılan faydaları elde edebilir:

- BT yatırımlarından beklenen faydaların, etkinlik ve verimlilik kriterlerine uygun olarak elde edilmesi,
- BT risklerinin kurum için kabul edilebilir düzeylerde yönetilmesi ve izlenmesi,
- BT'nin kurumsal hedeflere ulaşmada daha iyi katkı sağlaması,
- BT ile diğer iş süreçlerinin doğal entegrasyonu,
- BT performans yönetiminin, kurumsal performans yönetimine sürekli katkı vermesi,
- Kaynak israfı ve yanlış BT yatırımları nedeniyle doğabilecek ciddi mali kayıpların önüne geçilmesi,
- İnovasyon odaklı çözümler üretilerek, daha rekabetçi bir organizasyon yapısının sağlanması.

BT yönetişimi sorunu, BT denetimi kapsamında incelenirken; verimlilik, etkinlik, güvenilirlik ve uygunluk kriterleri belirleyici olacaktır. Söz konusu bilgi kriterlerinin birincil ve ikincil düzeyde ilgili olduğu BT süreçleri ve kontroller, COBIT, ITIL, TOGAF, ISO27K ve ISO/IEC 38500 gibi BT standartları ile sistematik hale getirilmiştir. Farklı modeller ortaya koymalarına karşın bu standartlardan yola çıkılarak oluşturulacak BT yönetişimi denetim programı aşağıdaki kontrolleri içerebilir:

- Kurumsal yönetişim ve BT yönetişimi ilişkisi,
- Kurumsal strateji ve BT stratejisi ilişkisi,
- BT stratejisi,
- BT yönetim çerçevesi, süreçler ve politikalar,
- BT organizasyonu, görev ve sorumluluklar,
- BT risk yönetimi,
- BT trendleri,
- Bilgi mimarisi,
- BT yatırımları yönetimi,
- Hizmet düzeyi anlaşmalarının yönetimi,

- BT uygulamaları yönetimi,
- BT altyapı yönetimi,
- BT güvenliği yönetimi,
- Mevzuata uyum.

Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri Çerçevesi, BT denetçisinin, BT yönetişimine ilişkin yapması gerekenleri şu şekilde sıralamıştır (ISACA, 2009:19):

- BT işlevlerinin kurumun misyonu, vizyonu, değerleri, hedef ve stratejileriyle uyumlu olup olmadığının incelenmesi,
- BT kaynaklarının ve performans yönetim sürecinin etkililiğinin denetlenmesi,
- Yasal ve çevresel zorunluluklar ile bilginin, kalite, güvenilirlik (mali nitelikte) ve güvenlik gereksinimlerine uygunluğunun denetlenmesi,
- BT ortamını olumsuz yönde etkileyebilecek risklerin incelenmesi,
- Risk odaklı bir yaklaşım kullanarak BT biriminin değerlendirmesi,
- Kurumun kontrol ortamının gözden geçirilmesi.

COSO Modeli iç kontrolü; kontrol çevresi, kurumun kendi risk değerlendirme süreçleri, bilgi ve iletişim, kontrol aktiviteleri ve kontrollerin izlenmesi olarak beş ayrı unsur ile açıklar. Söz konusu modeli kullanan Uluslararası Yüksek Denetim Kurumları Standartlarının (ISSAI), 1315 no'lu standardında BT kaynaklı önemli hata riskine ilişkin şu örneklere yer verilmiştir (INTOSAI, 2007:446-447):

- Kurumun stratejik planı ile BT stratejisi arasında uyumsuzluk,
- BT ortamında değişikliklerin yapılması,
- Mali raporlamaya ilişkin yeni sistemlerin kurulması.

Aynı şekilde Uluslararası İç Denetim Standartları'na göre (2110.A2); iç denetim faaliyeti, kurumun BT yönetişiminin kurumun strateji ve amaçlarını ayakta tutup tutmadığını ve destekleyip desteklemediğini değerlendirmek zorundadır (IIA, 2009:13).

BT yönetişiminin sağlanması konusunda özel sektör standartlardan ve iyi uygulama örneklerinden yola çıkabilirken; kamu kurumlarında hukuki düzenlemeler asıl etken olmaktadır. Ülkemizde Kamu İç Kontrol Standartları Tebliği'nin 12 no'lu standardında "İdareler bilişim yönetişimini sağlayacak mekanizmalar geliştirmelidir" denilerek bu konudaki zorunluluk mevzuatla sabit hale getirilmiş fakat bu şartın yerine getirilmesi için gerekli adımlar detaylı olarak ifade edilmemiştir. Benzer bir yapıya sahip olan Avrupa Birliği (AB) Komisyonu İç Kontrol Çerçevesi'nin 7 no'lu standardında, yeterli BT yönetişimi yapısının kurulması ve AB Komisyonu'nun BT yönetişim politikasının uygulanması gerektiği ifade edilmiştir. Ayrıca bu amaca ulaşmak için aşağıdaki şartlar sayılmıştır:

- BT yönetimine ilişkin (genellikle BT Yürütme Komitesi şeklinde) uygun teşkilatlanmanın tanımlaması,
- Bilişim sistemlerinde (bütçe kaynağına bakılmaksızın) son üç yılda kaydedilen tüm gelişmeleri kapsayan yıllık BT planlarının hazırlanması,
- Her bir bilişim sisteminin açıkça tanımlanmış bir yöneticisinin olması ve bir yürütme komitesi tarafından bu sistemin idare edilmesi,
- Yeni bilişim sistemleri projelerinin tümünün, bir vizyon belgesi temelinde onaylanması,
- Yeni bilişim sistemlerinin tamamının, AB Komisyonu'nun standart proje yönetim ve geliştirme yöntemleri kullanılarak geliştirilmesi ve ilk aşamadan itibaren güvenlik hususunun göz önünde bulundurulması (AB Komisyonu, 2007:11).

Tüm bu standartlar ve BT yönetişimine ilişkin kontroller, denetçiler için iç kontrollerin değerlendirilmesi noktasında önemli birer rehberdir. İç denetçi veya dış denetçiler; uygunluk denetimi, mali denetim veya bağımsız BT denetimlerini icra ederken, bu standartları esas alarak BT yönetişimini denetim kapsamına alabilir ve gerekli kontrol testleri ve/veya maddi doğrulama testlerini uygulayabilirler.

4.3. Bilgi Güvenliği Sorunu

Bilgi, organizasyonların en önemli varlığıdır. BT ortamında üretilen, işlenen, saklanan ve yok edilen bilgilerin bozulmasının engellenmesi, yetkisiz erişimlere karşı korunması, sürekliliğinin sağlanması ve bunlarla ilgili yasal yükümlülüklerin yerine getirilmesi amacıyla, strateji, politika ve eylem düzeyinde atılan adımlar bilgi güvenliğinin konusudur. Bilgi güvenliği, üç temel bilgi kriteri çerçevesinde tanımlanır (TSE, 2002):

- *Gizlilik*: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmek,
- *Bütünlük*: Bilginin ve işleme yöntemlerinin doğruluğunu ve tamlığını temin etmek,
- *Erişilebilirlik*: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etmek.

BT ortamlarında yönetilen bilgiye erişim, bilginin çalınması veya tahrip edilmesi manuel ortamlara göre daha kolay olmakta ve buna paralel olarak ortaya çıkan zararlar ise çok ciddi boyutlara ulaşmaktadır. Bilgi güvenliği yönetimi konusunda yeterli bilinç düzeyine ulaşamamış organizasyonlar, kötü niyetli saldırganlar için doğal hedef konumundadır. Bilişim teknolojilerinin iş süreçlerinin bir parçası olmasıyla birlikte, bilgiye her an ve her yerden erişmek beklentisi ve bu yönde alınan BT kararları ve uygulamalar, bilgi güvenliğine yönelik tehditlerin artışını da beraberinde getirmektedir (Deloitte, 2011).

Yapılan araştırmalar, BT kullanımı nedeniyle organizasyonların karşılaştığı risklerin en önemli kaynağının, bilgi güvenliği (kişisel verilerin korunması, verilerin saklanması ve yönetimi) olduğunu göstermektedir (Protiviti, 2012:3). Symantec tarafından 28 ülkeden, 2.152 küçük ve orta ölçekli (KOBİ) şirketin katılımıyla 2010 yılında yapılan araştırma sonuçlarına göre, KOBİ'ler için en önemli iş riskleri siber saldırılar ve veri(bilgi) kayıplarının yaşanmasıdır. Söz konusu şirketlerden % 73'ü siber saldırılara uğramış ve % 42'si ise gizli nitelikli kurumsal verilerini kaybetmiştir (Informationweek, 2010). Diğer bir araştırmaya göre, 2012 yılı için ilk beş güvenlik tehdidi şu şekildedir (Deloitte, 2011):

1. Mobil cihazlar (%34),
2. Üçüncü şahısları içeren güvenlik ihlalleri (%25),
3. Çalışan hatası ve ihmal (%20),
4. Gelişmekte olan teknolojilere hızlı geçiş (%18),
5. BT sistemleri ve bilginin çalışanlar tarafından kötüye kullanılması (%17).

Güvenlik açıklarından faydalanarak kuruma zarar veren dış tehditlerin yanı sıra kurum içi tehditler de (kullanıcılar ya da hizmet alımı yolu ile kuruma hizmet veren ve BT sistemlerine erişimi olan yükleniciler) çok ciddi zararlara neden olmaktadır. 2011 yılı Siber Güvenlik İzleme Araştırması'nın sonuçları, kurum çalışanları ve yüklenicilerince yapılan saldırıların, dış kaynaklı saldırılara göre %46 oranında daha fazla zarara yol açtığını ortaya koymaktadır (Karabat, 2012:46).

Kasım 2007'de kavşak çalışması yapan iş makinasının fiber kabloyu koparması sonucunda İMKB ilk seansının gerçekleştirilememiş olması (Karabacak, 2010), iş sürekliliği ve felaket kurtarma planlarının öneminin altını çizmektedir. Diğer yandan, Mart 2008'de Amerika ve Kanada'da hizmet veren Heartland Payment System'e SQL injection yöntemi ile yapılan siber saldırı sonucu, kurumun bilişim sistemlerinden 134 milyon kredi kartına ait gizli bilgilerin çalınması (CSOonline, 2012) veya ülkemizde bir gümrük memurunun şifresinin çalınması yoluyla 14 ayda 100 milyon TL civarında hayali ihracat yapılması (Gümrük ve Ticaret Bakanlığı, 2010) gibi vakalar, bilgi güvenliği konusundaki zafiyetlerin ekonomiye verebileceği zararların boyutlarını gözler önüne sermektedir.

Bilgi güvenliğine yönelik farklı detaylarda kontroller öngören ISO27K, Ortak kriterler, NIST SP 800 Serisi ve COBIT gibi uluslararası standartlar bulunmaktadır. Bu standartlar, kurum yöneticileri için olduğu kadar denetçiler için de başvuru kaynağıdır. Bilgi güvenliğinin denetim kapsamına alınması halinde, aşağıdaki hususlara ilişkin detaylı kontrolleri içeren denetim programları hazırlanabilir:

- Güvenlik politikaları,
- Örgütsel güvenlik,
- Varlık sınıflandırması ve denetimi,
- Personel güvenliği,

- Fiziki ve çevresel güvenlik,
- İletişim ve işletim yönetimi,
- Erişim denetimi,
- Sistem geliştirilmesi ve idamesi,
- İş sürekliliği,
- Mevzuata uyum (TSE, 2002).

Teknolojinin yardımı ile BT ortamında kişi veya kurumlara maddi veya manevi zarar verme olarak tanımlanan bilişim suçu (Eker, 2006:103) ulusal mevzuatlarda düzenlenmektedir. Bilgisayar sistemlerine ve servislerine yetkisiz erişim, bilişim sistemlerini bozma, verileri yok etme veya değiştirme, kanunla korunmuş bir yazılımın izinsiz kullanılması, bilişim yolu ile nitelikli dolandırıcılık gibi bilişim suçu türleri, ceza kanunları veya ilgili diğer mevzuatlarda tanımlanmaktadır ve çoğunlukla adli bilişimin konusudur. BT denetçisinin görevi, bu suçları araştırmak ya da suçluları yakalamak değildir ancak bu suç mekanizmalarına fırsat sağlayacak kontrol eksikliklerini tespit etmek ve gerekli kontrollerin kurulması için önerilerde bulunmaktır ki yapılan denetimin türü ve hedefine göre bilgi güvenliğine ilişkin denetim programının detayı değişecektir.

SONUÇ

Dijital devrim olarak da adlandırılan BT dönüşüm süreci, diğer meslekleri etkilediği kadar denetim mesleğini de etkilemiştir. Artık, kurumsal iş süreçlerinin BT ortamında yürütüldüğü ve izlendiği organizasyonlarda icra edilen denetimlerde, BT kontrollerinin değerlendirilmesi önem arz etmektedir ve bilişim alanının göz ardı edildiği denetimlerin geçerliliği ve kabul edilebilirliği giderek azalmaktadır.

Bu çalışmada, BT denetiminde değerlendirilmesi gereken kontrollerin, bilgi kriterlerinden yola çıkılarak belirlenebileceği tezi ortaya konulmuştur. Kamuda ve özel sektörde, organizasyonlar için en önemli varlık olan bilgi, alınacak stratejik kararlar ve atılacak operasyonel adımlar için belirleyicidir. Bu nedenle, organizasyonlar, iş hedefleri ile BT hedeflerini ilişkilendirirken bilgi kriterlerinden faydalanmaktadırlar. Aynı şekilde, bağımsız BT denetimlerinde ve diğer denetim türlerinin parçası olarak icra edilen BT denetimlerinde, denetimin esas unsuru olan ve denetim kanıtlarına dayanak teşkil eden bilginin; bütünlük, güvenilirlik, gizlilik (güvenlik), etkinlik ve verimlilik kriterleri açısından değerlendirilmesi gerekmektedir. Denetimin kapsamını belirleyecek bu değerlendirme, COBIT ve ilgili diğer dokümanlar kullanılarak yapılabilir. Bu çerçevede, bilişim alanındaki en önemli denetim konuları olan veri bütünlüğü ve güvenilirliği, BT yönetişimi ve bilgi güvenliği, bilgi kriterlerinden yola çıkılarak değerlendirilirken; uluslararası ve ulusal standartlar ile mevzuat hükümlerine referanslar verilmiştir.

KAYNAKÇA

Akolaş, Arzu (2004), "Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları", Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı 2004/12.

Amerika Birleşik Devletleri Sayıştayı - GAO (2009), Federal Information System Controls Audit Manual, Amerika Birleşik Devletleri.

Asya Ülkeleri Sayıştaylar Birliği - ASOSAI (2001), Introduction to IT Audit.

Asya Ülkeleri Sayıştaylar Birliği - ASOSAI (2003), IT Audit Guidelines.

Avrupa Birliği Komisyonu (2007), Revision of the Internal Control Standards and Underlying Framework, Brüksel.

Avrupa Birliği Sayıştayı - ECA (2011), Guideline for Audit of IT Environment, Lüksemburg.

Bilgi Sistemleri Denetim ve Kontrol Birliği - ISACA (2007), COBIT 4.1, Amerika Birleşik Devletleri.

Bilgi Sistemleri Denetim ve Kontrol Birliği - ISACA (2009), Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri, Amerika Birleşik Devletleri.

Bilgi Teknolojileri Yönetişim Enstitüsü - ITGI (2003), Board Briefing on IT Governance, Amerika Birleşik Devletleri.

Bilgi Sistemleri Denetim ve Kontrol Birliği - ISACA (2012a), COBIT 5, Amerika Birleşik Devletleri.

Bilgi Sistemleri Denetim ve Kontrol Birliği - ISACA (2012b), CISA Glossary, Amerika Birleşik Devletleri.

Bilişim Teknolojileri ve İnovasyon Kuruluşu - ITIF (2007), "Dijital Bilgi Devrimi Neden Bu Kadar Güçlü?", http://www.itif.org/files/DQOL-1.pdf, (Erişim Tarihi: 11.10.2012).

Champlain, J Jack (2003), Auditing Information Systems, John Wiley & Sons, Inc., New Jersey.

CSOonline (2012), "The 15 Worst Data Security Breaches of the 21st Century", http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century**,** (Erişim Tarihi: 03.10.2012).

Deloitte (2011), "Kurumların Bilgi Güvenliğine Yaklaşımı Zayıflıyor", http://www.deloitte.com/view/tr_tr/tr/7c2f092493584310VgnVCM2000001b56f00aRCRD.htm**,** (Erişim Tarihi: 03.10.2012).

Demirel, Yavuz ve Durna, Ufuk (2008), "Bilgi Yönetiminde Bilgiyi Anlamak", Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Sayı 30 (Ocak-Haziran).

Eker, Ö Umut (2006), "Türk Ceza Hukukunda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", TBB Dergisi, Sayı 62.

Gartner (2012), "Gartner Says Worldwide IT Spending On Pace to Surpass $3.6 Trillion in 2012", http://www.gartner.com/it/page.jsp?id=2074815, (Erişim Tarihi: 03.10.2012).

Gartner (2011), "IT Metrics: IT Spending and Staffing Report", http://www.sgn.co.uk/ScotiaGas/uploadedFiles/About_us/Stakeholder_info/Business_plan/Gartner%20it_metrics_it_spending_and_s_210146.pdf, (Erişim Tarihi: 03.10.2012).

Guttman, Barbara ve Roback, Edward A. (1995), Computer Security, NIST Special Publications, Devlet Matbaası, Washington.

Gümrük ve Ticaret Bakanlığı (2010), "Operasyon", http://eski.gumruk.gov.tr/tr-TR/kacakciliklamucadele/Sayfalar/operasyon.aspx, (Erişim Tarihi: 03.10.2012).

Hindistan Sayıştayı (2006), "IT Audit Manual Volume I", http://www.icisa.cag.gov.in/background%20material-it%20environment/it-audit-manual/vol-1.pdf, (Erişim Tarihi: 03.09.2012).

Hinnsen, Peter (2009), Business/IT Fusion, MachMedia, Belçika.

Hinnsen, Peter (2012), The New Normal, MachMedia, Belçika.

Informationweek (2010), "Symantec SMB Study Shows Security Concerns Rising", http://www.informationweek.com/security/vulnerabilities/symantec-smb-study-shows-security-concer/225700914, (Erişim Tarihi: 03.11.2012).

İç Denetçiler Enstitüsü - IIA (2009), Uluslararası İç Denetim Standartları.

Kalkınma Bakanlığı (2012), 2012 Kamu Bilgi ve İletişim Teknolojileri Yatırımları, Ankara.

Karabacak, Bilge (2010), "İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları", https://www.bilgiguvenligi.gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari-2.html, (Erişim Tarihi: 03.11.2012).

Karabat, Burçin Çetin (2012), "Increasing Awareness of Insider Information Security Threats in Human Resource Department", International Journal of Business and Management Studies, Yıl:4,No:1,http://www.sobiad.org/eJOURNALS/journal_IJBM/arhieves/2012_Vol_4_n_1/burcin%20_cetin_karabat.pdf ,(Erişim Tarihi: 03.11.2012).

Kayrak, Musa (2012), "Avrupa Birliği Sayıştayında Mali Denetim Çerçevesinde Yürütülen BS Denetimi", Dış Denetim, Sayı 5 (Temmuz - Ağustos - Eylül).

Menkus, Belden and Gallegos, Frederick (2001), An Introduction to the IT Auditing, EDP Auditing, Auerbach Publications, CRC Pres LLC, Amerika Birleşik Devletleri.

Protiviti (2012), "IT Audit Benchmarking Survey", http://www.protiviti.com/en-US/Documents/ Surveys/2012-IT-Audit-Benchmarking-Survey-Protiviti.pdf, (Erişim Tarihi: 02.11.2012).

Sayana, Anantha, S. (2002), "The IS Audit Process", ISACA Journal, Sayı 2002/1.

Sayıştay (2007), Yönetim Bilgi Sistemi Çerçevesi, Ankara.

Sayıştay (2008), Taslak Bilişim Sistemleri Denetim Rehberi, Ankara.

Schroeder, Ron H. (2009), "Will EDP Auditors be an Extinct Species by 2000 A.D.?", ISACA Journal, Sayı 2009/3.

Time Dergisi (2012), http://www.time.com/time/covers/0,16641,19830103,00.html, (Erişim Tarihi: 25.10.2012).

Türk Standardları Enstitüsü - TSE (2002), Bilgi Teknolojisi -Bilgi Güvenliği Yönetimi için Uygulama Prensipleri, Ankara.

Türkiye Bilişim Derneği - TBD (2010); "Bilişim Etiği", http://www.tbd.org.tr/usr_img/cd/kamubib14/raporlarPDF/RP2-2011.pdf, (Erişim Tarihi:11.10.2012).

Uluslararası Sayıştaylar Birliği - INTOSAI (1996), EDP Committee: IT Controls Student Notes.

Uluslararası Sayıştaylar Birliği - INTOSAI (2001), ISSAI 300.

Uluslararası Sayıştaylar Birliği - INTOSAI (2007a), Introduction to IT Audit.

Uluslararası Sayıştaylar Birliği - INTOSAI (2007b), ISSAI 1315.

Yıldız, Özcan R. (2007), "Bilişim Sistemleri Denetimi ve Sayıştay", Sayıştay Dergisi, Sayı 65 (Nisan-Haziran).

Watson, Richard T. (2007), "Information Systems (ed.) Amerika Birleşik Devletleri: Global Text", http://globaltext.terry.uga.edu/userfiles/pdf/Information%20Systems.pdf, (Erişim Tarihi: 21.10.2012).