T.C.
GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

BİLGİ TEKNOLOJİLERİ DENETİMİNİN İÇERİĞİ VE MALİ DENETİMDE KARŞILADIĞI RİSKLER

BİLAL BÖCEK

MUHASEBE FİNANSMAN BİLİM DALI

KASIM 2014


GAZİ ÜNİVERSİTESİ
Gazi
1926

BİLGİ TEKNOLOJİLERİ DENETİMİNİN İÇERİĞİ VE MALİ DENETİMDE KARŞILADIĞI RİSKLER

Bilal BÖCEK

YÜKSEK LİSANS TEZİ
İŞLETME ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

KASIM 2014

Bilal BÖLEK tarafından hazırlanan "Bilgi Teknolojileri Denetiminin Kapsamı ve Mali Denetimde Kullanılışı" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / ~~OY ÇOKLUĞU~~ ile Gazi Üniversitesi İşletme Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Unvanı Adı SOYADI Prof. Dr. Halim ERGEN
Anabilim Dalı, Üniversite Adı İşletme, Muh-Finans.
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum .....

Başkan : Unvanı Adı SOYADI Prof. Dr. Hasan Kaval
Anabilim Dalı, Üniversite Adı Muhasebe-Finansman Atılım Üni.
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum .....

Üye : Unvanı Adı SOYADI Y. Doç. Dr. Aden ALTAY
Anabilim Dalı, Üniversite Adı İşletme, Gazi Üniversitesi
Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/~~onaylamıyorum~~ .....

Tez Savunma Tarihi: 11.../..11../.2014

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Prof. Dr. Hikmet KAVRUK Y.
Sosyal Bilimler Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bilal BÖCEK

11.11.2014

BİLGİ TEKNOLOJİLERİ DENETİMİNİN İÇERİĞİ VE MALİ DENETİMDE KARŞILADIĞI RİSKLER

(Yüksek Lisans Tezi)

Bilal BÖCEK

GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

Kasım 2014

ÖZET

Bu çalışmada, uluslararası standartlar bağlamında bilgi teknolojileri denetiminin tanımının yapılması, içerik ve usulünün anlatılması, mali tablolar denetimine olan katkısı, kapsamının belirlenmesi, mali tablolar denetiminde risk önleme fonksiyonu ve mali tablolar denetimi içinde uygulamasında karşılaşılan sorunların ortaya konulması ile bu sorunlara karşı çözüm önerilerin geliştirilmesi amaçlanmıştır. Çalışmanın gerçekleşmesinde yerli ve yabancı kaynak araştırması yapılmıştır. Bu kapsamda, Sayıştay Başkanlığı kütüphanesinden, üniversite kütüphanelerinden, denetimle ilgili yerli ve yabancı kurum ve kuruluşların internet sitelerinden yararlanılmıştır. Çalışmanın birinci bölümünde bilgi teknolojileri denetimi ve ilgili kavramlar izah edilmeye çalışılmış, ikinci bölümde bilgi teknolojileri denetimi ve mali tablolar denetimi ilişkisi, bilgi teknolojileri denetiminin kapsamı, mali tablolar denetimine katkısı, riskleri önleme fonksiyonu anlatılmış, üçüncü bölümde örnek bilgi teknolojileri denetim raporu verilmiş ve son bölümde de bu bilgiler ışığında değerlendirmeler yapılmıştır.

Bilim Kodu : 1122
Anahtar Kelimeler : Bilgi teknolojileri denetimi, Mali denetim,
Sayfa Adedi : 115
Danışman : Prof. Dr. Halim ERGEN

CONTENT OF INFORMATION TECHNOLOGY AUDIT AND ITS RISK AVERSION FUNCTION IN FINANCIAL AUDIT

(M. Sc. Thesis)

Bilal BÖCEK

GAZİ UNIVERSITY

INSTITUTE OF SOCIAL SCIENCE

November 2014

ABSTRACT

The purpose of this study is to define the information technology audit and explain its nature and procedure in the context of the international standards and its contribution to financial audit, to introduce the problems encountered determining the scope of IT audit for financial audit, its risk prevention function and solutions against these problems is to be developed. Domestic and foreign sources in the realization of the research study was conducted. In this context, the library of the Court of Accounts, university libraries and web sites of domestic and foreign institutions and organizations related to auditing were benefited from. In the first part of this study information technology auditing and related concepts are explained, in the second part, information technology auditing and financial control relations, information technology audit scope, information technology audit contribution to financial audit and its risk prevention function is described. In the third section, sample information technology audit report was submitted and in the final chapter in this in light of evaluations are made.

Science Code : 1122

Keywords : Information technology audit, Financial Audit

Page Number : 115

Supervisor : Prof. Dr. Halim ERGEN

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren, kıymetli tecrübelerinden faydalandığım danışmanım, hocam Prof. Dr. Halim ERGEN'e, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli eşim Emine BÖCEK'e teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri
AICPA	Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü
BDDT	Bilgisayar Destekli Denetim Teknikleri (Computer-Assisted Audit Techniques-CAATs)
BT	Bilgi Teknolojileri
CIS	Sürekli ve aralıklı simülasyon (Continuous and Intermittent Simulation)
COBIT	Bilgi Teknolojileri ve İlgili Teknoloji için Kontrol Amaçları (Control Objectives for Information and Related Technology)
ISACA	Bilgi Sistemleri Denetimi ve Kontrolü Birliği (Information Systems Audit and Control Association)
NIST	Standartlar ve Teknoloji Ulusal Enstitüsü (National Institute of Standards and Technology)
SCARF	Sistem kontrol denetim inceleme dosyası (System control audit review file)
UFRS	Uluslararası Finansal Raporlama Standartları (International Financial Reporting Standards)

GİRİŞ

Bilgi sistemleri kullanımının iş hayatında yaygınlık kazanması ile artan önemi bilgi teknolojileri denetimi konusunu ön plana çıkarmaktadır. Verilerin otomatik olarak işlenmesinde ve elektronik ortamlarda saklanmasında genellikle göz ardı edilen bir yön vardır. Bilgi sistemleri yanılmaz değildir ve iyi şekilde uygulanmadığı, izlenmediği ve kontrol edilmediği zaman iş süreçlerini hedef alan önemli riskler oluşturabilir. Süreç ve kontroller doğru işlemediğinde eksik, yanlış ve geçersiz veri üretme olasılığı yüksektir. Bilgi teknolojilerinin yoğun kullanıldığı çevrelerde mali tablolar ve diğer mali veriler işletmelerin bilgisayar sistemlerinin bir çıktısıdır. Dolayısıyla da mali tablolar denetiminde mali verileri oluşturan bilgi sistemlerinin göz ardı edilmesi mümkün değildir. Diğer taraftan, artan bilgi güvenliği sorunları ve yasal mevzuatla birlikte kuruluşlar bilginin gizliliği, elverişliliği ve bütünlüğü konusunda önlemler almak ve bunları korumak zorundadırlar. Mali ve mali olmayan veri ve bilgileri elektronik ortamda işlem gören ve saklanan tüm kuruluşlar için yasal bir zorunluluktan öte kurumsal sürdürülebilirliklerinin güvencesi açısından bilgi teknolojileri denetimi kritik öneme sahip bir konudur.

Bilgi teknolojileri denetimi ve mali denetimle ilişkisinin ele alındığı bu çalışmanın birinci bölümünde kavramsal tanımlamalara yer verilmiştir. İkinci bölümde mali denetim ve bilgi teknolojileri denetimi tanımlanarak aralarındaki ilişki incelenmiş, mali denetim için yapılacak bilgi teknolojileri denetiminin kapsam sorunu, mali denetime katkısı ve mali denetimde karşıladığı riskler ele alınmıştır. Üçüncü bölümde bilgi teknolojileri denetim raporu örneği üzerinde durularak çalışma sonlandırılmıştır.

1. BÖLÜM

TANIMLAR VE KAVRAMSAL AÇIKLAMALAR

1.1. Bilgi Teknolojisi ve Bilgi Sistemleri

“Bilgi teknolojisi kavramı, bilgi üretmek için bilgi sistemlerinde kullanılan donanım ve yazılımların hepsine birden verilen addır. Bilgi sistemleri kavramı ise kullanıcılara çıktı bilgi vermek amacıyla bilgi toplayan, depolayan ve veriyi yöneten bilgisayar tabanlı bileşenler ile elle kontrol edilen bileşenlerden oluşan insan yapımı sistemlerdir” (Gelinas, ve diğerleri, 2012: 14). Bilgi teknolojisi ve bilgi sistemi kavramları bazen birbirlerinin yerine kullanılmaktadır.

Bilgi sistemleri ürettikleri bilgi ile yöneticilerin firmanın faaliyetlerini planlama ve kontrol etmede büyük kolaylık sağlar. Üretilen bilginin kalitesi ve güvenilirliği doğru karar vermede önemli bir belirleyicidir. Bilgi üretim sürecindeki herhangi bir zayıflık doğru çıktının oluşmasına ve dolayısıyla doğru karar vermeyi olumsuz etkiler.

1.1.1. Parti/Yığın Sistemler ve Online Sistemler

“Yığın/parti sistemi, verilerin belli bir merkezde toplanarak bir defada toplu olarak sisteme girişi yapılmasıdır” (Cascarino, 2012: 8). Bu şekilde yapılan veri girişlerinde işlemlerde hata yapılma oranı hayli yüksektir. Dolayısıyla bu tür sistemlerin denetiminde temel denetim hedefi tamlık ve doğruluktur. Bilgisayar destekli ticaretin ilk yıllarından 1960’lu yılların sonlarına kadar işlemlerin çoğu yığın/parti sistemi ile gerçekleştirilmiştir.

Online sistemlerin ortaya çıkmasıyla yığın sistemleri ve dolayısıyla yığın sistemlerine ilişkin kontroller de ortadan kalkmıştır. “Bugünün sistemlerinde veri girişi ve işleyişi online sistemlerde ve gerçek zamanlı olarak ve küçük yığınlar halinde yapılmaktadır” (Cascarino, 2012: 20). Veri girişlerinin yapıldığı terminaller lokal bölgelerde olabileceği gibi uzak mesafelerde de olabilir. Farklı tipte terminaller olsa da denetimde ana kontrol hedefleri aynıdır: Mevcudiyet, güvenilirlik, gizlilik ve doğruluk.

1.1.2. Elektronik Veri Alışverişi (EDI)

“Elektronik veri alışverişi (EDI), ticaret yapan iki kuruluş arasında, insan faktörü olmaksızın bilgisayar ağları ile belge ve bilgi değişimini sağlayan bir sistemdir” (Cascarino, 2012: 20). Bu kavram 1970'den beri bilinmekte ve satınalma siparişi, fatura gibi geleneksel satıcı-alıcı ilişkilerini otomatikleştirme için kullanılmaktadır. İş dünyasında kullanılan kâğıt belge değişiminin yerine geçmektedir. Stok yönetimi ve ürün sevkiyatı gibi farklı alanlar da otomasyona geçtiği için şirketler veya birimler arası veri aktarımı çok daha farklı alanlara kaymakta ve genişlemektedir.

1.1.3. Elektronik Ticaret (e-ticaret)

“e- ticaret, bilgi ve iletişim teknolojilerini kullanarak müşterilerin ihtiyaçlarını ve beklentilerini daha iyi karşılamak için dışsal ve içsel veri üretim sistemlerinin birbirine bağlanması ve daha hızlı veri alış-verişinin sağlanmasıdır” (Cascarino, 2012: 21). e-ticaret, elektronik satınalmadan tedarik yönetim süreçlerine kadar birçok iş süreçlerini kapsar. Mal ve hizmetlerin üretim, tanıtım, satış, sigorta, dağıtım ve ödeme işlemleri bilgisayar ağları üzerinden yapılır. Elektronik ticaret, ticari işlemlerden biri veya tamamının elektronik ortamda gerçekleştirilmesi yoluyla reklam ve pazar araştırması, sipariş ve ödeme, teslimat olmak üzere üç aşamadan oluşmaktadır.

1.1.4. Bulut Bilişim (cloud computing)

“Bulut bilişim veya işlevsel anlamıyla çevrim içi bilgi dağıtımı; bilişim aygıtları arasında ortak bilgi paylaşımını sağlayan hizmetlere verilen genel addır. Bulut bilişim bu yönüyle bir ürün değil, hizmettir; temel kaynaktaki yazılım ve bilgilerin paylaşımı sağlanarak, mevcut bilişim hizmetinin bilgisayarlar ve diğer aygıtlardan elektrik dağıtıcılarına benzer bir biçimde bilişim ağı (tipik olarak İnternet'ten) üzerinden kullanılmasıdır” (Cascarino, 2012: 22).

Bulut sözcüğü dosyaların sağlandığı konumu işaret etmektedir. Klasik bir algı olarak işleme ve saklama konumlarının aynı aygıtta bulunması durumu klişeleşmiştir. Ancak saklama boyutu bulutlara yani saklama ve altyapı hizmeti

barındıran hizmetlere doğru kaymaktadır. Bu gidişin ilk öncü uygulamaları, İnternet sağlayıcıları tarafından, yedekleme amacıyla sunulan bulutlardır. Örneğin, Türkiye'de hizmet veren bir İnternet sağlayıcısı olan *TTNET; TTNET Bulutu* adlı hizmetle Türkiye piyasasına girmiştir. Google gibi uluslararası bilişim şirketleri ise; *Google Docs* gibi çevrim içi bilgi işleme özelliği sunan uygulamalar geliştirmiştir. Ayrıca Microsoft ve Intel gibi büyük teknoloji firmaları da bu teknolojiyi bilişim tüketicisine sunmuştur.

1.2. Bilgi Teknolojileri ile İlgili Güvence Hizmetleri

Bilgi teknolojileri güvence hizmetlerinin talebini etkileyen önemli etmenler internetin ve e-ticaretin gelişmesidir. İnternetteki bilginin bilgilerin güvenliği ve gizliliğine ilişkin endişeler e-ticaretin potansiyel büyümesini yavaşlatmıştır. Ayrıca internette mevcut olan eş anlı bilgilerin miktarı güvence ihtiyacını finansal tablolar gibi belirli bir tarihteki bilgilerden eş anlı bilgi üreten süreçlerin güvenilirliğine ilişkin güvencelere kaydırmıştır. Örneğin, sipariş ve ödeme gibi pek çok işletme fonksiyonu bilgisayarlar arasında doğrudan elektronik bilgi alışverişi (EDI) ile internet üzerinden yerine getirilmektedir. İşletmeler ve bilgiler çevrimiçi ve eş anlı olarak paylaşıldığı için elektronik olarak işlem gören bilgiler ve işlemler ile ilgili bilgilerin güvenliğini içeren bilgisayar kontrollerine ilişkin güvenceler için talep artmaktadır. Denetim firmaları bu işlevlere ilişkin güvence hizmetleri verebilirler. Bilgi teknolojileri ile ilgili güvence hizmetlerinin iki örneği web sitesi kontrollerine ilişkin güvence ve bilgi sistemleri güvenilirliğine ilişkin güvencelerdir (Güredin, 2010: 6).

1.2.1. WebTrust Hizmetleri

İnternet üzerinden yapılan işlemlerdeki ani artış sonucunda güvence hizmetlerine olan ihtiyacın artmasına karşılık verebilmek için Amerikan ve Kanada Yeminli Mali Müşavirler Enstitüleri (AICPA) birlikte WebTrust güvence hizmetlerini yarattılar. Bu hizmeti vermek için AICPA'dan yetki alan denetim firmaları elektronik WebTrust mührü ile onaylamak suretiyle web sitesi kullanıcılarına güvence verirler. Bu mühür, web sitesinin sahibinin işletmecilik uygulamaları, işlemlerin dürüstlüğü ve bilgi süreçlerine ilişkin belirlenmiş kriterlere uyduğuna dair güvence verir.

WebTrust bir onaylama hizmetidir ve WebTrust mührü elektronik ticaret uygulamalarının açıklanması ile ilgili yönetim iddialarına ilişkin denetçi raporunun sembolik gösterimidir (Güredin, 2010: 7).

1.2.2. SysTrust Hizmetleri

AICPA ve CICA, bilgi sistemlerinin güvenilirliğine ilişkin güvence sağlamak amacıyla birlikte SysTrust hizmetlerini yarattılar. SysTrust, güvenlik ve bilgilerin dürüstlüğü gibi konularda sistem güvenilirliğini değerlendirmeye ve test etmeye yönelik onaylama tipi bir sözleşmedir. WebTrust güvence hizmetleri esas olarak bir web sitesini kullanan üçüncü şahıslara güvence vermeyi amaçlarken SysTrust hizmetleri işletme yönetimine, yönetim kuruluna ve üçüncü şahıslara eş anlı bilgi üretmede kullanılan bilgi sistemlerinin güvenilirliğine dair güvence vermeyi amaçlar (Güredin, 2010: 8).

12.3. Diğer Bilgi Türlerine İlişkin Güvence Hizmetleri

Denetçilerin verebileceği hizmet türlerinin sınırı yoktur. Amerikan meslek odası Güvence Hizmetleri Özel Komitesince yapılan bir araştırma büyük denetim firmalarınca verilmekte olan 200'den fazla güvence hizmeti saptamıştır. (Güredin, 2010:8).

1.3. Muhasebe Bilgi Sistemleri ve Girdi Birimleri

"Muhasebe bilgi sistemi (MBS), işletmenin varlıkları ve bu varlıkların kaynakları olan sermaye ve borçlar üzerinde değişme yaratan mali nitelikteki işlemlere ait verileri toplayan, toplanan verileri işleyerek bilgiye dönüştüren ve ortaya çıkan bilgileri raporlayan bir bilgi sistemidir" (Sürmeli, 2005: 98). Muhasebe bilgi sisteminde bilgiler girdi-işleme-çıktı çerçevesinde işleme tabi tutulur.

1.3.1. Kaynak Dokümanı

"Kaynak doküman, verilerin elektronik olarak işlenmesi amacıyla verilerin makine tarafından okunabilir bir araca uyarlanmasıdır. Örneğin zaman kartları, ücret

pusulaları, iş başvuru formları, patent giriş formları, satınalma faturaları, satış faturaları, nakit makbuzları ve ücret bordroları kaynak dokümanlara örnek olarak gösterilebilir" (Sürmeli, 2005: 98).

Kaynak dokümanlar bilgisayar ortamında oluşturulan dosyaların zarar görmesi veya yok olması durumunda yedek olarak hizmet sunar. Ayrıca bir işlemin somut kanıtını oluşturması nedeniyle kaynak dokümanlar bir denetim izinin başlangıç noktasını da oluşturmaktadır.

1.3.2. Veri Uyarlama

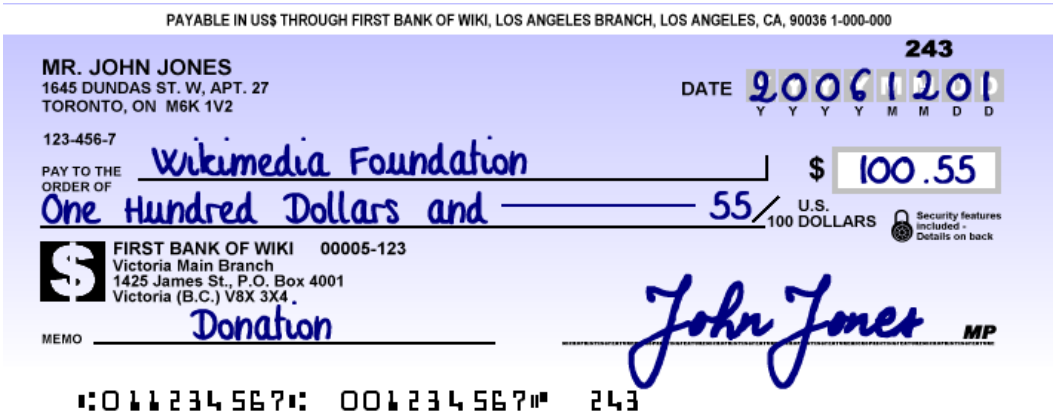
Elle hazırlanan kaynak dokümanlarının en büyük dezavantajı bilgisayar tarafından okunamamasıdır. Bu nedenle kaynak dokümanları verilerinin elektronik olarak işlenmesi için öncelikle bilgisayar tarafından okunabilir şekilde uyarlanması (kopyalanması) gerekmektedir. Ancak bu veri uyarlaması (kopyalaması); verimsiz, emek yoğun, zaman alıcı ve maliyetli bir işlem olmasının yanında veri kaybı, hata, hile, suistimal, sabote etme gibi olasılıklara da ortam hazırlamaktadır. Tüm MBS'lerdeki bilgisayar tarafından okunan veriler düşünüldüğünde bu durumun önemi çok daha iyi anlaşılmaktadır. Bu sorunu aşmak için bazı aygıtlar bulunmaktadır (Yalkın, 2011).

1.3.2.1. POS makineleri (Point of sale)

"İşletmelerin satış noktalarının, şubelerinin, tahsil yerlerinin birden çok olduğu durumlarda satışların yapıldığı anda ve yerde yapılan satışların anında izlenmesi, kayıtlara geçirilmesi ve tahsilat işleminin yapılabilmesi amacıyla kullanılan sabit veya mobil olabilen satış noktası araçlarıdır. POS araçları satış yapıldığı anda verilerin gerçek zamanlı olarak yazılımlar aracılığıyla kaydedilmesini ve merkezi bilgisayara aktarılmasını sağlar" (Sürmeli, 2005: 98).

1.3.2.2. Manyetik mürekkep karakterli okuyucular (Magnetic ink character recognition-MICR)

Manyetik mürekkep karakter tanıma (MICR) çek ve diğer belge işlemlerini hızlandırmak ve kolaylaştırmak için bankacılık sektöründe ağırlıklı olarak kullanılan bir karakter tanıma teknolojisidir. MICR çizgisi denilen MICR kodlama, çek ve diğer kuponların en altında yer alır. Bu kodlar genellikle belge türü, banka kodu, banka hesap numarası, çek numarası, çek miktarı vb. bilgileri içerir. Teknoloji, MICR okuyucularına bilgileri tarayıp okuyarak doğrudan veri toplama cihazlarına aktarmayı sağlar. Barkotlar ve benzeri teknolojilerin aksine, MICR karakterler insanlar tarafından kolayca okunabilir.



Şekil 1.1. MICR kodlama kullanılan çek örneği (www.en.wikipedia.org, 2014)

1.3.2.3. Optik karakter tanıma (Optical Character recognition –OCR)

Optik karakter tanıma, fotoğraf ve tarama yöntemiyle elde edilmiş görüntü veya basılı metinlerin elektronik bilgiye dönüştürerek bilgisayar ortamında okunmasını sağlayan aygıtlardır. Pasaport belgeleri, faturalar, banka ekstresi, makbuzlar, kartvizit, posta veya çeşitli basılı kayıtlardaki bilgilerin bilgisayar ortamına aktarılmasında yaygın olarak kullanılan bir yöntemdir. OCR kaynak dokümanları da MICR gibi hem kişiler hem de bilgisayar tarafından okunabilmektedir.

1.3.2.4. Manyetik şeritli plastik kartlar

Manyetik şeritli plastik kartlar kaynak dokümanlar arasında önemli yer tutarlar. Kart üzerindeki manyetik şeritte kullanıcılara ilişkin veriler depolanmaktadır. Kredi kartları, bankamatik kartları manyetik şeritli kartlardandır. Kişinin kimlik bilgileri, hesap numarası vb. verileri taşıyan bu şeritler optik karakter kart okuyucularla bilgi sistemine giriş yapılmasında kolaylık sağlar.

1.3.2.5. Biometrik tarayıcılar

“Biometrik tarayıcılar; insanların parmak izi, göz retinası, iris, yüz şekli, ses, imza, avuç içi vs. gibi karakteristiklerini saptayarak bilgisayar sistemleri, veri bankaları vb. ortamlara giriş için kimlik doğrulamasını yapmaktadırlar. Biometrik sistemler temelde, kişinin sadece kendisinin sahip olduğu, değiştiremediği ve diğerlerinden ayırt edici olan, fiziksel veya davranışsal bir özelliğinin tanınması ile çalışmaktadırlar; ancak bu sistemlerin güvenilir olmalarının yanı sıra pratik olmaları da gerektiği için kişileri hangi yöntemler ile saptadıkları da önemli bir etkendir. Sonuç olarak biometri yöntemlerinin güvenlik sistemlerinin geliştirilmesinde, suçluların bulunmasında ve insanların tanımlanmasında kullanımı gittikçe artmaktadır” (Jain ve diğerleri, 2008: 1). Türkiye’de Sosyal Güvenlik Kurumu’nun (SGK) sağlık alanındaki suistimalleri önlemek için hazırladığı avuç içi damar izi sistemiyle biometrik kimlik doğrulama sistemine 20 ilde uygulamaya başlamıştır.

2. BÖLÜM

DENETİM, MALİ TABLOLAR DENETİMİ VE BİLGİ TEKNOLOJİLERİ DENETİMİ

2.1. Denetim

Denetim kavramının tek ve kesin bir tanımını yapmak biraz zordur. Tanınmış birçok yazar denetim kavramının tanımı yapmıştır ve her bir tanım denetimin farklı yönlerine vurgu yapmaktadır.

Genel olarak denetim, "İktisadi faaliyet ve olaylarla ilgili iddiaların önceden saptanmış ölçülere uygunluk derecesini araştırmak ve sonuçları ilgi duyanlara bildirmek amacıyla tarafsızca kanıt toplayan ve bu kanıtları değerleyen sistematik bir süreçtir" (Donald ve William, 1997: 2).

Montgomery'e göre, "Denetim, bir işletme veya kuruluşun defter ve kayıtlarının finansal ve operasyonel gerçekleşmeleri doğru yansıtıp yansıtmadığını tespit etmek ve raporlamak için yapılan sistematik incelemedir".

Spicer ve Pegler denetim tanımını biraz daha genişletmiştir, "Denetim, bir işletmenin defter, kayıt ve belgelerinin denetçiyi işletmenin bilançosunun düzgün hazırlandığı konusunda tatmin edecek düzeyde incelenmesi ile elde edilen bilgiler ışığında ilgili dönemde elde edilen kar veya zarar ile yapılan açıklamaların işletmenin faaliyetlerini gerçek ve adil bir şekilde yansıtıp yansıtmadığına karar vermektir".

Lawrence R. Dicksee'ye göre, "Denetim, muhasebe kayıtlarının ilgili oldukları işlemleri tam ve doğru yansıtıp yansıtmadığını araştırmak amacıyla muhasebe kayıtlarının incelenmesidir. Bazı durumlarda denetim, bu işlemlerin kendileri otorite tarafından desteklenip desteklenmediğini tespit için gerekli olabilir."

Amerikan Muhasebeciler Enstitüsü, 9 No.lu Muhasebe Araştırma Bülteni'nde (Accountin Research Bulletin No: 9) denetimi şu şekilde tanımlamıştır:

Genel olarak, muhasebe belgeleri ile onu destekleyen kanıtların bir görüşe ulaşabilmek için incelenmesidir. Özellikle,

1. Ödeme veya borçlara ilişkin iddialar ile bunları destekleyici kanıtların, gerçekleşen harcamaların yetkilendirme dahilinde olup olmadığını, usulüne uygun ve tam olarak yapılıp yapılmadığını tespit etmek amacıyla incelenmesidir.
2. Benzer karakterli veya benzer amaçlar taşıyan ve sadece gerçekleşen işlemleri yansıttığını iddia eden hesapların incelenmesidir; örneğin tahsilat ve ödeme belgelerine dayanan hesap işlemleri gibi.
3. Daha geniş kapsamda düşünüldüğünde, denetim sadece hesapların incelenmesi faaliyeti değil, aynı zamanda hesapların tam olarak sunulması ve gerçek durumu yansıtması bakımından değerlemelerin, tahminlerin ve görüşlerin de incelenmesidir.

Denetim süreci, sermaye piyasalarının sağlıklı kurgulanmış, kullanıcıları tarafından bilinen, güvenilen ve talep edilen bir kontrol mekanizmasıdır. Buna rağmen denetimin ortaya çıkışı, bugüne kadar varoluş sebebi ve sürekli gelişimi hakkında bilinen gerçekler sınırlıdır. Denetimin ortaya çıkışı 1929 yılında Amerika Birleşik Devletlerinde ortaya çıkan ekonomik kriz ile yakından alakalıdır; ancak bilimsel temelleri daha sonraki yıllarda atılmıştır. 1961 yılında Mautz ve Sharaf temelleri 1930'lu yıllara kadar dayanan bir projenin sonunda Denetimin Felsefesi (The Philosophy of Audit) adlı eseri yayınladılar; ancak muhasebe teorisinin aksine denetim teorisi çok az kişinin ilgisini çekmiştir. Denetim felsefesi, denetim metodolojisi ve denetimin ön kabulleri üzerine geniş bir tartışma ortamı başlatmışlardır. Bunun yanında denetimin temelini oluşturan denetim kanıtı, denetim öncesi hizmetler, tarafsız sunum, bağımsızlık ve etik davranış gibi hususları da tartışmaya açmışlardır.

"Mautz ve Sharaf'ın yenilikçi yaklaşımı denetim teorisinin kurulmasında yeni ufuklar açmıştır ve bu çalışma denetim literatüründe kilometre taşı olarak kabul edilmektedir. Onlara göre, bir denetim teorisi ortaya koyabilmek için denetimin doğasına ve problemlerine belirli ilkeler ışığında bakmak gerekir. Bu da denetimin metodunu, ön kabullerini ve konseptini araştırmayı gerektirir. Bu bağlamda, ilk kez denetim prensiplerini ayrıntılı olarak içeren bir denetim teorisini öne sürdürülerek kurumsal

örgütlere denetimin uygulanması ve fikir konusunda kolaylık sağlayan bir yapı ortaya koymuşlardır" (Soltani, 2007: 10).

Mautz ve Sharaf'a göre geniş bir denetim anlayışına sahip olmak için denetimin beş düzeyli yapısını anlamak gerekir. En alt basamakta bütün temel disiplinlerin ve teorik bilimin üzerine inşa edildiği filozofik temel yer alır. Bu filozofik temellerden esas kavramların geliştirilmesine zemin hazırlayan önermeler çıkarılabilir. Bundan sonra teorinin etrafında şekillenen kavramsal çerçeve ortaya çıkar. Uygulayıcılara rehberlik etmek üzere gücünü bu kavramsal çerçeve ve önermelerden alan talimatlar geliştirilir. Son olarak da kuralların gerçek olaylara uygulandığı pratik uygulamaları oluşturan daha üst bir yapı ortaya çıkar. Sonuç olarak birinci, ikinci ve üçüncü seviyede yer alan filozofik temel, önermeler ve kavramsal çerçeve uygulamaları şekillendiren talimatları oluşturur.

Denetim, diğer bütün bilim alanlarında olduğu gibi filozofik bir temele dayanmalıdır ve onu oluşturan temel disiplinlerden asla ayrılmamalıdır; ancak denetçiler bazen denetimin teorisinden ziyade denetim yöntem ve uygulamalarına ilişkin problemlere daha çok ilgi duymaktadırlar. Denetim alanında teori ve uygulama arasında çok yakın bir ilişki vardır, şöyle ki uygulamada karşılaşılan sorunlara kesin çözüm ancak teorinin kullanılması ve geliştirmesi ile bulunabilir. "Teorik bakış açısına sahip olmak, uygulayıcılara denetimlerde tutarlılık sağladığı gibi denetim alanında denetçiye üstünlük de sağlar. Dahası, iyi kurgulanmış bir denetim teorisi ile denetçi sermaye piyasalarında gerçek bir ekonomik ajan olabilir" (Soltani, 2007: 10).

Mautz ve Sharaf (1961) denetimin muhasebenin bir bölümü olarak görülmesine karşı çıkmışlardır. Onların görüşlerine göre denetim ve muhasebe yakın ilişki içinde olmalarına rağmen doğaları tamamen farklıdır. Muhasebe finansal verilerin toplanması, sınıflandırılması, özetlenmesi ve raporlanmasını içerir, işletme faaliyetlerinin ölçülmesi ve raporlanmasıyla ilgilenir. Muhasebenin görevi yığınlar halindeki ayrıntılı bilgileri yönetilebilir ve anlaşılabilir hale getirmektir; ancak denetim sayılanların hiçbiriyle ilgilenmez. Denetim işletme faaliyetlerini ve koşullarını dikkate alır, fakat onları ölçme ve raporlama gibi bir görevi yoktur. Onun görevi muhasebeye ilişkin ölçüm, değerlendirme ve raporları teftiş etmektir.

2.1.1. Denetimin amaçları

Denetimin amacı genel olarak, “hataların yapılmasını engellemek, önlemek olabileceği gibi hata ve yanlışlıkları düzeltme ve gerekliyse reform yapılmasına ışık tutmak da olabilir” (Atay, 1999: 22-23).

Bu işlevlerin yanı sıra denetimin amacı, “Denetlenen kurumun amaç ve politikasına açıklık getirmek, amaç ve politikayı geliştirmek, amaca ulaşmada ilgililere yardımcı olmak, yapılan çalışmaların, hizmet edilen toplumun ihtiyaçlarını karşılayacak biçimde geliştirilmesine katkıda bulunmak, kurumla ilgili yenilik ve gelişmeleri izlemek açısından yönetime önemli katkılar sağlamak” (Saran, 1995) şeklindedir.

Denetimin amaçları genel hatları ile aşağıdaki gibi sınıflandırılabilir (Kumar ve Sharma, 2013: 5):

1. Öncelikli/ana amaç,
2. Tali amaç,
3. Özel amaç,

Öncelikli/ana amaç: Muhasebe verilerinin denetiminde temel gaye muhasebe kayıtlarının muhasebe dönemi içinde gerçekleşen iktisadi olayları tam ve doğru olarak yansıtıp yansıtmadığına karar vermektir. Dolayısıyla finansal tablolar denetiminde bağımsız denetçinin öncelikli hedefi finansal tabloların gerçek ve tarafsız şekilde kuruluşun finansal durumunu ve faaliyet sonuçlarını gösterip göstermediğine karar vermek ve görüş açıklamaktır. Hata ve hileleri tespit etmek denetimin temel hedefi gibi görülse de bu amaç ancak tali bir hedeftir.

Tali amaç: Denetçi kuruluşun finansal durumu hakkında görüş açıklarken muhasebe defterlerine, kayıtlarına ve bunları destekleyen dokümanlara bakmak zorundadır. Bu incelemeler sırasında birtakım hata ve hileler ortaya çıkabilir. Hata kavramı, muhasebe dilinde kasıtsız olarak olayları gerçeğe aykırı yansıtmak şeklinde tanımlanır. Hatalar, maddi hatalar olabileceği gibi bir muhasebe prensibinin uygulanmaması veya yanlış uygulanması şeklinde de olabilir. Hile, karşı tarafı aldatmak veya karşı tarafa zarar vermek maksadıyla başvurulan yöntemlerdir. Hile, genellikle iki veya daha fazla kişi

tarafından yapılır, denetçi tarafından ortaya çıkarılması özel çaba gerektirir. Hata ve hilenin önlenmesi denetimin tali amacıdır.

Özel Amaçlar: Denetim otoritelerinin denetim tanımlarının analizinden ve denetim alanındaki yeni gelişmelerden anlaşılabileceği gibi denetim sadece finansal tablolar denetimi değildir. Faaliyet denetimi, maliyetlerin gözden geçirilmesi, vergi kanunlarına uyum gibi hususlar denetimin daha geniş kapsamı içinde özel amaçlı denetimler olarak adlandırılır. Özel amaçlı denetimlerin denetim hedefleri de özel gaye taşıyacaktır.

2.1.2. Denetimin sınıflandırılması

Denetim türleri değişik ölçütler altında sınıflandırılabilir. Denetimi, denetimi yapanların niteliğine ve denetimin amacına göre iki sınıfa ayırabiliriz. “Denetçilerin niteliğine göre denetim türleri iç denetim, bağımsız denetim ve kamu denetimlerinden oluşmaktadır. Denetim ile elde edilmek istenen amaca göre ise denetim türleri finansal tablolar denetimi, uygunluk denetimi ve faaliyet denetimi olmak üzere üç başlık altında sınıflandırılmaktadır” (Donald ve William, 1997: 4).

2.1.2.1. Denetçilerin niteliğine göre denetim türleri

Denetçi, “Denetim faaliyetlerini yürüten, mesleki bilgi ve deneyime sahip, bağımsız davranabilen ve yüksek ahlaki nitelikleri taşıyan uzman kişilerdir.” (Maliye Hesap Uzmanları Derneği, 1997: 7).

Denetim faaliyetini yürüten denetçiler çeşitli unvanlar altında çalışabilirler. Denetçilere taşıdıkları unvanlara göre iç denetçi, bağımsız denetçi ve kamu denetçisi denir. İşletme dışından bağımsız uzmanlar tarafından yapılan denetime dış denetim veya bağımsız denetim denirken İşletmenin bünyesinde veya işletme adına çalışan denetçilerin yaptıkları denetime iç denetim, kamu tarafından görevlendirilmiş denetim elemanlarının yaptıkları denetimlere ise kamu denetimi denir. Bu kapsamda değerlendirilen denetçi statülerine göre denetim türleri aşağıda ayrıntılı olarak açıklanmıştır (Kavut ve diğerleri, 2009: 35).

2.1.2.1.1. Bağımsız denetim

Bağımsız denetim, işletme dışından işletme ile herhangi bir organik bağı olmayan kişi ve kurumlar tarafından yapılan denetimlerdir. Bağımsız denetim; finansal tabloların, genel kabul görmüş muhasebe kavram, ilke ve standartlarına uygunluğu ile bilgilerin doğruluğunun ve gerçeği dürüst bir biçimde yansıtıp yansıtmadığının, denetçiler tarafından denetim ilke ve kurallarına göre, defter, kayıt ve belgeler üzerinden incelenmesi ve tespit edilen sonuçların rapora bağlanması sürecidir. (Kavut ve diğerleri, 2009: 36). Bağımsız denetim kapsamında denetim yapan denetçilere bağımsız denetçiler denilmektedir. Bağımsız denetçiler (external auditors) “Denetlenen kuruluştan bağımsız sertifikalı kamu denetçileridir ve denetim hizmetlerini sözleşmeye dayalı olarak yürütürler” (Donald ve William, 1997: 6). Bağımsız denetimlerin çoğunluğunu finansal tablo denetimi oluşturmaktadır.

Bağımsız denetim sürecinde denetçinin bağımsız olması esastır, bu nedenle bağımsız denetimde denetçinin aşağıdaki koşulları karşılıyor olması zorunludur (Kavut ve diğerleri, 2009: 36):

- İşletme ile denetim sözleşmesinde belirlenen tutar dışında bir ücret ilişkisi olmamalıdır ve bunun dışında ücret veya başka bir isim altında ödeme yapılmamalıdır.
- İşletme ile herhangi bir ekonomik faaliyet içerisinde olmamalı, herhangi bir iş ilişkisi, danışmanlık, ticaret gibi bir ilişki bulunmamalıdır.
- İşletme ile herhangi bir borç alacak ilişkisi söz konusu olmamalı, işletmeden borç almamalı veya borç vermemelidir.

2.1.2.1.2. İç denetim

İç denetim, işletme içi daimi statüde çalışan ya da işletme dışından sürekli olarak iç denetçi statüsünde hizmet veren finansal nitelikli ve finansal nitelikli olmayan tüm işletme faaliyetlerinin incelenmesidir. Diğer bir deyişle, kamu veya özel sektörde kurum veya işletmeye bir ücret akdi ile bağlı olarak çalışan kişilerin yönetim adına üstlenmiş oldukları bir denetim türüdür (Kavut ve diğerleri, 2009: 37).

İç denetçiler (internal auditors) “Kuruluş içinde örgütlenmiş, kuruluşun faaliyetlerini inceleyen ve değerlendiren fonksiyonel bağımsızlığı olan ve aynı zamanda kuruluşun bağımlı çalışanı olan denetçilerdir.” (Donald ve William, 1997: 6). Genellikle iç denetçiler uygunluk denetimi ile birlikte faaliyet denetimi de yaparlar. Kuruluşun birçok fonksiyonunun yönetimin politikalarına, kanunlara ve diğer düzenlemelere uygunluğunu araştırırlar. Aynı zamanda muhasebe ile ilgili bilişim sistemlerinin düzgün çalışıp çalışmadığını da denetlerler. Genellikle iç denetim sonucunda elde edilen bulgular üst yönetime veya yönetim kuruluna bağlı denetim komitesine raporlanmaktadır.

İç denetim işletmeler için faaliyetlerinin etkinliğini inceleyen, işletmenin hedeflerine ne ölçüde ulaştığını ortaya çıkaran önemli bir denetim fonksiyonudur. İç denetçiler yönetim kuruluna bağlı olarak onların belirlediği görev alanı içinde kalarak çalışmalarını yürütürler. İç denetçilerin görev kapsamında aşağıdaki faaliyetler sayılabilir:

- İşletmenin muhasebe işlemlerini ve hazırlanan raporların doğruluğunu tespit etmek,
- İşletme faaliyetlerinin bütçe hedeflerine ve planlara uygun olup olmadığını tespit etmek,
- Yönetim tarafından belirlenen politika, yönerge ve uygulamalara uygunluğu tespit etmek,
- İşletmedeki hata veya hilelerin ortaya çıkarmak,
- Faaliyet ve uygunluk denetimlerinin yürütmek,
- Yönetimin istediği özel denetimleri gerçekleştirmektir.

2.1.2.1.3. Kamu denetimi

Kamu kurumlarına bağlı olarak çalışan ve kamu yararını gözeterek görev yapan kişilerin yaptıkları denetimlere kamu denetimi adı verilir. Kamu denetimi, kamu kurum ve kuruluşları ile özel sektör işletmelerinin kamu tarafından görevlendirilmiş elemanlar tarafından incelenmesidir (Kavut ve diğerleri, 2009: 38).

Kamu denetçileri "…kamusal örgütlere bağlı olarak çalışan…" (Güredin, 2010: 21) denetçilerdir. Çeşitli devlet kurumları içinde kurulup örgütlendirilmiş olan bu denetim birimleri kamu ve özel işletmelerin yasalara, yönetmeliklere, devletin ekonomik politikasına ve kamu yararına bağlılık derecesini izler ve denetler. Tarafsız ve objektif davranmakla birlikte kamu yararı ön planda tutularak denetim faaliyeti yürütülür.

Kamu denetimi yapan bazı kamu denetçileri aşağıda sıralanmıştır:

- Sayıştay Denetçileri
- Vergi müfettişleri
- SPK Denetçileri
- BDDK Denetçileri
- SGK Müfettişleri

2.1.2.2. Amaçlarına göre denetim türleri

Denetim; denetim çalışmasının ne amaçla yapıldığına veya denetimin konusunun ne olduğuna göre de sınıflandırılabilmektedir. Denetim faaliyeti ile ulaşılmak istenen amaca göre denetim türleri; finansal tablolar denetimi, uygunluk denetimi ve faaliyet denetimi olmak üzere üç başlıkta sınıflandırılmıştır. Amaç finansal tabloların bir bütün olarak doğru ve güvenilir olup olmadığını saptamak olduğunda, finansal tablolar denetiminden söz edilir. Denetimle elde edilmek istenen amaç işletme faaliyetlerinin etkin yürütülüp yürütülmediğini, hedeflerini gerçekleştirme derecesini saptamak olduğunda yapılan denetim çalışması faaliyet denetimi olarak tanımlanır. Uygunluk denetiminde ise amaç, belirli bir otorite tarafından belirlenmiş ölçütlere ne ölçüde uyulduğunun tespitidir (Kavut ve diğerleri, 2009: 39).

2.1.2.2.1. Finansal tablolar denetimi

Finansal tablolar denetimi, bir kuruluşun sunmuş olduğu finansal tablolara ilişkin kanıt toplama ve bu kanıtları finansal tablolarda ileri sürülen hususların genel kabul görmüş muhasebe ilkeleri veya diğer kapsamlı muhasebe ilkelerine uygun olup olmadığına karar vermedir (Donald ve William, 1997: 4). "Finansal Tablolar Denetimi" ve "Mali

Tablolar Denetimi" kavramları birbirleri yerlerine kullanılmaktadır ve aynı anlama gelmektedir.

2.1.2.2.2. Uygunluk denetimi

Uygunluk denetimin amacı kuruluşun/kişinin kanunlara ve diğer düzenlemelere uygun davranıp davranmadığının araştırılmasıdır (Donald ve William, 1997: 4). Denetim kriteri kanun, tüzük, yönetmelik gibi yasal otorite tarafından konulan düzenlemeler olabileceği gibi kuruluşu ilgilendiren diğer düzenlemeler de olabilir.

Uygunluk denetimi hem kurum dışı kişiler hem de kurum içi kişiler tarafından yapılır. Kurum dışı kişiler tarafından yapılana en iyi örnek kamu idareleri tarafından yapılan vergi denetimleridir. Banka müfettişleri tarafından bankanın hesap ve işlemlerinin incelenmesi ise kurum içi denetime örnek olarak verilebilir.

2.1.2.2.3. Faaliyet denetimi

Faaliyet denetimi, denetim tanımının geniş kapsamı içinde değerlendirilir. Yönetimin iddialarının değerlendirilmesindeki denetim kriteri diğer denetim kriterlerinden farklıdır. Amerikan Yeminli Mali Müşavirler Enstitüsü'ne (AICPA) göre faaliyet denetimi; performans ölçümü, gelişme fırsatlarını yakalama, gelişme için öneriler getirme veya diğer amaçlar için sistematik olarak kurumsal faaliyetlerinin incelenmesidir (Donald ve William, 1997: 4). Faaliyet denetimi, kuruluşun organizasyon yapısını, iş akışlarını ve yönetim performansını tespit etmeye yönelik geniş kapsamlı bir inceleme faaliyetidir. Kuruluşun finans, pazarlama, satın alma, araştırma geliştirme ve insan kaynakları gibi bölümlerinin işletme politikalarına ne düzeyde uygun davrandığının incelenmesi de faaliyet denetiminin konusunu oluşturur.

2.2. Mali Tablolar Denetimi

"Finansal Tablolar Denetimi" ve "Mali Tablolar Denetimi" kavramları birbirleri yerlerine kullanılmaktadır ve aynı anlama gelmektedir.

Mali tablolar denetimi, “Bir kuruluşun sunmuş olduğu finansal tablolara ilişkin kanıt toplama ve bu kanıtlarla finansal tablolarda ileri sürülen hususların genel kabul görmüş muhasebe ilkeleri veya diğer kapsamlı muhasebe ilkelerine uygun olup olmadığına karar vermedir.” (Donald ve William, 1997: 4).

Ülkemizde faaliyet gösteren bağımsız denetim firmalarından KPMG firmasının mali tabloların denetimine ilişkin tanımı şöyledir; “Mali tablolar denetimi bir şirketin finansal tablo ve dipnotlarının Uluslararası Finansal Raporlama Standardı (UFRS), Amerikan Sistemine göre Genel Kabul Görmüş Muhasebe Standartları (US GAAP) veya regülatörlerin yayımlamış olduğu standartlara uygun olup olmadığı konusunda görüş verilmesini içermektedir” (www.kpmg.com.tr, 2014).

Mali tablolar denetimi bağımsız denetçiler tarafından gerçekleştirilmektedir. “Finansal tabloların bir bağımsız denetçi tarafından denetlenmesinin amacı; işletmenin finansal durumunu, faaliyet sonuçlarını ve finansal durumundaki değişiklikleri dürüst bir biçimde ve genel kabul görmüş muhasebe ilkelerine veya UFRS‘ye (Uluslararası Finansal Raporlama Standartları-International Financial Reporting Standards-IFRS) uygun olarak sunduğuna dair bir görüş sunulmasıdır.” (Jancura, 1974: 2).

Bir özel sektör kuruluşunun mali tablolar denetimi ile kamu sektörü kuruluşunun mali tablolar denetimi özü itibariyle aynı olmakla birlikte kamu sektörü kuruluşunun denetimi bir takım farklılıklar da içermektedir. Uluslararası Yüksek Denetim Kurumları Teşkilatı (INTOSAI) ’nin bir meslek standardı olan Uluslararası Yüksek Denetim Kurumları Standartlarından (ISSAI) 1003 No.lu standarda göre bu fark şöyledir:

“Bir özel sektör kuruluşunun mali denetimi söz konusu olduğunda denetimin amacı, bir dizi beyana dayalı olarak bir güvence görüşü bildirmekle sınırlıdır. Diğer yandan kamu sektöründe yapılan mali denetimin amacı, genelde mali tabloların önemli olan tüm açılardan ilgili mali raporlama çerçevesine uygun olarak hazırlanıp hazırlanmadığı konusunda görüş bildirmekten daha geniş kapsamlıdır. Mevzuat, yönetmelikler, bakanlık talimatları, hükümetin politika şartları ve yasama kararlarından doğan denetim yetki ve görevi veya kamu kurumlarına yönelik yükümlülükler daha başka amaçlar doğurabilir” (ISSAI 1003).

Bağımsız denetim Amerika Birleşik Devletleri ve Avrupa Birliği üyesi ülkelerde halka açık işletmeler için zorunludur. Kuzey Amerika Gümrük Anlaşması'nı (NAFTA) imzalayan ülkelerde bağımsız denetim Amerikan Genel Kabul Görmüş Muhasebe İlkeleri'ne (US GAAP) göre yapılırken; AB'de bağımsız denetim, finansal tabloların UFRS'ye göre gerçeğe uygun ve dürüst olarak sunulup sunulmadığını değerlendirecek şekilde yapılmaktadır.

Türkiye'de mali tablolar denetimi kamu sektöründe ve özel sektörde farklı kurumlar tarafından gerçekleştirilmektedir. Düzenlilik denetimleri kapsamında gerçekleştirilen kamu sektöründeki mali tablolar denetimi Sayıştay Başkanlığı tarafından gerçekleştirilirken özel sektörde bu denetimler bağımsız denetim firmalarınca gerçekleştirilmektedir.

Mali tablolar denetimi yanında bu bölümde güvence hizmetlerinden de bahsetmek gerekir. Güvence hizmeti kavramı denetim kavramından daha geniş kapsamlı bir kavramdır. Mali tablolar denetimi sadece ilgili karar vericilere mali tablolara ilişkin bir güvence sunar. Güvence hizmetleri bilginin kalitesini, kapsamını geliştirerek karar vericilere bağımsız profesyonel hizmet sunar. Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü'ne (AICPA) göre "güvence hizmeti karar vericiler için bilginin kalitesini ve kaynağını geliştiren bağımsız profesyonel hizmetlerdir" (AICPA,1997). Uluslararası Muhasebeciler Birliğine göre (IFAC) güvence hizmeti, belli bir kritere göre denetim konusunun çıktıları üzerinde denetçinin veya uygulayıcının bilginin kullanıcılarının güven derecesini arttırmak üzere görüş beyan etmesidir. Güvence hizmeti sözleşmeleri birçok değişik şekil ve kapsamlarda olabilir: Firmanın finansal performansı ve genel durumu hakkında olabileceği gibi finansal olmayan hususlara ilişkin de olabilir. Bu anlamda finansal tablolar denetimi bağımsız denetçiler tarafından gerçekleştirilen bir güvence hizmeti de sayılabilir.

2.3. Bilgi Teknolojileri Denetimi

"Bilişim sistemleri denetimi, bilgisayar sistemlerinin varlıkları koruyup korumadığını, veri bütünlüğünü sağlayıp sağlamadığını, örgütsel hedeflere etkin şekilde ulaşılmasına yardımcı olup olmadığını ortaya koyan ve kaynakların verimli kullanıp kullanmadığını

belirlemek için kanıt toplayan ve değerlendiren sistematik bir süreçtir. Bilişim sistemleri denetimi geleneksel denetim hedeflerini destekler.” (Weber, 2013: 35).

Bilgi sistemleri kullanımının iş hayatında yaygınlık kazanması bilgi teknolojileri (BT) denetimi konusunu ön plana çıkarmıştır. Finansal tablolar ve diğer finansal veriler işletmelerin bilgisayar sistemlerinin bir çıktısıdır. Dolayısıyla finansal tablo denetiminde bilgi sistemlerinin göz ardı edilmesi denetimin güvenilirliğini zedeleyecektir. “Başarılı bir denetim yapılabilmesi için iç kontrollere yönelik uygulama kontrolleri gibi ayrıntılı kontrollerin yapılması gerekmektedir. İşletmelerin iç kontrollerinin gözden geçirilmesi ve bilgi sistemlerinin değerlendirilmesi için asıl gerekli olan bilgi teknolojileri denetimidir.” (Weber, 2013: 37). Bağımsız denetçiler mali denetim sürecinde iç kontrollerin etkinliğine göre denetim yaklaşımı belirlemekte ve hesap alanları ve örnekleme kararlarını vermektedirler.

İç denetim ve bağımsız denetimin kapsam ve amaçları farklı olmasına rağmen hem iç denetçiler hem de bağımsız dış denetçiler bilgi teknolojilerinin denetiminde benzer faaliyetler yürütmektedir. Mali denetim ve bilgi teknolojileri denetimi arasındaki ilişkinin incelendiği bu bölümde denetçi kavramı hem bağımsız dış denetçiyi hem de iç denetçiyi kapsayacak şekilde kullanılmıştır. Her ne kadar bağımsız dış denetim ve iç denetim uygulama benzerlikleri gösterseler de amaç, kapsam ve uygulanan yöntemler bakımından farklıdırlar. Buna karşın, bir kuruluşun iç denetçileri ile bağımsız denetçileri arasında yoğun bir iş birliği ve etkileşim söz konusu olmaktadır. İç denetçiler işletmenin finansal tablolarını değerlendirirken genellikle dış denetçilerin gerçekleştirdiği denetimleri dikkate almaktadırlar. Dış denetçiler de iç denetim raporlarından yararlanırlar.

“Bilgi sistemleri ve bilgi teknolojilerinin denetçiler tarafından değerlendirilmesi, bilgi sistemleri denetimi kavramını doğurmaktadır. Bilgi teknolojileri denetimi ise, bir işletmenin bilgilerinin doğruluğunun tasdik edilmesi için o işletmenin bilgi sistemlerinin, uygulamalarının ve işlemlerinin değerlendirilmesinden ibarettir. Bu değerlendirme bilgisayar tabanlı uygulamaların verimliliği, etkinliği ve ekonomikliğinin belirlenmesini ve bilgisayarın bir denetim aracı olarak kullanılmasını da kapsamaktadır. Ayrıca değerlendirmede geçerli, yeterli, güvenilir bilgi sistemlerinin tasdiki yapılırken, bilgi

teknolojileri ortamındaki iç kontrollerin yeterliliği de denetlenmektedir.” (Yalkın, 2011: 27).

İç ve dış denetimde bilgi teknolojilerinin denetimi önemlilik taşımaktadır. İç denetim kapsamında yapılacak bilgi teknolojileri denetimi ile dış denetim kapsamında yapılacak bilgi teknolojileri denetimi taşıdığı amaçlar ve kapsam bakımından farklılık gösterir. Şöyle ki iç denetim kapsamında yapılacak bir bilgi teknolojileri denetimi tüm bilgi teknolojileri alanlarını ve bileşenlerini kapsadığı halde dış denetim kapsamında yapılacak bir bilgi teknolojileri denetimi sadece mali tabloların üretilmesinde kullanılan sistem ve teknolojileri kapsayacaktır.

2.3.1. BT denetimine ilişkin uluslararası standartlar

Objektif ve kabul edilebilirliği yüksek bir denetim raporu için BT denetçisinin BT denetim standartlarına uygun denetim gerçekleştirmesi gerekir. 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, Bilgi Teknolojileri İçin Kontrol Hedefleri anlamına gelmektedir ve Bilgi Sistemleri Denetimi ve Kontrolü Birliği (ISACA) tarafından yayınlanmaktadır. COBIT iş riskleri, kontrol ihtiyaçları ve teknik hususlar arasında köprü vazifesi görür. Bir alan ve süreç çerçevesinden iyi uygulamalar sağlar ve yönetilebilir aktiviteler ve mantıksal yapı sunar. COBIT ilk kez Nisan 1996’da yayınlanmıştır. COBIT 4.0, COBIT 3 üncü baskının geliştirilmesidir ve düzenleyicilere uyumu vurgulamış, BT tarafından kazandırılan değerlerin artması için organizasyonlara yardım etmiş, aynı görüşü benimsemeyi sağlamış ve COBIT çerçevesinin uygulanmasını basitleştirmiştir. Mayıs

2007'de COBIT 4.1 versiyonu yayınlanmıştır. COBIT 5.0 Haziran 2012'de yayınlanmıştır. RISK IT, Val IT ve COBIT 4.1 çerçevelerini içermekte ve Bilgi Teknolojilerinde Kurumsal Yönetişim kavramı üzerinde yoğunlaşmaktadır.

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

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.

ITILv3 (Bilişim Teknolojileri Altyapı Kütüphanesi): BT hizmet yönetiminin kurumsal ihtiyaçlara cevap verecek şekilde planlanması, yürütülmesi, ölçülmesine ilişkin standartları ve iyi uygulama örneklerini ortaya koyan konusunda dünya genelinde en fazla kabul görmüş yaklaşımdır. Dünyada ileri gelen birçok özel şirket ve kamu kurumunca kullanılan ITIL, BT hizmetlerinin verimliliğini artırmak, maliyetleri düşürmek, üçüncü taraflardan hizmet alımından uygun değer 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 ITIL çerçevesine başvurabilir.

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.

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

2.3.2. Bilgi Teknolojisi Denetimine İlişkin Mesleki Örgütler

Bilgi teknolojileri denetimine ilişkin uluslararası mesleki örgüt ISACA'dır. ISACA-Uluslararası Sistem Denetimi ve Kontrol Birliği (International Systems Audit and Control Association-ISACA) elektronik veri süreçlerini denetleyen ve bilgisayar sistemlerini kontrol eden bir grup tarafından 1967 yılında kurulmuştur. Birliğin görevi, kurumsal ve sistem kontrollerini denetleyen denetçilerin mesleki yeterliliklerini geliştirmek ve desteklemektir. Ayrıca, 1969 yılında; Elektronik Veri Süreçleri Denetçileri Birliği (Electronic Data Processes Auditors Association) kurularak bilgi teknolojileri denetimi alanında bilgi kaynağı ve rehberlik sağlayacak bir kuruluş oluşturulmuştur.

Günümüzde ISACA'nın, sayısı 110.000'e ulaşan ve 180 ülkede faaliyet gösteren üyesi bulunmaktadır. Üyeler; bankacılık, finans, muhasebe, üretim ve kamu gibi çeşitli sektörlerde çalışan bilgi sistemi denetçileri, bilgi sistemi güvenlikçileri, danışmanlar, iç denetçiler ve eğitimciler gibi profesyonellerden oluşmaktadır. ISACA'nın 80 ülkede faaliyet gösteren birimi bulunmaktadır. Bu birimlerde ISACA yerel düzeyde eğitim düzenlemekte ve bilgi teknolojileri araştırma projeleri yürütmektedir. ISACA'nın yayınladığı denetim ve kontrol standartları dünya genelinde kabul görmektedir. Bu nedenle ISACA'nın Sertifikalı Bilgi Sistemleri Denetçisi (CISA), Sertifikalı Bilgi Sistemleri Yöneticisi (CISM) ve Sertifikalı Bilgi Güvenliği Yöneticisi (CGEIT) gibi çeşitli meslek unvanları vermek için düzenlediği sınavlar bulunmaktadır. Ayrıca ISACA bilgi kontrolü alanında periyodik bir bilimsel dergi yayınlamaktadır (www.isaca.org, 2014).

2.3.3. Bilgi Teknolojileri Denetimi ve COBIT Çerçevesi

Teknolojinin yoğun olarak kullanıldığı günümüzde iç kontrol sistemlerinin denetimi konusu önemli hale gelmiştir. Ortaya çıkan denetim skandalları, BT kontrolleri ve BT güvenliği konusunda bir çerçevenin ortaya konulmasını gerektirmiştir. BT kaynaklarının işletme gereksinimleri dikkate alınarak etkinlik, verimlilik, gizlilik, mevcudiyettik, bütünlük, güvenilirlik, uyum, bilginin güvenilirliği gibi konulara etkisi COBIT çerçevesinde ele alınmıştır. COBIT çerçevesinde öne sürülen süreçler bilgi teknolojilerine yönelik kontrolleri ele alan herkese açık olan standartlardır ve BT

Yönetişim Enstitüsü tarafından geliştirilmekte ve yayınlanmaktadır. Türkiye'de Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından yayınlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" uyarınca bankalara COBIT'te yer alan usul ve esaslar uygulanması zorunludur.

COBIT iç kontrol sürecinde iç ve dış denetçiler için aşağıdaki gibi bir yol haritası sunmaktadır (Soltani, 2007: 423):

1. ***Plan ve Kapsam***: Finansal raporlama süreci, genel kabul görmüş muhasebe ilke ve standartlarına uyum, yolsuzluğu önlemeye ilişkin programlar ve kontroller konusunda BT rolü belirlenir.

2. ***Belirlenmiş BT bileşenleri üzerinde risk değerlendirmesinin yapılması***: Potansiyel risklerin belirlenmesi ve gerçekleşmesi durumunda olası sonuçları ve etkileri değerlendirilir.

3. ***Önemli hesap alanları ve kontrollerinin belirlenmesi:*** Önemli hesap alanlarına ilişkin uygulama kontrollerinin belirlenmesi ve belgelenmesini içerir.

4. ***Belge kontrolü tasarımı:*** Belgeler elektronik ortamda olabileceği gibi kağıt ortamında basılı da olabilir ve süreç modelleri, prosedürler, görev tanımları gibi bilgiler içerir.

5. ***Kontrol tasarımlarının değerlendirilmesi:*** Değerlendirme kontrol risklerinin kabul edilebilir seviyede olup olmamasının tespitini içerir. Bunlar için atanmış kontrollerin riskleri önleyiciliği, tespit edici yönleri araştırılır, manuel veya otomasyon sistemlerin kullanımı belirlenir.

6. ***Operasyonel etkinliğin değerlendirilmesi:*** Kontrollerin işleyip işlemediği test edilir.

7. ***Eksikliklerin belirlenmesi ve düzeltilmesi:*** BT kontrolleri önemli zafiyetler içeriyorsa bunların mali veriler üzerindeki etkileri ve boyutları ortaya konur.

8. ***Belgeleme süreci ve sonuçlar:*** Test sonuçları değerlendirme süreci boyunca belgelendirilir ve kayıt edilir.

9. ***Sürdürülebilirliğin kurulması:*** BT yönetimi, BT iç kontrol programının etkin bir şekilde yürütülmesini desteklemelidir. Kontrol değerlendirmeleri ve yönetimin yetkinliği BT örgütlenmesinin ve kültürünün bir parçası olmalı ve uzun dönemde sürdürülmelidir."

2.3.3.1. COBIT prensibi

Kuruluşların iş hedeflerini ve gereksinimlerini karşılayacak bilgilerin üretimi ve aktarımının hızlı, sürekli ve güvenli olarak sağlanabilmesi için teknoloji kullanımından kaynaklanan risklerin belirlenmesi, yönetimi ve kontrolünün etkin ve verimli olarak yapılması gerekmektedir. Kısaca "Teknoloji risklerini nasıl yöneteceğiz ve bağlı oldukları yapıyı daha güvenli hale nasıl getireceğiz?" sorularının yanıtları, sadece bilgi işlem yöneticileri değil, teknoloji yoğun çalışan ve iş süreçlerine teknolojiyi entegre etmiş olan tüm kurumların yöneticileri için önem taşımaktadır. COBIT, bu sorulara sistematik bir yaklaşım sergileyerek ve yönetsel ihtiyaçlara da yanıt verecek şekilde oluşturulmuş bir yöntemdir (Artinyan, 2014: 1).

2.3.3.2. COBIT mimarisi

COBIT'te herhangi bir kurumda yer alabilecek tüm teknoloji süreçlerini kapsayan yapısı içerisinde 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. BT Yönetişim Enstitüsü COBIT'in oluşturulmasında tüm en iyi uygulamalar ve standartları (COSO, ISO 9000, Spice, CMM, ITIL, BSI7799 vb.) referans olarak ele almış, dünya çapında akademisyen, uzman, danışman ve analistler ile ortak bir çalışma yürütmüştür. COBIT'de yer alan "Yönetim Rehberi-Management Guidelines" içerisinde tüm teknoloji süreçleri için Olgunluk Modeli (Maturity Model), Kritik Başarı Faktörleri (Critical Success Factors), Ana Hedef Göstergeleri (Key Goal

Indicators) ve Ana Performans Göstergelerinin (Key Performance Indicators) tanımlanmış olması sayesinde, 34 süreç dahilinde, organizasyonun hedeflere ulaşma derecesi ölçümlenebilmektedir (Artinyan, 2014: 2).

COBIT, bilgi işlem teknolojilerine dayanan kritik iş süreçlerini desteklemeyi hedeflemektedir. 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. 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: (Artinyan, 2014: 3)

- 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 ulaşamamamızın 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.

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 Izleme ve Değerlendirme (Monitor and Evaluate) grupları şemsiyesindeki süreçlerin, En Iyi 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 teknolojiden dünya standartlarında faydalanması, iş geliştirme fırsatları yaratması, risklerini minimize etmesi ve teknolojinin sağladığı rekabet avantajını güçlendirmesi hedeflenmiştir. COBIT'in uygulamaya geçirilmesinin yönetsel amaçları şunlardır (Artinyan, 2014: 4):

- Varlıkların korunması: Sadece BT Denetiminin değil, her türlü denetimin en temel amacı kurumsal varlıkların korunmasıdır. Burada daha çok bankanın bilgi kaynakları, insan kaynakları ve teknoloji yatırımları varlık olarak ele alınmaktadır. Varlıkların korunması amacı sadece koruma ile ilgili gereksinimleri yerine getirmek değil, bu varlıkların araştırılması, seçimi, değerlendirmesi, elde edilmesi ve kullanıma sokulması gibi varlıkla ilgili her aşamada kullanılan kaynakların (mali kaynaklar, insan gücü, zaman...) kaybını da önlemek anlamına gelmektedir.
- Bilginin Doğruluk ve Bütünlüğü (Data Integrity): Bilginin tam, hatasız veya bozuk olmaması, doğru olarak ele alınması, doğru saklanması ve gerçek dünya ile uyum göstermesi anlamındadır. Ayrıca datanın bozulmamış; doğru ve tam kodlanmış ve doğru ve tam geçişinin yapılmış olduğunu belirlemek.
- Etkinlik Denetimi
- Verimlilik Denetimi

2.3.3.3. Olgunluk modelleri

Bilgi teknolojilerinin iş hayatındaki önemi arttıkça, oldukça yüklü yatırım ve riskli proje yönetimlerini gerektiren bilgi teknolojileri süreçlerinin olgunluk seviyeleri hakkında güvence sağlayacak denetim metodolojilerine olan ihtiyaç da artmaktadır. Bu amaçla COBIT için düzenlenmiş olan olgunluk seviyeleri kurumun bugün nerede olduğunu,

endüstrideki durum ve karşılaştırmalarını ve kurumun ileride nerede olmak istediği sorularına cevap vermektedir. Son zamanlarda COBIT olgunluk seviyeleri hakkında bir sürü spekülasyonun ortaya atılması COBIT 4.1'in ortaya çıkması ile durmuştur. Ana hatları ile COBIT Olgunluk Modellerinin hesaplaması şu şekildedir:

	Anlayış ve Farkındalık	**Eğitim ve İletişim**	**Süreç ve Uygulamalar**	**Teknoloji Kullanımı**	**Uygunluk**	**Uzmanlık**
0	Yok	yok	yok	yok	yok	yok
1	Farkındalık var	İhtiyaç olduğunda münferit iletişim sağlanıyor	İhtiyaç olduğunda münferit dokümantasyon ve süreç yaklaşımı sağlanıyor	yok	yok	yok
2	İhtiyacın bilincine varılmış	Genel konular ve ihtiyaçlar üzerine iletişim sağlanıyor	Ortak / benzer ancak kişi insiyatifinde uygulamalar var	Ortak / benzer araçlar kullanılmaya başlanmış	Münferit durumlarda standart olmayan izleme yöntemleri kullanılıyor	yok
3	Önlem alınması yönünde anlayış oluşmuş	Kişisel girişimler ve bireysel eğitimler mevcut	Prosedürler oluşturulmuş ve dökümante edilmiş, bunların iyileştirilmesine başlanmış	Ortak yöntemlerin kullanılması için standard oluşturulmuş	Standart olmayan izleme ve ölçme yöntemleri kullanılıyor; kurumsal karne uygulaması yapılan alanlar olabiliyor; kişiye bağlı sebep-sonuç ilişkileri gözlenebiliyor	İş süreçlerine teknoloji uzmanlarının da katılımı sağlanıyor
4	Tüm gereklilikler biliniyor	Program yönetimi ve resmi eğitim var	Süreç sahipliği ve sorumlulukları belirlenmiş, süreç olgunluğu sağlanmış, kurum içi en iyi uygulamalara geçilmiş	Teknolojik olgunluğa ulaşılmış, standard yöntemlerin kullanılması sağlanmış	Belirlenen süreçlerde kurumsal karne uygulaması yapılıyor, farklılıklar izleniyor ; sebep-sonuç analizi standard olarak uygulanıyor	Konuyla ilgili tüm uzmanların katılımı sağlanıyor
5	Üst düzey ve ileri görüşlü bir anlayış seviyesi var	İletişim ve eğitim konularında en iyi yöntemler uygulanıyor ve en yeni gelişmeler takip ediliyor	Sektör ve konu ile ilgili en iyi yöntemler uygulanmakta	En gelişmiş teknolojiler uygulanmakta, teknoloji kullanımı optimize edilmiş	Tüm süreçlerde kurumsal karne uygulaması yapılıyor, farklılıklar izleniyor ve iyileştirici önlemler alınıyor; sebep-sonuç analizi her durumda yapılıyor	Yabancı uzmanların ve endüstri liderlerinin danışmanlığı alınıyor

Şekil 2.1. COBIT olgunluk modellerinin hesaplaması (Artinyan, 2014: 5)

2.3.4. Bilgi teknolojileri denetimi ile ilgili Türkiye'deki mevzuat ve düzenlemeler

Ülkemizde bankalarda kullanılan yazılım ve donanımın, bilgi sistemi süreçlerinin, mali veri üretiminde kullanılan bilgi sistemi ve süreçlerinin ve ilgili iç kontrollerin değerlendirilmesi amacıyla Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından bilgi sistemleri denetimine ilişkin yönetmelik çıkarılmıştır. Bu yönetmelikle BT denetimi bankacılıkta yasal bir zorunluluk haline gelmiştir.

Uzman sistemleri ve denetim personelini elde tutmanın maliyeti çok yüksek olduğu için pek çok kuruluş, BT denetimini dışarıdan bir firmaya vermeyi veya dışarıdan bir firmayla ortak yürütmeyi tercih etmektedir. BDDK tarafından da bu denetim hizmetinin bağımsız denetim kuruluşlarınca yapılması öngörülmüştür. Basel II düzenlemeleri ve yeni Türk Ticaret Kanunu ile birlikte tüm işletmeler için bilgi güvenliği kurumsal yönetim kalitesi açısından önem kazanmıştır, yasal yükümlülüklerin yanı sıra işletmelerin kurumsal derecelendirmelerinde temel değerlendirme faktörlerinden birini oluşturmaktadır.

2.3.4.1. BDDK mevzuatı

Bilgi Sistemleri ve bankacılık süreçlerine ilişkin BDDK tarafından çıkarılan düzenlemeler:

- Yönetmelikler
    - Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik
- Tebliğler
    - Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ
    - Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Tebliğ

- Genelgeler

    - Bilgi Sistemlerine İlişkin Sızma Testleri Hakkında Genelge
    - Yönetim Beyanına İlişkin Genelge (2010/3)
    - Bağımsız Denetim Takip Sistemine (BADES) ilişkin genelge
    - ATM'lerde Kimlik Doğrulamaya İlişkin Genelge
    - Bilgi Sistemleri Denetimlerinde Tespit Edilen Bulguların Kodlanması Hakkında Genelge

Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliğe göre;

Bankalar ile bilgi sistemleri ve bankacılık süreçlerinin denetimine ilişkin rapor oluşturulması amacıyla sınırlı olmak üzere konsolidasyon kapsamındaki ortaklıkları, bankalara bilgi sistemleri hizmeti veren destek hizmeti kuruluşları, bilgi sistemleri ve bankacılık süreçlerinin denetimini yapmaya yetkili kuruluşlar, bağımsız denetim kuruluşları ve dış hizmet sağlayıcı kuruluşlar bankaların bilgi sistemleri ile bankacılık süreçlerinin denetlenmesi kapsamında bu yönetmelik hükümlerine tabidir.

Bilgi sistemleri ve bankacılık süreçleri denetimi (BSD); 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. BSD'nin temel amacı denetlenenin bilgi sistemleri ve bankacılık süreçlerinin ve bu sistem ve süreçlere ilişkin iç kontrollerinin uyumluluk, etkinlik ve yeterliliği hakkında görüş oluşturulmasıdır.

2.3.4.1.1. Bankacılık bilgi sistemleri denetimi

Bilgi sistemleri denetiminde denetçi, bilgi sistemleri genel kontrollerini, önemlilik kriterini esas alarak belirlediği kapsam dâhilinde uyumluluk, etkinlik ve yeterlilik açısından incelemeye tâbi tutar. Genel kontroller, tesis edilmelerinde esas alınan çerçeve, standart ya da metodolojiden bağımsız olarak; bankalarda bilgi sistemleri

yönetiminde esas alınacak ilkelere ilişkin BDDK tarafından yapılan düzenlemelerdeki hükümler gözetilerek, COBIT'e göre denetlenir.

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.

2.3.4.1.2. Bankacılık süreçleri denetimi

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.

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. (Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik, 2010, s. Md.25):

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.

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 dahil eder, etkinlik ve yeterlilikleri ile bankacılık süreçleri üzerindeki kontrollere olan etkilerini değerlendirir.

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.

2.3.4.1.3. İç kontrol ve iç denetim sistemine ilişkin değerlendirme

Denetçi, bilgi sistemleri genel kontrolleri ve bankacılık süreçleri üzerindeki kontrollerle sınırlı olmak üzere denetlenenin iç kontrol ve iç denetim sistemleri bünyesinde yürüttüğü çalışmalarını önemlilik kriteri çerçevesinde değerlendirir. Bu kapsamda; (Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik, 2010: Md.26)

a) İç kontrol sistemine ilişkin yürütülen faaliyetler incelenirken asgari olarak:

1. Kontrol ortamına ilişkin hususlar,
2. Yönetim tarafından etkin ve yeterli bir iç kontrol sisteminin tesis edilmesi, işletilmesi ve gözetimine ilişkin benimsenen yaklaşım ve uygulaması,
3. Kanunun 75 inci maddesinde çerçevesi çizilen etik ilkelerin uygulanması ve çalışanların bu konudaki farkındalık düzeyi

dikkate alınır.

b) İç denetim biriminin iç kontrol sisteminin etkinlik, yeterlilik ve uyumluluğunun gözetimine ilişkin yürüttüğü faaliyetler ve performansını değerlendirir.

c) İç denetim biriminin değerlendirilmesi kapsamında denetlenenin bilgi sistemleri denetimi faaliyetleri dikkate alınır. Denetlenenin bilgi sistemleri denetimi fonksiyonu değerlendirilirken asgari olarak;

1. Ekibin organizasyon içerisindeki yeri ve bağımsızlığı,

2. Ekibi oluşturan personelin nitelik ve sayı açısından yeterliliği,
3. Planlanan ve gerçekleştirilen denetim çalışmaları,
4. Denetim sonuçlarının takibi

incelenir.

ç) Denetçi, denetlenenin iç kontrol sistemine ilişkin risk değerlendirme sürecinde yürütülen faaliyetler ve performansını değerlendirir.

2.3.4.1.4. Bilgi sistemleri ve bankacılık süreçleri denetimi faaliyetlerinin yürütülmesi

BSD faaliyetlerini gerçekleştirilebilmesi için bağımsız denetim kuruluşunun yönetmelik kapsamında; denetim yapma yetkisini haiz olması ve denetlenenle denetim sözleşmesi yapmış olması gereklidir.

Yetkili kuruluşlar, bilgi sistemleri ve bankacılık süreçleri denetiminin gerçekleştirileceği dönemde, denetlenenin bağımsız denetim faaliyetini de yürütüyor olmak zorundadırlar.

Bankacılık süreçleri denetimi, yetkili kuruluş tarafından bu faaliyeti yürütmekle görevlendirilen finansal denetçi tarafından, bilgi sistemleri denetçisi ile birlikte gerçekleştirilir.

2.3.4.2. Türk Ticaret Kanunu

6102 sayılı Türk Ticaret Kanunu 14.02.2011 tarih ve 27846 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Mevzuatta yapılan bu düzenleme ile 01.01.1957 tarihinde yürürlüğe girip uzun yıllar uygulanan 6762 sayılı Eski Türk Ticaret Kanunu yürürlükten kalkmış bulunmaktadır.

6102 sayılı TTK, sadeleştirilmiş dili ve içerdiği hükümler açısından 6762 sayılı TTK‘dan önemli farklılıklar içermesinin yanında bilgi teknolojileri dahil birçok açıdan yenilenmiştir. Söz konusu kanun BT denetimine ilişkin bir zorunluluk getirmese de sermaye şirketlerinde BT konusunu önemli hale gelmektedir.

6102 sayılı Kanunun “Elektronik işlemler ve bilgi toplumu hizmetleri” bölümünün “İnternet sitesi” başlıklı 1524 üncü maddesi her sermaye şirketine bir internet sitesi açma veya şirketin internet sitesi zaten mevcutsa bu sitenin belli bir bölümünü aşağıdaki hususların yayımlanmasına özgülemek zorundadır:

- Pay sahibini, küçük yatırımcıyı, alacaklıyı ve şirkette menfaati olan kişileri ilgilendiren şirket ile ilgili tüm bilgileri,
- Genel kurul toplantısı belgeleri ve çağrıları,
- Yılsonu ve ara dönem finansal tabloları ile özel amaçlarla çıkarılan bilançolar ve diğer finansal tablolar, pay ve menfaat sahipleri bakımından bilinmesi gerekli finansal raporlamalar, bunların dip notları ve ekleri,
- Birleşme ve bölünme bilançoları,
- Denetleme raporları,
- Değerleme raporları,
- Rüçhan hakkı kullanma çağrıları,
- Tasfiyeye ilişkin ilanlar,
- İptal davası ilanları,
- Şeffaflık ilkesi ve bilgi toplumu açısından açıklanması zorunlu bilgileri,
- Bilgi alma kapsamında sorulan sorular ve bunlara verilen cevaplar ile pay sahiplerinin veya ortakların aydınlatılması için diğer kanunlarda öngörülen hususları,
- Yönetim kurulu başkanına ve üyelerine ve şirket yöneticilerine ödenen her türlü paralar, temsil ve seyahat giderleri, tazminatlar, sigortalar ve benzeri ödemeleri,
- Pay sahiplerini ve sermaye piyasasını ilgilendiren konulara ilişkin yetkili kurul ve bakanlıkların konulmasını istedikleri bilgileri koyma zorunluluğu getirilmiştir

İnternet sitesinin bilgi toplumu hizmetlerine ayrılmış bölümü herkesin erişimine açıktır. Erişim hakkının kullanılması, ilgili olmak veya menfaati bulunmak gibi kayıtlarla sınırlandırılamayacağı gibi herhangi bir şarta da bağlanamaz. Bu ilkenin ihlali hâlinde herkes engelin kaldırılması davasını açabilir.

İnternet sitesinin bu maddenin amaçlarına özgülenmiş kısmında yayımlanan içeriğin başına tarih ve parantez içinde “yönlendirilmiş mesaj” ibaresi konulur. Bu ibareli mesaj ancak Kanuna ve ikinci fıkrada anılan yönetmeliğe uyulmak suretiyle değiştirilebilir. Özgülenen kısımda yer alan bir mesajın yönlendirildiği karinedir. Sitenin, bir numara altında tescili ve ilgili diğer hususlar Sanayi ve Ticaret Bakanlığı tarafından bir yönetmelikle düzenlenir.

Bu Kanun ve ilgili diğer kanunlarda veya idari düzenlemelerde daha uzun bir süre öngörülmedikçe, şirketin internet sitesine konulan bir içerik, üzerinde bulunan tarihten itibaren en az altı ay süreyle internet sitesinde kalır; aksi hâlde konulmamış sayılır. Finansal tablolar için bu süre beş yıldır.

Yönlendirilmiş mesajların basılı şekilleri TTK’ nın 82 nci madde uyarınca saklanır. İnternet sitesinde yer alacak bilgiler metin hâline getirilip şirket yönetimi tarafından tarih ve saati gösterilerek noterlikçe onaylı bir deftere sıra numarası altında yazılır veya yapıştırılır. Daha sonra sitede yayımlanan bilgilerde bir değişiklik yapılırsa, değişikliğe ilişkin olarak yukarıdaki işlem tekrarlanır.

Kanunun “Beyanlar, belgeler ve senetler” başlıklı 1525 inci maddesine göre;

Tarafların açıkça anlaşmaları ve 18 inci maddenin üçüncü fıkrası saklı kalmak şartıyla, ihbarlar, ihtarlar, itirazlar ve benzeri beyanlar; fatura, teyit mektubu, iştirak taahhütnamesi, toplantı çağrıları ve bu hüküm uyarınca yapılan elektronik gönderme ve elektronik saklama sözleşmesi, elektronik ortamda düzenlenebilir, yollanabilir, itiraza uğrayabilir ve kabul edilmişse hüküm ifade eder.

Kanunun “Güvenli elektronik imza” başlıklı 1526 ncı maddesine göre;

Konişmentonun, taşıma senedinin ve sigorta poliçesinin imzası elle, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla da atılabilir. Düzenlendikleri ülke kanunlarının izin verdiği ölçüde bu senetlerde yer alacak kayıtlar el yazısı, telgraf, teleks, faks ve elektronik diğer araçlarla yazılabilir, oluşturulabilir, gönderilebilir.

Ticaret şirketleri ile gerçek ve tüzel kişi diğer tacirlere ilişkin olarak, bu Kanunun zorunlu tuttuğu bütün işlemler elektronik ortamda güvenli elektronik imza ile de yapılabilir. Bu işlemlerin dayanağı olan belgeler de aynı usulle elektronik ortamda düzenlenebilir. Zaman unsurunun belirlenmesi gereken ve tüzükte düzenlenen hâllerde güvenli elektronik imzaya eklenen zaman damgasının tarihi, diğer hâllerde merkezî veri tabanı sistemindeki tarih esas alınır.

Şirket adına imza yetkisini haiz kişiler şirket namına kendi adlarına üretilen güvenli elektronik imzayla imza atabilirler. Bu durumda, kullanılacak nitelikli elektronik sertifikalarda sertifika sahibi alanı içerisine, sertifika sahibinin ismiyle birlikte temsil ettiği tüzel kişinin de ismi yazılır. Bu husus tescil ve ilan edilir.

Kanunun “Elektronik ortamda kurullar” başlıklı bölümünün 1527 nci maddesine göre;

Şirket sözleşmesinde veya esas sözleşmede düzenlenmiş olması şartıyla, sermaye şirketlerinde yönetim kurulu ve müdürler kurulu tamamen elektronik ortamda yapılabileceği gibi, bazı üyelerin fiziken mevcut bulundukları bir toplantıya bir kısım üyelerin elektronik ortamda katılması yoluyla da icra edilebilir. Bu hâllerde Kanunda veya şirket sözleşmesinde ve esas sözleşmede öngörülen toplantı ile karar nisaplarına ilişkin hükümler aynen uygulanır.

Kollektif, komandit, limited ve sermayesi paylara bölünmüş şirketlerde, şirket sözleşmesinde ve esas sözleşmede öngörülerek elektronik ortamda ortaklar kuruluna ve genel kurula katılma, öneride bulunma ve oy verme, fizikî katılımın, öneride bulunmanın ve oy vermenin bütün hukuki sonuçlarını doğurur.

Birinci ve ikinci fıkrada öngörülen hâllerde, elektronik ortamda oy kullanabilmek için, şirketin bu amaca özgülenmiş bir internet sitesine sahip olması, ortağın bu yolda istemde bulunması, elektronik ortam araçlarının etkin katılmaya elverişliliğinin bir teknik raporla ispatlanıp bu raporun tescil ve ilan edilmesi ve oy kullananların kimliklerinin saklanması şarttır.

Birinci ve ikinci fıkrada anılan şirketlerde esas sözleşme veya şirket sözleşmesi gereği şirket yönetimi, bu yolla oy kullanmanın bütün şartlarını gerçekleştirir ve ortağa gerekli bütün araçları sağlar.

Anonim şirketlerde genel kurullara elektronik ortamda katılma, öneride bulunma, görüş açıklama ve oy verme, fizikî katılmanın ve oy vermenin bütün hukuki sonuçlarını doğurur. Bu hükmün uygulanması esasları bir tüzük ile düzenlenir. Tüzükte, genel kurula elektronik ortamda katılmaya ve oy vermeye ilişkin esas sözleşme hükmünün örneği yer alır. Anonim şirketler tüzükten aynen aktarılacak olan bu hükümde değişiklik yapamazlar. Tüzük ayrıca oyun gerçek sahibi veya temsilcisi tarafından kullanılmasını sağlayan kurallar ile 407 nci maddenin üçüncü fıkrasında öngörülen komiserlerin bu hususa ilişkin yetkilerini içerir. Bu tüzüğün yürürlüğe girmesi ile birlikte genel kurullara elektronik ortamda katılma ve oy kullanma sisteminin uygulanması pay senetleri borsaya kote edilmiş şirketlerde zorunlu hâle gelir.

Kanunun “Uygulama kuralları” başlıklı 1528 inci maddesine göre elektronik ortamı kullanmak isteyen ortaklar, pay sahipleri ve yönetim kurulu üyeleri elektronik posta adreslerini şirkete bildirmek zorundadırlar.

2.3.4.3. Basel II – Operasyonel risk

Operasyonel risk, “Yetersiz ve başarısız içsel süreçlerden, personel ve sistemlerden ya da dışsal olaylardan kaynaklanan, doğrudan veya dolaylı zarar riskidir” (Boyacıoğlu, 2002: 52).

Ülkemizde 2012 yılında BDDK tarafından çıkarılan ve yayınlan ‘Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik’te operasyonel risk “Yetersiz veya başarısız iç süreçler, insanlar ve sistemlerden ya da harici olaylardan kaynaklanan ve yasal riski de kapsayan zarar etme olasılığı” şeklinde tanımlanmaktadır.

Operasyonel riskler; personel riski, teknolojik riskler, organizasyon riski, yasal riskler ve dış risklerden oluşmaktadır. BT denetimi;

- Banka yönetiminin ve personelin yetersizliğinden, ihmalinden, görevlerini unutmalarından ya da kötüye kullanmalarından veya kasıtlı olarak suç sayılan eylemleri gerçekleştirmelerinden kaynaklanan personel risklerini;
- Virüs problemleri, yetersiz ya da güncelliğini yitirmiş sistemlerden kaynaklanan bilgisayar ve iletişim sistemlerindeki teknik sorunlar ve aksamalardan kaynaklanan teknolojik riskleri;
- Örgüt içerisindeki kademeler arasındaki bilgi akışının yetersizliği, yetki sınırlarının kesin olmaması, yapı/işleyiş değişikliklerinden doğan belirsizliklerin neden olduğu organizasyonel riskleri ve
- Deprem, yangın, sel gibi felaketlerden kaynaklanan riskler, banka dışı sahtekarlık olayları, web sitelerinin kötüye kullanımı, enerji kesintisi gibi dış risklerin azaltılmasında önemli rol oynar.

2.4. Bilgi Teknolojileri Denetiminin Gerçekleştirilmesi

Yüzlerce analistin, programcının çalıştığı, birçok bilgisayarın, verinin, sistem ve alt sistemlerin bulunduğu bir kuruluşta BT denetimi yapabilmek ciddi bir tecrübe ve birikimi gerektirir. Yoğun bilgisayar kullanılan çevrelerde denetçilerin veri işleme süreçlerinin tamamını detaylı incelemeleri mümkün değildir. Bu nedenle denetçiler örnekleme yaparak denetimleri için gerekli güvenceyi oluştururlar. “Örnekleme, kontrollerin ve hesap bakiyelerinin yüzde yüz incelenmediğinde başvurulan bir yöntemdir. Bilgisayar ortamındaki veriler için genelleştirilmiş denetim yazılımları geliştirilmiştir (GAS). Bu yazılımlar veriler uygun olduğunda yüzde yüz inceleme yapmaya imkan verir ve denetçinin belli spesifik alanlara yoğunlaşabilmesini sağlar.” (Johnstone ve diğerleri, 2014: 318).

Bilgisayar sistemlerinin ortaya çıkışından beri denetçiler denetimin doğasının değişmesi gerektiği yönünde görüş belirtmişlerdir. Ancak günümüzde bakıldığında böyle bir düşüncenin geçerliliğinin kalmadığı görülmektedir. Bilgisayar sistemlerini yoğun kullanıldığı kuruluşlarda diğer kuruluşlarda olduğu gibi denetçiler ekonomik faaliyetlerin önceden belirlenmiş kriterlere ve standartlara uygun olarak kaydedilmesi ve raporlanması konusunda yeterli çalışma yapıp tarafsız görüş vermek

durumundadırlar. Yani denetçinin gerçekleştirdiği temel fonksiyonlarda bir değişiklik söz konusu değildir.

2.4.1. Kontrollerin Yapısı

ISA 330 No'lu Standarta göre denetçi, risk değerlendirmesinde kontrollerin operasyonel etkinliğine güvendiyse veya maddi doğrulama testleri tek başına yeterli düzeyde denetim kanıtı sunmuyorsa seçilen kontrollerin operasyonel etkinliğini araştırmak zorundadır.

BT denetçilerinin temel hedeflerinden biri kontrollerin güvenli ve etkin şekilde işleyip işlemediğini ortaya koymaktır. Burada kontrol denildiğinde kontrolün ne anlama geldiğinin ortaya konmasında fayda vardır. "Genel olarak kontrol, usulsüz işlemleri önleyen, ortaya çıkaran veya düzelten bir sistemdir." (Weber, 2013: 59). Bu tanımın üç boyutu vardır:

Birincisi, kontrol bir sistemdir. Diğer bir deyişle kontrol birbirleri ile ilişkili, belli bir amacı elde etmeye özgülenmiş bileşenlerden oluşan bir kümedir. Kontrol dendiğinde çoğu zaman kontrolün sadece bir özelliği anlaşılır. Birçok kişi işlemlerinde şifre kullanmaktadır; ancak şifre ve şifreleme tek başına bir kontrol değildir. Şifre sadece yetkili kişilerin verilere ulaşmasını ve işlem yapmasını sağlar. Şifre, bilgisayar sistemi içinde düşünüldüğünde güvenli işlem yapmayı, şifrelemeyi, şifre geçerliliğini, şifrelerin veri tabanında saklanmasını ve devamında korunmasını, kırılamamasını, yetkilisinin dışında değiştirilememesini içeren birçok fonksiyonu bünyesinde barındıran bir kontroldür. Dolayısıyla denetçinin şifre ve şifrelemeye ilişkin bütün boyutları düşünerek değerlendirme yapması gerekir.

İkincisi, kontrolün temel hedefi usulsüz işlemlerdir. Usulsüz işlemler sisteme yetkisiz erişim, hatalı, eksik, gereksiz, geçersiz veri girişi hususlarını içerir. Örneğin veri girişinden sorumlu personel sisteme eksik, hatalı veri girişi yapabilir. Yine sistemin istenmeyen bir duruma sürüklenmesinden kaynaklanan hatalı veri üretimi gerçekleşebilir.

Üçüncüsü, kontroller usulsüz işlemlerin *önlenmesi, ortaya çıkarılması, düzeltilmesinde* kullanılır. Örneğin;

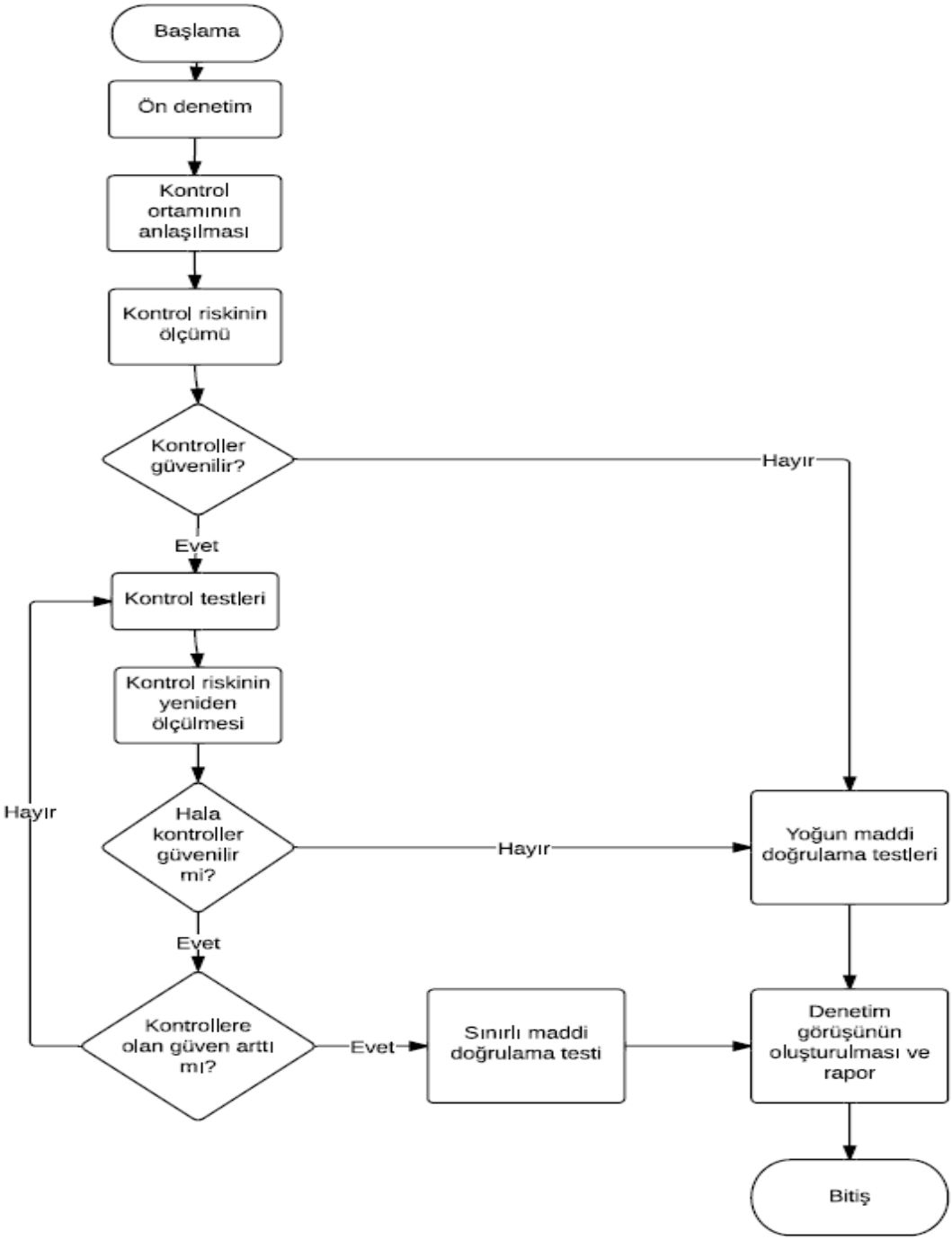
1) ***Önleyici kontroller***: Personelin yanlış veri girişini önlemek için kaynak dokümanlarında talimatlar bulunması önleyici bir kontroldür.
2) ***Tespit edici kontroller***: Veri giriş programlarının terminallerden yapılan hatalı veri girişlerini tespit etmesi böyle bir kontroldür.
3) ***Düzeltici kontroller***: Programların veri iletişim hatlarının yoğunluğundan kaynaklanan hataların düzeltilmesi için bünyelerinde özel kodları barındırmaları bu tür bir kontroldür.

Kontrollerin nihai amacı usulsüz işlemlerden kuruluşun zarar görmesini minimuma indirmek ve yok etmektir. Denetçinin amacı ise kontrollerin olup olmadığını ve düzgün işleyip işlemediğini ortaya koymaktır. Her türlü usulsüz işlemi önleyecek en az bir kontrolün sistemlerde olması gerekir.

Kontrollerin test edilmesi 4 adımda gerçekleştirilebilir (Houck, 2003: 158):

1) Fayda-Maliyet analizi yapmak,
2) Test edilecek kontrollerin belirlenmesi,
3) Kontrol testlerinin gerçekleştirilmesi,
4) Sonuçların değerlendirilmesi.

2.4.2. Bilgi Teknolojileri Denetim Süreci



Şekil 2.2. Bilgi teknolojileri denetim süreci (Weber, 2013: 72)

2.4.3. Bilgi Teknolojileri Denetiminin Planlanması

BT Denetim ve Güvence Standartları 5 No'lu Standarta göre "Denetçi, denetiminin hedeflerini karşılayacak bilgi sistemleri denetim kapsamını ve yürürlükteki kanun ve mesleki denetim standartlarıyla uyumlu planlamalıdır. BT denetçisi, risk tabanlı bir denetim yaklaşımı geliştirmeli ve belgelendirmelidir. BT denetçisi, denetimin doğasını ve hedefleri, zamanlaması ve kapsam ve hedeflerini ve gerekli kaynakların ayrıntılarını listeleyen denetim planını geliştirmeli ve belgelendirmelidir." (ISACA, 2005). Planlama denetçinin, denetlenen kuruluşun bilişim sistemlerine ilişkin kontrolleri değerlendirmek için maddi kanıt toplamanın etkin ve verimli metotlarını belirlemesine yardımcı olur.

11 No'lu Standarta göre "BT denetçisi, BT denetim planının tamamını geliştirmede ve BT denetim kaynaklarının etkili dağıtımı için önceliklerin belirlenmesinde kullanılabilecek uygun bir risk değerlendirme tekniği veya yaklaşımı kullanmalıdır. BT denetçisi, kişisel denetim planlamasında, denetlenen alanla ilgili riskleri tanımlamalı ve değerlendirmelidir. (ISACA, 2005).

Risk değerlendirmesi, BT denetim alanında denetlenebilir birimleri kontrol etmek, gözden geçirmek ve en yüksek risklere sahip alanları seçmek ve BT planına dahil etmek için kullanılan bir tekniktir. Denetim alanın belirlenmesi, kurumun BT stratejik planı işleyişine ve ilgili yönetim birimleriyle yapılan görüşmelerinin bilgisine dayanmalıdır.

12 No'lu Standarta göre "BT denetçisi, denetim usullerinin sınırı, doğası ve zamanlaması belirlenirken denetimin önemliliği ve bunun denetim riskiyle ilişkisini göz önünde bulundurmalıdır. BT denetçisi, kontrollerin olmaması veya zayıf olması ihtimalini veya kontrollerin olmamasının veya zayıflığının bilgi sistemlerinde önemli hatalara veya ciddi zayıflıklara yol açıp açmadığını dikkate almalıdır. BT denetçisi, küçük kontrol hataların ve kontrollerin olmaması veya zayıf olmasının toplam etkisinin bilgi sistemlerinde önemli hata veya ciddi zayıflıklara dönüşüp dönüşmediğini dikkate almalıdır. BT Denetçisinin raporu, yetersiz kontrollerin olması veya kontrollerin olmaması ve kontrol hatalarının önemini ve bu zayıflıklardan kontrol hatalarının ve ciddi zayıflıkların kaynaklanma olasılığını açıklamalıdır." (ISACA, 2006).

Denetim riski, BT denetçisinin denetim bulgularına dayanarak yanlış sonuçlara ulaşma riskidir. Denetim riski yapısal risk, kontrol riski ve tespit riski bileşiminden meydana gelir. BT denetçisi, denetimi planlarken ve yürütürken denetim riskini kabul edilebilir bir seviyeye indirmeye ve denetim hedeflerini gerçekleştirmeye çalışmalıdır. Planlama aşamasında denetçi açısından en zor karar her bir hesap alanı için kontrol riski seviyesini belirlemektir. Kontrol riskinin belirlenmesinde denetçinin bilgi sistemleri bilgisi ve tecrübesi önemlidir. Denetçi kontrol riskini belirlerken iç kontrol ortamını çok iyi anlamalıdır. İç kontroller birbiriyle ilişkili 5 bileşenden oluşmaktadır:

1) ***Kontrol çevresi***: Muhasebe ve kontrol sistemlerinin kurulmasını, prosedürlerinin işlemesini sağlayan unsurları ifade etmektedir. Kontrol çevresi; yönetimin felsefesinde, işleri yürütme şeklinde, yetki ve sorumlulukların tayin edilmesinde, performans ölçümünde yönetimin gösterdiği tutum ve davranışlarda ortaya konmaktadır.

2) ***Risk ölçümü***: Kuruluşun karşı karşıya olduğu risklerin ortaya çıkarılması, analiz edilmesi ve yönetilmesine yönelik unsurlardır.

3) ***Kontrol faaliyetleri***: İşlemlerin yetki dahilinde yapılması, görevlerin ayrılığı, yeterli dokümantasyon ve kayıt, varlıkların korunması, performans ve kayıtlı miktarların değerlendirilmesine yönelik bağımsız kontrollerin olup olmadığına yönelik faaliyetlerdir.

4) ***Bilgi ve iletişim***: Personel arasında bilgi akışının sağlanması, yetki ve sorumluluklarda yapılan değişikliklerin zamanında duyurulmasıdır.

5) ***İzleme***: İç kontrollerin güvenli şekilde işlediğini gösteren unsurlardır.

Bir kuruluşta iç kontrol ortamının anlaşılması yönetim kontrollerinin ve uygulama kontrollerinin ayrı ayrı incelenmesini gerektirir. Denetçi, kontrol çevresi ile risk ölçümü unsurlarını yönetim kontrollerine bakarak anlayabilir. Örneğin denetçi, bilişim sistemleri gözetim komitesinin olup olmadığını sorguladığında aslında denetçi iç kontrol çevresini, risk değerlendirme unsurlarını araştırıyor demektir. Yine denetçi, bir takım özel kontrol faaliyetlerini ancak yönetim kontrolleri ile birlikte uygulama kontrollerini de

inceleyerek anlayabilir. İzleme faaliyetlerini de yönetim kontrollerine bakarak anlayabilir. Örneğin denetçi yönetimin personelin performansını değerlendirme yöntemlerini incelediğinde izleme unsurunu anlamaya çalışıyor demektir.

Uygulama kontrolleri de kuruluşların teşkilatlanmasına göre çok çeşitli olabilir. Merkezi kuruluşlarda uygulama kontrolleri genellikle tek bir döngüden oluştuğu için bir aşamada incelenebilir. Ne var ki dağınık kuruluşlarda uygulama kontrollerinin incelemesi çok sayıda aşamadan oluşabilir. Her bölüm kendi satış ve tahsilat döngüsüne, ücret ve personel döngüsüne, stok ve depolama döngüsüne ve maliye döngüsüne sahip olabilir. Denetçi denetimi için önemli olan her bir döngüyü alt sistem ve uygulama sistemlerine ayırarak bu sistemlere ilişkin kontrolleri test etmek ve güvence elde etmek durumundadır.

Kontrollerdeki zayıflıklar, eğer kontrollerin olmaması kontrol hedeflerinin gerçekleştirilmesinde makul bir güvence sağlamada başarısızlıkla sonuçlanıyorsa önemlill kabul edilir. Önemli olarak sınıflandırılan bir zayıflık şu anlama gelir:

- Kontroller yerinde değildir.
- Kontroller kullanımda değildir.
- Kontroller yetersizdir.

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

2.4.3.1. Denetlenen kurumun bilişim sistemleri hakkında bilgi edinme

Denetlenen kuruluşun bilişim sistemleri altyapısı, organizasyonu, bütçesi ve önceki yıllarda bilişim sistemlerine ilişkin bulgular içeren iç ve dış denetim raporları genel hatları ile incelenmelidir.

Bu aşamada önemli adımlardan biri iş akış şemalarını çıkarmaktır. İş akış şemaları, iş akış süreçlerinde; süreç adımlarının, otomatik veya manuel kontrollerin, sürecin özel durumlarını da gösteren alternatif akış yollarının, paralel işleyen adımların gösterildiği

diyagramlardır. Bu şemalarda, yapılan işin kurumun hangi birimi tarafından ve hangi sistem kullanılarak yapıldığı da görülebilmelidir. Kuruluş iş akışlarını incelerken, iş süreçlerinde oluşturulmuş kontroller belirlenmelidir.

2.4.3.2. Mali yönetimle ilgili bilişim sistemlerinin belirlenmesi

Denetçi, bilişim sistemleri envanterini çıkartarak, hangi bilişim sistemlerinin mali tablolara bilgi ürettiğini, mali işlemlerin özellikle hangi bilişim sistemlerinde yürütüldüğünü tespit eder ve bu sistemlerden hangilerinin mali denetim açısından kritik olduğunu belirler.

2.4.3.3. Bilişim sistemlerinin karmaşıklığı hakkında değerlendirme yapılması

Bu değerlendirme sistemlerin karmaşıklık derecesi, sistemdeki bilgilerin gizliliği, veri giriş yöntemleri, denetim izine ulaşma konusundaki sorunlar, bilişim sistemlerinde son dönemde yapılmış geliştirme ve değişiklikler göz önünde bulundurularak yapılır. BT denetimlerinde karmaşık sistemlerle başa çıkmanın iki yolu vardır:

Birincisi,

1) BT denetiminin amacına uygun olarak sistemleri alt sistemlere ayırmak,
2) Her bir alt sistemin güvenilirliğini test etmek ve elde edilen sonuçlara göre bütün sistemi değerlendirmek.

(Alt sistemler üst sistemlerin ihtiyaç duyduğu belli bir görevi ifa eden ve ana sistemin temel amaçlarını gerçekleştirmesine yardımcı olan, fiziksel varlıklardan ziyade mantıksal bileşenlerden oluşan sistemlerdir.)

İkincisi,

Karmaşık olduğu tespit edilen sistemler için uzman kişilerden destek almaktır.

2.4.3.4. Ön risk değerlendirmesinin yapılması

Elde edilen bilgiler ışığında, belirlenen sistemlerde önemlilik, kritiklik, karmaşıklık, teknik altyapı, kontrol çevresi kriterlerine göre risk değerlendirmesi yapılmalıdır ve risk puanları dikkate alınarak, denetimde öncelik verilecek sistemlerin, önemlilik sıralaması belirlenmelidir. Planlama çalışmaları neticesinde denetçi, hangi genel kontrollerin test edilmesi gerektiğine ve uygulama kontrollerinin denetlenip denetlenmeyeceğine karar verir.

“Özellikle AB Komisyonun ABAC ve SAP gibi önemli kaynak yönetim sistemleri üzerindeki uygulama kontrolleri, bu sistemlerin asıl sahipleri olan Genel Direktörlüklerde test edilir. Bu sistemlerin sadece kullanıcısı olan kurum veya birimlerde BS denetimi, genel kontroller ve uygulama kontrollerinin veri girişi kontrolleri ile sınırlıdır. Denetim kapsamına alınacak genel kontroller ve uygulama kontrollerinin neler olduğu, denetimin planlama aşaması sonunda hazırlanacak denetim planında yer alır.” (Kayrak, Avrupa Birliği Sayıştayında Mali Denetim Çerçevesinde Bilişim Sistemleri Denetimi, 2011:20-21).

Bu aşamada temel amaç, denetim hedefleri ile ilgili risklerin belirlenmesi ve bunlara karşılık var olması gereken kontrollerin neler olduğunun tespit edilmesidir.

2.4.4. BT Kontrolleri

ISA 315’e göre, denetçi bilgi sistemlerinden kaynaklanan riskleri anlamalı ve değerlendirmelidir.

“Bilgi sistemlerinin kuruluşlarda kullanılması kontrol faaliyetlerinin gerçekleştirilmesini etkiler. Bu nedenle denetçinin bilgi sistemlerinden kaynaklanan riskleri değerlendirmek için genel BT kontrollerini ve uygulama kontrollerini değerlendirmesi gerekir.” (Puttick ve diğerleri, 2007: 473).

“BT denetçisi, kurumun iç kontrol ortamının bütünleşik bir parçası olan BT kontrollerini izlemeli ve değerlendirmelidir. BT denetçisi, BT kontrollerinin tasarımı, uygulanması,

işletimi ve geliştirilmesi ile ilgili öneriler sağlayarak yönetime yardımcı olmalıdır." (ISACA, 2006; 15 No'lu standart).

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

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

BT denetçisi, BT kontrol süreçlerinin durumuyla ilgili güvence sağlamak amacıyla, BT denetim kaynaklarının etkili dağılımı için öncelikleri belirlemede ve tüm denetim planının geliştirilmesinde uygun bir risk değerlendirme tekniği ya da yaklaşımı kullanmalıdır. Kontrol süreçleri, risklerin, risk yönetimi süreciyle oluşturulmuş risk toleransları içerisinde bulunmasını sağlamak amacıyla tasarlanmış kontrol çevresinin bir parçası olan politikalar, usuller ve etkinliklerden oluşur.

BT denetçisi, BT kontrollerini bilgisayar aracılığıyla gözden geçirirken seçici denetim kanıtlarını toplama ve sürekli olarak BT denetçisine sistem güvenilirliğini izleme olanağı sunan sürekli güvencenin kullanımında veri analiz tekniklerinin kullanımını düşünmelidir. Kurumlar üçüncü tarafları kullandıklarında bu taraflar kurumun kontrollerinde ve ilgili kontrol hedeflerinin başarılmasında temel unsur haline gelebilir. BT denetçisi, BT çevresi, ilgili kontroller ve BT kontrol hedefleriyle ilişkili olarak üçüncü tarafların yürüttüğü rolü değerlendirmelidir.

BT kontrolleriyle ilgili ayrıntılı bilgi için aşağıda belirtilen ISACA ve BT Yönetişim Enstitüsü rehberlerine başvurulabilir:

- Rehber G3 Bilgisayar Destekli Denetim Tekniklerinin (BDDT) Kullanımı
- Rehber G11 Yaygın BS Kontrollerinin Etkisi
- Rehber G13 Denetim Planlamasında Risk Değerlendirmesinin Kullanımı
- Rehber G15 Planlama
- Rehber G16 Kurumsal BT kontrollerinde Üçüncü Tarafların Etkisi

- Rehber G20 Raporlama
- Rehber G36 Biyometrik Kontroller
- Rehber G38 Erişim Kontrolleri
- COBIT Çerçevesi ve Kontrol Hedefleri

BT kontrolleri genel kontroller ve uygulama kontrolleri olmak üzere iki kategoride incelenebilir.

2.4.4.1. Genel kontroller

Genel Kontroller, kuruma ait tüm bilişim sistemleri faaliyetlerinin sürekliliğinin sağlanmasına yönelik yapı, yöntem ve prosedürlere ilişkin kontrollerdir. Bu kontroller uygulama yazılımları ve bunlara ilişkin kontroller için güvenli bir ortam oluşturur. Genel kontroller aşağıda belirtilen kontrol alanlarından oluşur:

- Yönetim Kontrolleri
- Fiziksel ve Çevresel Kontroller
- Ağ Yönetimi ve Güvenliği Kontrolleri
- Mantıksal Erişim Kontrolleri
- İşletim Kontrolleri
- Değişim Yönetimi Kontrolleri
- Acil Durum ve İş Sürekliliği Planlaması Kontrolleri (Sayıştay, 2013:11).

2.4.4.1.1. Yönetim kontrolleri

Kurum yönetimi, bilişim sisteminin kurum amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almakla yükümlüdür. Yönetim kontrollerinin amacı güvenli ve yeterli bir bilişim ortamının sağlanması için uygun politika ve prosedürler oluşturmaktır. Bu kontroller denetçiye alt düzeydeki ayrıntılı kontrollerin varlığı ve etkinliği konusunda makul bir güvence sağlar. Yönetim kontrolleri, stratejik planlama, güvenlik politikaları, organizasyon, varlık yönetimi, personel ve eğitim politikaları ile yasal düzenlemelere uygunluk alanlarından oluşur. (Sayıştay, 2013: 11).

2.4.4.1.2. Fiziksel ve çevresel kontroller

Fiziksel ve çevresel kontrollerin amacı, bilişim sistemleri donanımın ve yazılımının kasten ya da kazaen oluşan hasarlara, izinsiz erişim sonucu bozulma veya çalınma ile her türlü çevresel tehlikelere karşı korunmasıdır. Bilişim sistemleri, bu sistemlere erişme yetkisi olmayan kişilerin yol açabilecekleri hasarlara ve müdahalelere karşı fiziksel engeller konulmak suretiyle korunurken; yangın, su (ya da aşırı nem), elektrik, voltaj dalgalanmaları veya güç yetersizlikleri gibi çevresel tehlikelere karşı ise, bunlara ilişkin uygun önlemler alınarak korunmalıdır (Sayıştay, 2013: 28).

Fiziksel ve çevresel korumaya yönelik kontrollerin hiç veya yeterli düzeyde kurulamaması durumunda, bilişim sistemleri, personelinin isteyerek veya istemeyerek verebileceği zararlara açık hale gelebilir; kritik veya gizli bilgi görülebilir, kopyalanabilir veya kaybedilebilir; bilişim sistemleri yangın, sel, elektrik kesintileri veya voltaj düzensizlikleri, sıcaklık ve nem gibi çevresel tehlikelerle kısmen veya tamamen çalışamaz duruma gelebilir ve hizmette aksaklıklara veya veri kayıplarına neden olabilir. Bu nedenle, kurum yetkisiz fiziksel erişime ve çevresel tehlikelere ilişkin yazılı güvenlik politikasına ve prosedürlerine sahip olmalı ve ana bilişim sistemlerinin bulunduğu binalara yetkisiz fiziksel erişimi önlemek için gerekli tedbirleri almalıdır. Bunun için, binalarda göze çarpmayan ve kullanılma amaçlarıyla ilgili en az göstergelerle belirlenmeli; uygun sızma tespit sistemleri (hırsız alarmı, kamera, projektör vs.) kurulmalı; stratejik noktaları izlemek üzere video kameralar konulmalı ve kayıtları saklanmalı; kurum binalarına girişlerde güvenlik görevlileri konumlandırılmalı; bina girişlerinde personel kimlik kartlarının kullanımına ilişkin uygulama geliştirilmeli; gelen ziyaretçiler deftere kaydedilmeli, ziyaretçi defterlerinde tarih, giriş-çıkış saati, imza, nereye gittiği, kiminle görüşeceği, hassas alanlara giriş yetkisi verilmiş olup olmadığı, bu alanlarla ilgili güvenlik bilgilerinin kendilerine anlatılıp anlatılmadığı, güvenlik görevlisi refakatinin gerekip gerekmediği gibi hususlar yer almalı; işten ayrılan personelin kurum kaynaklarına fiziksel erişimini engelleyen prosedürler bulunmalıdır (Yıldız, 5018 Sayılı Kanun ve Bilişim Sistemleri Denetimi, 2010: 123).

2.4.4.1.3. Ağ yönetimi ve güvenliği kontrolleri

Ağ yönetimi ve güvenliği kontrollerinin amacı, ağ sistemini oluşturan tüm varlıkların korunması, ağ hizmetlerinin güvenli bir şekilde yürütülmesi ve ağ aracılığıyla gerçekleşebilecek yetkisiz erişim ve bunlar dolayısıyla oluşabilecek tehlikelerin önlenmesidir. Ağ, veri paylaşımı amacıyla iki ya da daha fazla cihazın birbiriyle bağlantılı hale getirilmesiyle oluşturulan bir yapıdır. Yüzlerce iş istasyonu veya kişisel bilgisayardan oluşabileceği gibi iki bilgisayarın birbirine bağlanmasıyla da elde edilebilir. Bu ağ ortamıyla iletişim, bilgiye ulaşım, kaynak paylaşımı, yedekleme gibi hizmetler sağlanabilmektedir (Sayıştay, 2013: 36).

Ağı oluşturan sistemler tasarlanırken veya devreye alınırken güvenlik unsuru hesaba katılmadığında, bu sistemlerin çeşitli zayıflıkları nedeniyle kötü niyetli veya meraklı kişiler tarafından sistemler ve hizmetler kullanılamaz hale getirilebilir ya da kurumlar için çok önem taşıyan bilgilerin öğrenilmesi/değiştirilmesi mümkün olabilir. Veriler bozulabilir, kaybolabilir ve/veya çalınabilir, kötüye kullanılabilir; yetkisiz işlem tesis edilebilir; ağ bağlantıları ve sunucular kolaylıkla zarar görebilir; güvenliği zayıflatacak ve sistemde açıklıkların meydana gelmesine sebebiyet verecek virüs gibi kötü niyetli yazılımlar bulaşabilir; sistemin yavaş çalışması nedeniyle işin yürütülmesinde çeşitli aksamalar meydana gelebilir; Ceza Kanunu gibi yürürlükteki yasal mevzuat ihlal edilebilir. Bu nedenle, ağlar, yetkisiz erişimlerin engellenerek sadece yetkili kullanıcıların erişebilmesi için kontrol edilmelidir.

Fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir değeri bulunmadığından ağın fiziksel unsurlarının (kablolar, sunucular, iletişim araçları vs.) güvenliği fiziksel ve çevresel kontroller altında sağlanmalıdır. Bununla birlikte ağ ve internet güvenliğinin sağlanması için başka kontrollerin de kurulması gerekmektedir. Bilişim sistemleri güvenlik politikasının bir parçası olarak ağ ve internet kullanımına ilişkin güvenlik politikası olmalıdır. Şifre seçiminde e-posta eklentileri kullanımına kadar güvenlik konularında kullanıcıların ve bilgi işlem yöneticilerinin bilinçlendirilmesi sağlanmalıdır.

2.4.4.1.4. Mantıksal erişim kontrolleri

Mantıksal erişim kontrollerinin amacı, işletim sistemine, ağa, veri tabanına ve uygulama programlarına yetkisiz erişimin önlenmesi ve bilginin değiştirilmesi, açığa çıkarılması ve kaybına karşı korunmasıdır. Mantıksal erişim kontrolleri, hem sistem hem de uygulama düzeyinde ortaya çıkabilir. Bilişim sistemi ortamındaki erişim kontrolleri ağa, işletim sistemine, sistem kaynaklarına, veri tabanına ve uygulama programlarına erişimi sınırlandırırken, uygulama düzeyindeki kontroller, tek tek uygulamalar bünyesindeki kullanıcı faaliyetlerini kısıtlar (Sayıştay, 2013: 64).

Mantıksal erişim güvenliğinin üç temel öğesi vardır. Bunlar, kullanıcı kimliğinin tanıtılması, kullanıcı kimliğinin onaylanması ve kaynak korumasıdır (Özkul, 2002):

- **Kullanıcı kimliğinin tanıtılması:** Kullanıcının kendisini bir kullanıcı adı ve giriş şifresi ile bilgisayara tanıtmasıdır.
- **Kullanıcı kimliğinin onaylanması:** Kullanıcının yazdığı kimlik bilgilerinin bilgisayar tarafından tutulan bir kütükteki bilgiler ile karşılaştırılarak doğruluğunun onaylanmasıdır.
- **Kaynak koruması:** Kaynaklar, bilgisayar dosya ve klasörleridir. Kullanıcının kendisini sisteme tanıtıp onay almasından sonra sistemin, o kullanıcının erişmeye yetkili olduğu kaynaklar dışındaki dosya ve uygulamalara erişmesine izin vermemesidir.

Mantıksal erişim kontrollerinde kurumca politika ve prosedürlerin tanımlanmamış olması durumunda ortaya çıkabilecek riskler aşağıda belirtilmiştir:

- Kurum varlıklarına erişimde yetki karmaşıklığına, sorumluların belirlenememesine, kullanıcıların yeterli düzeyde bilgilenememelerine yol açması,
- 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),
- Kullanıcı şifrelerinin çalınması ve kullanılması,
- İşten ayrılan personelin sisteme yetkisiz erişebilmesi,
- Erişim politikasından sapmaların tespit edilememesi,
- Yetkisiz erişim teşebbüslerinin ve etkilerinin belirlenememesi,
- Yönetimce gerekli önlemlerin alınamaması,

Kurum bilişim sistemlerinde mantıksal erişim kontrollerine ilişkin politika ve prosedürlerin olmaması veya yetersiz olması sonucu meydana gelecek riskleri minimize edecek temel kontrol faaliyetleri şunlardır:

- Sistem ve uygulama programlarına erişimin güvenli olmasını sağlayan bir mantıksal erişim politikası olmalıdır.
- Kurumun şifre politikası olmalıdır.
- Kullanıcı erişim yönetimine ilişkin prosedürler tanımlanmış olmalıdır.
- Sistem ve uygulama programlarına erişimler kayıt altına alınmalı ve izlenmelidir.
- Yetkisiz erişimler raporlanmalı ve yönetimce gereken işlemler süratle yapılmalıdır.

2.4.4.1.5. İşletim kontrolleri

İşletim kontrollerinin amacı bilişim sisteminin kendinden beklenen faaliyetlerin sürekliliğini ve güvenliğini sağlayacak şekilde işletilmesidir. İşletim kontrolleri aşağıdaki alanlara göre incelenir:

- **İşletim sistemi ve bilgisayar işlemleri kontrolleri:** Uygulama yazılımların üzerinde çalıştığı işletim sisteminin kurulum ve işletilmesi ile bakım işlemlerinin sorunsuz yürütülmesini ve tüm bilgisayar işlemlerinin güvenli bir şekilde gerçekleştirilmesini sağlamaya yönelik her türlü kontrollerdir.

- **Veri tabanı güvenlik kontrolleri:** Birbirleriyle ilişkili verilerin güvenli bir şekilde kaydedilip depolanmasını, belgelendirilmesini ve gerektiğinde de güvenli ve çok amaçlı kullanılmasını sağlayacak her türlü kontrollerdir.

Sistem kapasite ve performans durumunun düzenli olarak izlenmesi sağlanarak gelecekte gerekli olacağı düşünülen kapasite tahminleri ve planları yapılmalıdır. Bilgi ortamı araçlarının (kasetler, manyetik ve optik diskler vs.) oluşturulma, transfer, korunma ve saklanma gibi işlemleri etkin şekilde yönetilmelidir. Bilişim sisteminden sorumlu birimin diğer birimlere sağlayacağı hizmetler yazılı olarak tanımlanmış olmalıdır. Bir başka konu ise, olay yönetimine ilişkin önceden belirlenmiş prosedürlerin olmamasıdır. Olayların takip ve çözümü için bunların tanımlanması, kaydının tutulması, analiz ve destek hizmetlerinin sağlanmasına yönelik prosedürler belirlenmeli, olayın işe etkisi değerlendirilmeli ve bir daha olmasını önleyecek çarelere ilişkin planlar yapılmalıdır. Ayrıca olayların istatistiklerinin çıkarılarak yönetime bildirilmesi sağlanmalıdır. Yine olay yönetimi ile işbirliği içerisinde bulunmak kaydıyla problemlerin yönetimine ilişkin prosedürler belirlenerek ve yardım masası kurularak problemlerin uzman personele aktarılmasını sağlayacak yapı oluşturulmalıdır (Yıldız, 5018 Sayılı Kanun ve Bilişim Sistemleri Denetimi, 2010: 126).

2.4.4.1.6. Sistem geliştirme ve değişim yönetimi kontrolleri

Bu kontrollerin amacı sistem geliştirme üzerindeki tüm proje yönetimi ve kontrollerinin tatmin edici olmasını, kalıcı ve yeterli iç kontrol ve denetim izine sahip olmasını, sistem geliştirme kalitesinin artırılmasını ve sistemin kullanıcıların ihtiyaçlarını karşıladığı kadar kurumun stratejik amaçlarını da desteklemesini sağlamaktır (Sayıştay, 2013: 87).

Sistem geliştirmede, bir sistemin kurulması için gerekli olan adımların neler olabileceğini öngörmenin yanında, kurumlarda yürütülecek her türlü bilişim sistemleri projelerinin de nasıl ele alınması gerektiği konusunda rehberlik sağlamaktadır. Değişim yönetimi ise, kullanıcı görev ve sorumluluklarında meydana gelecek değişimlere ilişkin prosedürlerin de içinde yer aldığı kurum bilişim sistemlerinin

donanım, yazılım, ağ gibi tüm unsurları içine almakta ve her türlü değişimin yazılı kurallar çerçevesinde yürütülmesini öngören kontrollerden oluşmaktadır.

Bu kontrollerin yeterli düzeyde uygulanmaması durumunda, sistem geliştirme projelerinin yetersiz düzeyde hazırlanmasına yol açabilir; proje kurum ihtiyaçlarına veya kullanıcı gereksinimlerine cevap veremeyebilir; kaynakların israf edilmesine yol açabilir; sistemin kurulumuna ilişkin sözleşmelerde yeterli güvenceler olmayabilir. Bu nedenle, başarılı bir bilişim sistemleri projesinin yeterli bir iç kontrol ve denetim izini de içerecek şekilde nasıl yürütüleceğini gösteren adımlara değinmek gereklidir.

Öncelikle, sistem geliştirme için standart hale getirilmiş politika ve prosedürler bulunmalıdır. Önceden belirlenmiş standartlar yeni bir sistemin geliştirilmesine yönelik süreç esaslı kontroller sağlar ve bu sürecin uyulması gereken aşamalarını gösterir. Sistem geliştirmenin söz konusu aşamalarına ilişkin olarak uygulama ve standartların, başlangıç, sistem analizi ve tespiti, sistem tasarımı, sistem geliştirme, kabul testi, uygulama ve uygulama sonrası kabul ve inceleme konuları itibariyle tutarlılığı sağlanmalıdır. (Yıldız, Bilişim Sistemleri Denetimi ve Sayıştay, 2007: 126)

2.4.4.1.7. Acil durum ve iş sürekliliği planlaması kontrolleri

Acil durum ve iş sürekliliği planlaması ile ilgili kontrollerin amacı acil durum nedeniyle bilişim sistemlerinin geçici veya sürekli olarak aksaması durumunda kurumun işlevlerini sürdürebilmesini ve tutulan bilginin işlenmesi, erişilmesi ve korunması yeteneklerinin kaybedilmemesini sağlamaktır.

Acil durum, deprem, yangın, fırtına, sel, bombalama, sabotaj, donanım veya yazılım hatası, elektrik ve telekomünikasyon kesintisi gibi önceden tahmin edilebilen veya edilemeyen iç veya dış faktörler sonucu meydana gelen ve kurumun normal olarak işlerini sürdürmesi durumunu aksatan her şey olabilir. Bu çerçevede, kurumlar detaylı bir acil durum ve iş sürekliliği planına sahip olmalıdır.

Acil durum ve iş sürekliliği planının olmaması veya yetersiz olması kurumu aşağıdaki risklerle karşı karşıya getirecektir:

- Felaketlere maruz kalma olasılığının artması,
- Felaketin verdiği zararlarla başa çıkma imkanının azalması,
- Felaketten kaynaklanan kaybın veya zararın ağırlaşması,
- Karşılaşılan felaket sonrasında makul bir sürede kurum faaliyetlerinin yeniden başlatılamaması,
- Yasal veya üçüncü kişilere karşı olan sorumlulukların zamanında yerine getirilememesi,
- Bir felaket durumunda iletişim imkanları, bilgi işleme kapasitesi, eğitimli insan kaynağı ve tüm varlıklar yitirilebileceğinden kurumun faaliyetlerini sürdürmesinde devamlılığın sağlanamaması (Sayıştay, 2013: 99).

Bu nedenlerle, etkisi yıkıcı boyutlarda olabilecek acil ve beklenmedik durumların kuruma verebileceği kayıp veya zararları en aza indirmek için önceden tahmin edilebilen veya edilemeyen iç veya dış faktörlerden kaynaklanan acil durumlara karşı hazırlıklı olunmalıdır. Bu nedenle kurumda acil durum ve iş sürekliliği için bir yönetim süreci oluşturulmalıdır.

2.4.5. Uygulama kontrollerinin Değerlendirilmesi

“Uygulama kontrolleri, bilgilerin sistemlere ya da programlara tam olarak, zamanında ve sadece bir kere girilmesini, bilgi-işlem ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleşmesini, raporların tam ve güvenilir olarak üretilmesini, yetkili kişilere ulaştırılmasını ve uygun şekilde arşivlenmesini sağlayan kontrollerdir” (Sayıştay, 2013: 99).

Uygulama kontrolleri değerlendirilirken uygulamaların güvenilirliğine ilişkin makul bir güvence elde edebilmek için uygulamalarda olması gereken kontroller test edilerek kanıt toplanır. Bu aşamada bilgisayar destekli denetim tekniklerinden (BDDT) de yararlanılır. BDDT, programlardaki süreçlerin doğruluğunun saptanması ve veri dosyalarının incelenmesinde kullanılır. Programlardaki süreçlerin doğruluğunun saptanmasında, anlık görüntü alma (snapshot), iz sürme (tracing), log analizi gibi teknikler kullanılabilir. Verilerin doğruluğu ve dosya güvenilirliği için paralel simülasyon,

mükerrerlik kontrolü, sınıflandırma, örnekleme, karşılaştırma gibi analiz tekniklerinden yararlanılabilir. (Yıldız, Bilişim Sistemleri Denetimi ve Sayıştay, 2007: 128)

Uygulama kontrolleri aşağıda belirtilen başlıklar altıda incelenebilir:

- Girdi Kontrolleri,
- Veri Transfer Kontrolleri,
- İşlem Kontrolleri,
- Çıktı Kontrolleri.

2.4.5.1. Girdi kontrolleri

Girdi kontrollerin amacı verilerin sisteme, tam, doğru ve yetki dahilinde girilmesini sağlamaktır. Girdi üzerindeki kontroller sistemin bütünlüğü açısından önemlidir.

Veri girişine ilişkin olarak karşılaşılabilecek risklerden bazıları şunlardır: (Sayıştay, 2013: 108).

- Yetkili olmayan kişilerce veri girişi yapılması
- Eksik veya hatalı veri girilmesi
- Mükerrer kayıtların sistem tarafından kabul edilmesi
- Hatalı veri girişlerinin tespit edilememesi
- Erişim Kontrollerinin ihlal edilmesi
- Görevlerin ayrılığı ilkesine uyulmaması

Veri kaynaklarının kontrolü, işlemlere kaynak teşkil edecek olan verilerin manuel ortamda hazırlanması, incelenmesi ve onaylanması aşamalarını içerir. Veri kaynaklarının kontrolü, verilerin bilgisayar uygulamalarına girişi yapılmadan önce doğru ve güvenli olmalarını sağlamak için oluşturulur.

Veri kaynaklarının hatasız olması için gerekli tedbirlerin alınmış olması gerekir. Bu tedbirlerin başında, veri girişi yapacak personelin güvenilir olması, görevlerin ayrılmış olması, yetki ve sorumlulukların açıkça belirlenmiş olması, kaynak dokümanların iyi

tasarlanmış, numaralandırılmış ve güvenliklerinin sağlanmış olması ve veri kaynaklarının yetkili personel tarafından incelenip onaylanmış olması gelir.

“Ayrıca, düzeltilmiş her bir hatalı kaynak dokümanı için hata kütüğü tutulması gerekir. Bu kütükte, doküman numarası, işlem numarası, hata nedeni, oluşturulma tarihi, düzeltme tarihi ve hazırlayan personelin kimliği yer almalıdır.” (Özkul, 2002).

2.4.5.2. Veri transfer kontrolleri

Veri transferi kontrolleri verilerin tam, doğru, zamanında ve güvenli bir şekilde transferini sağlamayı amaçlar. Sistemler arasında veri transferi için çeşitli metotlar bulunduğundan her bir metot için kullanılan prosedürlerin iyi anlaşılması gerekir. Bu kontrollerin uygulanmasındaki aksaklıklar transfer edilen verinin bozulmasına, kaybolmasına, çalınmasına, değiştirilmesine veya veri iletiminin aksamasına neden olabilir.

Veri transfer kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır;

- Veri transferinden sorumlu personele rehberlik yapacak prosedürler tanımlanmış olmalıdır.
- Veri transferi ile ilgili detaylı teknik bilgiler yazılı hale getirilmeli ve personel ihtiyaç duyduğunda bu bilgilere erişebilmelidir.
- Sistemler arasında yapılan veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller olmalıdır (Sayıştay, 2013: 113).

2.4.5.3. İşlem kontrolleri

İşlem kontrollerin amacı verilerin uygulama programları içinde tam ve doğru olarak işleme tabi tutulmasını ve denetlenebilir olmasını sağlamaktır. Girdi ve üretilen verinin tam ve doğru işlenmesi çeşitli bilgisayar kontrollerin uygulama programlarına entegre edilmesiyle sağlanmaktadır.

İşlem kontrollerinin yetersizliği aşağıda yazılı risklerin gerçekleşmesine neden olabilir: (Sayıştay, 2013: 116)

- Sürecin yanlış işletilmesi,
- Sistematik hataların oluşması,
- Yanlış dosyaların işleme tabi tutulması,
- Hataların tespit edilip düzeltilememesi,
- Denetim izinin kaybolması ve işlem sahibine başvurulamamasına,
- Mantıksız işlemlerin meydana gelmesi,
- İşlemlerin doğrulanamaması,

İşlem kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır;

- İş ve zaman çizelgesi hazırlanmalı ve bu çizelge kullanıcı ve işletim personeli tarafından anlaşılır olmalıdır.
- Yönetim tarafından bilgisayar işlemlerinin doğru zamanda ve doğru bir silsile ile işletildiğinin teyidini sağlayan yeterli bir kontrol mekanizması kurulmalıdır.
- Süreçte başarısızlık veya problemle karşılaşıldığında, personel, işlemleri onaylandıkları en son noktadan yeniden başlatabilmelidir.
- Bütün işlemler ve bilgisayar kaynaklı hatalar hata ve beklenmedik durum raporlarında yer almalı ve bunlar yönetim tarafından gözden geçirilmelidir.

2.4.5.4. Çıktı kontrolleri

Çıktı kontrollerin amacı, çıktıların tam, doğru ve zamanında üretilmesini, doğru yere veya kişilere dağıtılmasını, gizliliklerinin korunmasını, tespit edilen hataların detaylı olarak incelenmesini ve gereğinin yapılmasını sağlamaktır. “İşlem zayıflıklar zaman zaman çıktı üzerindeki güçlü kontrollerle telafi edilebilmektedir. Girdi ve işlem açısından iyi kontrol edilen sistem çıktının kontrolsüz olup olmadığı tam olarak sarsabilir. Çıktı safhasının sonunda yürütülen uyumlaştırma döngüde önceki safhaların tamlık ve kesinliği üzerinde çok önemli bir güvence sağlayabilir. Çıktı kontrollerinin yetersizliği durumunda, çıktılar tam ve doğru olmayabilir, uygun bir şekilde

sınıflandırılıp dağıtılamayabilir; yetkisiz kişilerin eline geçebilir; hatalar tespit edilemeyebilir ve düzetilemeyebilir; çıktılar muhafaza edilemeyebilir.” (Yıldız, 5018 Sayılı Kanun ve Bilişim Sistemleri Denetimi, 2010).

Çıktı kontrollerine ilişkin riskleri makul seviyeye düşürecek temel kontroller şunlardır; (Sayıştay, 2013: 119).

- Çıktıların elde edilmesine ve korunmasına ilişkin bir prosedür olmalıdır.
- Çıktıların dağıtımı ile ilgili prosedürler tanımlanmalı ve uygulanmalıdır.
- İlgili personel tarafından çıktı raporlarının doğruluğu gözden geçirilmeli ve hataları düzeltilmelidir.
- Çıktılara ilişkin hata veya beklenmedik durum raporu üretilmeli ve yönetim tarafından gözden geçirilmelidir.
- Çıktılar önceden tanımlanmış arşiv yönetmeliğine göre muhafaza edilmelidir.
- Kullanıcılar tarafından kullanılan özel rapor yazım araçları kontrol edilmelidir.

2.4.6. Denetimin raporlanması

“BT denetçisi, denetimin tamamlanması sonucunda uygun biçimde bir rapor hazırlamalıdır. Rapor kurumu, hedeflenen kitleyi ve sunum sınırlamalarını tanımlamalıdır.

Denetim raporu, yürütülen denetim işinin kapsamını, hedeflerini, denetim dönemini ve zamanlamasını, doğasını ve sınırlarını ortaya koymalıdır. BT denetçisinin denetimle ilgili olarak bulgularını, sonuçlarını ve önerilerini, sahip olduğu çekincelerini, niteliklerini veya sınırlandırmalarını belirtmelidir. BT denetçisi, raporlanan sonuçları destekleyecek uygun ve yeterli denetim kanıtlarına sahip olmalıdır. BT denetçisi, raporunu bitirdiği zaman raporunu imzalamalı, tarih atmalı ve denetim yönetmeliği veya hizmet sözleşmesine göre sunmalıdır.” (ISACA, 2005, 7 No'lu Standart).

Detaylı ana rapor ise aşağıda belirtilen bölümler itibariyle oluşturulur (Özkul, 2002):

- **Rapor özeti:** Özet, detaylı denetim raporundan önce yer almalıdır. Kısaca denetçinin temel bulguları ile görüş ve önerilerine yer verilmelidir. Rapor özeti, rapor detaylarını okuyacak zamanı olmayan ilgililerin raporun temel bulgularını çabukça anlamalarını sağlar.

- **Giriş bölümü:** Raporun ana bölümünün girişinde bulunan bu bölüm, denetlenen kurum, inceleme yapan denetçiler, denetimin kapsamı ve denetimin nasıl yapıldığı konusunda bilgiler içermelidir.

- **Ana rapor gövdesi bölümü:** Raporun ana gövdesi, detaylı denetim bulgularını içermelidir. Rapor, mantıklı ve tutarlı bir yapıda ele alınmalı örneğin, konularına göre bölümleme yapılmalı ve kontrol yetersizlikleri ile denetçi bulguları her bir konu için ayrı ayrı belirtilmelidir.

- **Öneriler bölümü:** Bu bölümde, tespit edilen riskleri düşürecek önerilerde bulunulmalıdır. Denetçi, ileri sürdüğü önerilerin mantıklı, anlaşılabilir, uygulanabilir ve kurumun durumuna uygun olmasına dikkat etmelidir.

- **Kurumun denetim bulgularına ilişkin yorumları:** Bu bölümde, denetlenen kurumun denetim bulgularına ilişkin cevap ve yorumları varsa, onlara yer verilmelidir.

2.4.7. Denetim Sonrası İzleme Faaliyetleri

“Bulguların ve önerilerin raporlanmasından sonra, BT denetçisi yönetim tarafından zamanında ve uygun bir şekilde harekete geçilip geçilmediğini belirlemek için ilgili bilgileri istemeli ve değerlendirmelidir.” (ISACA, 2005, 8 No'lu Standart).

“Eğer yönetim, rapordaki uygulama önerilerine dair eylem planını BT denetçisiyle tartışmış ya da ona bildirmiş ise, bu eylemler nihai raporda yönetimin verdiği yanıt olarak kaydedilmelidir. Denetim sonrası izleme faaliyetlerinin doğası, zamanlaması ve kapsamı raporlanan bulguların önemini ve düzeltici faaliyetlerin gerçekleştirilmemesinin etkisini dikkate almalıdır. Asıl raporla ilgili olarak, BT denetim sonrası faaliyetlerin zamanlamasını bağlantılı risklerin doğası ya da büyüklüğü ve

kuruma maliyeti gibi çok sayıda varsayıma bağlı olarak ortaya çıkan mesleki yargısıyla belirlemelidir. İç denetim BT birimi, yönetimin eylemleri etkili biçimde uygulamasını sağlamak ve izlemek için denetim sonrası izleme süreci oluşturmalıdır. Aksi takdirde üst yönetim harekete geçmemenin riskini kabul eder. Denetim sonrası izleme faaliyetleri sorumluluğu, iç denetim birimi yönetmeliğinde tanımlanabilir. Görevin alanı ve şartlarına bağlı olarak dış BT denetçileri, kendilerinin üzerinde anlaştıkları önerileri izlemek için bir iç BT denetim birimine güvenebilirler. Önerileri uygulamak için yapılan etkinliklerle ilgili olarak yönetimin bilgi sağladığı ve BT denetçisinin de sağlanan bu bilgilerle ilgili şüphelerinin oluştuğu durumlarda, denetim sonrası izleme faaliyetleriyle ilgili sonuca varmadan önce gerçek durumun belirlenmesi amacıyla uygun test ya da diğer usullerin kullanılması gereklidir. Üzerinde anlaşmaya varılmış ama uygulanmamış önerileri de içeren, denetim sonrası izleme faaliyetlerinin durumuyla ilgili bir rapor eğer var ise denetim komitesine sunulabilir veya aynı rapor diğer bir seçenek olarak uygun seviyedeki kurum yönetimine sunulabilir. Denetim sonrası izleme faaliyetlerinin bir parçası olarak BT denetçisi eğer uygulanmadıysa bulguların hala geçerli olup olmadığını değerlendirmek durumundadır.” (Yurdagül, 2010: 16)

2.4.8. Eşzamanlı denetim teknikleri

Eş zamanlı denetim teknikleri, denetçilerin bilgisayar tabanlı uygulama sistemlerin güvenilirliğine ilişkin denetim kanıtı toplarken kullandıkları araçlardır. Kanıt toplama işi sistemler normal veri işleme süreçlerini gerçekleştirirken ve sistemi aksatmadan gerçekleştirilir. Bu teknikler veri tabanı yönetim sistemi gibi uygulama yazılımları veya sistem yazılımları içine gömülü program talimatları yoluyla gerçekleştirilmektedir. Duyarlı ve yüksek önemliliğe sahip uygulama sistemleri içinde eşzamanlı denetim teknikleri sürekli uygulanabileceği gibi belli aralıklarla veya riskli dönemlerde uygulanabilir. Uygulama sistemleri işlerken yüksek riskli bir hatanın veya usulsüzlüğün meydana gelmesi halinde denetçiye raporlanır.

Eş zamanlı denetim tekniklerinin ortaya çıkışı 1960’ların sonları ile 1970’lerin başlarında bilgisayar sistemlerinin denetim ihtiyacından ortaya çıkmıştır. Başlıca ortaya çıkma sebepleri şunlardır (Weber, 2013: 779):

Kağıt belgeye dayalı denetimlerin kaybolması: Tarihsel olarak, denetçiler muhasebe sistemlerinde meydana gelen olayları belgeleyen basılı kağıtlar üzerinden denetimleri yürütmüşlerdir. Muhasebe sistemlerindeki hata ve yolsuzluklara ilişkin bu kağıt belgeler esas alınmış ve referans gösterilmiştir. Düzgün tasarlanmamış bir muhasebe sistemi muhasebe işlemlerini kaydetmede yetersiz kalabilir. Eşzamanlı denetim teknikleri muhasebe sistemlerinin işlemleri tam ve doğru kaydedip kaydetmediği konusunda güvence verir.

Muhasebe işlem süreçlerinin karmaşık olması: Denetçilerin bir uygulama sistemini anlamada kullandıkları yol önemli bir muhasebe işleminin sistemde izlediği süreci takip etmektir. Manuel sistemlerde bu tekniği kullanmak basittir. Bilgisayar sistemlerinin artan kullanımı ile uygulama sistemleri daha karmaşık hale gelmiştir ve denetçilerin bir işlem hakkında kanıt toplaması ve bu kanıtları anlaşılır şekilde bir araya getirip raporlaması için eş zamanlı denetim tekniklerine ihtiyacı vardır.

Hata ve usulsüzlüklerin zamanında belirlenmesi: Bilgisayar sistemlerinin hızlı işlemesi nedeniyle hata ve usulsüzlükler zamanında tespit edilmesi zordur. Bunun sonucu olarak kuruluşlar önemli kayıplara maruz kalabilirler. Geleneksel geriye dönük denetim hata ve usulsüzlüklerin zamanında tespit edilmesinde yetersiz kalmaktadır. Denetçiler meydana gelen hata ve usulsüzlükleri zamanında tespit etmek için eşzamanlı denetim tekniklerini kullanmaktadırlar.

Bilgi sistemlerinin artan entegrasyonu: Bilgi sistemleri hem organizasyon içinde hem de organizasyonun dışındaki sistemlerle giderek daha da entegre hale gelmektedir. Bunun sonucu olarak bilgi sistemlerinin karmaşıklığı artmaktadır. Eş zamanlı denetim teknikleri bilgi sistemlerinin farklı bileşenlerinin diğer sistemleri nasıl etkilediği konusunda denetçiye yardımcı olur.

Bilgi sistemlerinin farklı yerlerde konumlandırılmış olması: Bilgi sistemlerinin dağınık olması bu sistemleri destekleyen fiziksel alt yapının farklı olmasına, heterojen donanım ve yazılım platformlarına neden olmaktadır. Denetçi, bilgi işlem süreçlerini incelemede dağınık halde olan tüm sistemleri incelemede yetersiz kalabilir. Bu durumda eşzamanlı denetim teknikleri uzak sistemlere monte edilebilir.

Hata ve usulsüzlüklerin etkisinin artması: Sistemlerin giderek daha entegre hale gelmesi meydana gelecek hata ve usulsüzlüklerden kaynaklanacak kayıpları arttırmaktadır. Örneğin tek bir sistem içinde bir bilgisayar virüsünün olması iletişim ağları üzerinden diğer sistemlere de ulaşabilir ve etkileyebilir.

Sistemlerde Entropi bulunması: Tüm sistemler bozulma ve çökme eğilimi gösterirler. Bilgi sistemleri de sistem tasarım hataları veya programlama hataları nedeniyle yavaş işlemeye, etkinliğini ve verimliliğini kaybetmeye yüz tutabilir.

Önemli eşzamanlı denetim teknikleri şunlardır:

1. Entegre test tesisi tekniği
2. Enstantane tekniği (snapshot),
3. Sistem kontrol denetim inceleme dosyası ve
4. Sürekli ve aralıklı simülasyon.

1. Entegre test tesisi tekniği (Integrated Test Facility): Entegre test tesisi tekniği, uygulama sistemlerinin verileri tam, doğru ve tutarlı bir şekilde işleyip işlemediğini test etmek için hayali veriler, hayali olaylar kurup giriş yapılarak sonuçlarının araştırılmasıdır. Örneğin bordro sisteminin denetiminde denetçi hayali bir kişi oluşturarak sisteme girişini yapar ve bordro sisteminin beklenen sonuçları verip vermediği araştırılır.

2. Enstantane tekniği (Snapshot): Enstantane tekniği işlemlerin işleyiş şeklini incelemekte ve fotoğrafını çekmektedir. Belirlenmiş işlemler enstantane sürecini başlatan bir özel kod ile işaretlenerek bilgisayar programındaki denetim modülleri; bu işlemleri ve bu işlemlerin ana dosya kayıtlarını faaliyetlerinden önce ve sonra kaydetmektedir. Enstantane verileri özel bir dosyada kaydedilmekte ve denetçi tarafından her uygulama adımının düzgün çalışmış olduğunu onaylamak için gözden geçirilmektedir.

3. Sistem kontrol denetim inceleme dosyası (System control audit review file-SCARF): Denetçinin önemli gördüğü hesap alanlarına bir denetim yazılımı yerleştirilmesi ve bu alanda denetlenen kuruluş tarafından yapılan işlemlerin

kayıtlarının tutulması ve gerektiğinde incelenmesini kapsamaktadır. Örneğin 1990 yılında bir sigorta şirketi çalışanı poliçe sahibi müşterilerden birinin adını ve adresini kendi adı ve adresi ile değiştirerek usulsüz olarak fonları çekmiş ve para transferinde bulunmuştur. Bu şekilde gerçekleşen usulsüz işlemler SCARF yöntemiyle tespit edilebilmektedir.

4. Sürekli ve aralıklı simülasyon (Continuous and Intermittent Simulation-CIS): Uygulama sistemlerinin veri tabanı yönetim sistemlerindeki bir bilgiyi güncellemesi veya uygulama dosyalarını sorgulamasına ilişkin kayıtların tutulmasıdır. SCARF yönteminde sıra dışı işlemlerin tespitinde uygulama sistemleri içine kurulmuş denetim modülünden yararlanılırken CIS yönteminde veri tabanı yönetim sistemleri içine kurulmuş modüllerden yararlanılır. Örneğin bir kredinin müşteri tarafından vadesinden önce ödenmesinde ödenecek tutarı hesaplayan bilgisayar uygulamasının doğru çalışıp çalışmadığından endişe eden bir denetçi düşünün. Bu durumda veri tabanı yönetim sistemi bu işlemi denetçinin ilgi alanında olduğu için bu işlem kayıt edecektir. Kaydedilen bu işlem denetim modülünden geçirilerek geri ödeme miktarı hesaplanacak ve denetim modülünde hesaplanan tutar ile uygulama sistemi tarafından hesaplanan tutar karşılaştırılacaktır. İki tutar arasında fark olması durumunda bu işlemin denetçiye raporlanması için denetim dosyasına atılacaktır.

2.4.9. Bilişim Teknolojisindeki Gelişimin Denetime Etkisi

Kuruluşların varlığını sürdürmesi ve uzun dönem hedeflerini gerçekleştirmesinde bilginin ve bilgi teknolojilerinin yönetimi önem taşımaktadır. Bilgiye ve bilgiyi üreten sistemlere olan ihtiyacın gün geçtikçe artması kuruluşların bu sistemlere olan bağımlılığını arttırmıştır.

Bilgi sistemleri düşük maliyetlerle kısa zamanda ve daha kaliteli bilgi üretmekte, hizmet sunulmasını sağlamakta ve dolayısıyla yöneticilerin bilgi sistemlerine olan talebini arttırmaktadır. Diğer taraftan, artan bilgi sistemlerine yönelik suçlar, bilgi savaşları, siber terörizm gibi tehditler bilgi teknolojileri konusunda bilinçlenmeyi ve önlem almayı arttırmıştır. Gelişen teknolojinin örgütleri yeniden şekillendirdiği günümüzde teknolojik

uygulamaların yeni iş fırsatları ortaya çıkarması ve daha düşük maliyetlerle daha kaliteli hizmet sunulabilmesi teknolojiye olan ilgiyi daha da arttırmaktadır.

Bir kurumda bilişim sistemlerinin kullanılmasıyla şu avantajlar sağlanabilir:

- Doğru ve güvenilir bilgi üretilmesi,
- Verilere kolay erişim sağlanması,
- Veri girişi ile manuel ortamda yapılan birçok ara işlemin ortadan kalkmasıyla işlemlerin otomatik yapılması,
- Veri depolanmasında yer tasarrufu sağlanması,
- Karmaşık işlemlerin daha kolayca analizi,
- İş verimliliğinin artması ve maliyetlerin düşmesi.

Teknolojik gelişimlerin denetim üzerinde başlıca iki yönlü etkisinin bulunduğunu söylemek mümkündür:

1. BDDT'lerin denetimlerde kullanılması
2. Yoğun bilişim sistemlerinin kullanılmasının yeni risk alanları oluşturması.

Bilişim sistemlerinin varlığı temel denetim amaçlarını değiştirmez. Bununla birlikte, denetim kanıtını, denetim izini ve iç kontrol ortamını değiştirmesi, yeni suç ve hata yapma mekanizmaları ve fırsatları ortaya çıkarması denetçinin riskler hakkındaki görüşleri üzerinde etkili olur. Denetim sürecinde, tekniğinde, kanıtlarında ve en önemlisi denetim anlayışında değişimlerin yaşanmasına neden olabilmektedir. "Denetlenen kurumlarda bilişim teknolojisi kullanımı;

- Denetim kanıtı ve denetim izini değiştirir,
- İç kontrol ortamını değiştirir,
- Yeni suç ve hata yapma mekanizmaları ve fırsatları ortaya çıkarır ve yeni denetim prosedürleri oluşturulmasına sebep olur." (Özkul, 2002).

Bu değişim, denetçinin yeni duruma uyum sağlamasını ve elektronik bilgi ortamlarının denetim sürecini nasıl etkileyebileceğini dikkate almasını gerektirmektedir. Bilişim teknolojilerinin denetlenen kurumlarda yoğun şekilde kullanılmasının beraberinde

getirdiği riskleri makul seviyeye düşürecek kontrol mekanizmalarının kurulması ve belirli standartlar çerçevesinde bu kontrollerin kurulup kurulmadığının denetlenmesi gerekliliği bulunmaktadır.

Bilgisayar sistemlerinin denetiminde güvenilirliğe ilişkin kanıt toplama işi manuel sistemlere ilişkin kanıt toplama işinden daha zor ve karmaşıktır. Denetçiler bilgisayar sistemlerinde manuel sistemlerde olmayan çeşitli ve karmaşık iç kontrol teknolojileri karşılaşmaktadırlar. Örneğin bir disk sürücünün tam ve doğru çalışıp çalışmadığını ortaya koymak için bir takım donanımsal kontrollere ihtiyaç vardır. Yine aynı şekilde manuel sistemlerde olmayan sistem geliştirme ve iyileştirme kontrolleri bilgisayarlı sistemlerinin denetlenmesinde test edilmesi gerekmekte ve bu kontroller için denetim prosedürleri geliştirilmektedir. Diğer taraftan denetçi yeterli kanıt toplayabilmek için bu kontrollerin yapısını iyi anlaması gerekir.

Donanım ve yazılımlar sürekli geliştiği ve yenilendiği için kontrol teknolojilerinin anlaşılması denetçi zorlamaktadır. Örneğin günümüzde veri transferi ve veri iletişimi hızla gelişmekte ve buna bağlı olarak veri gizliliğine yönelik kriptolama çalışmaları da gelişmektedir. Denetçiler iletişim ağlarının güvenilirliğine ilişkin değerlendirme yaparken bu gelişmeleri takip etmesi ve gelişmelere ayak uydurması gerekir.

Gelişmekte olan kontrol teknolojileri denetçilerin kontrollerin güvenilirliğine ilişkin kanıt toplamasını da güçleştirmektedir. Bazı durumlarda denetçiler manuel yollarla kanıt toplamakta yetersiz kalabilmektedirler. Bu gibi durumlarda kanıt toplayabilmek için bilgisayar sistemlerine ihtiyaç duyarlar. Bu amaçla genelleştirilmiş denetim yazılımları kullanılarak denetçilerin manyetik verilere erişmesi, gerekli analizleri yaparak kanıt toplaması kolaylaştırılmıştır.

Benzer şekilde veri iletim ağlarının yeterli düzeyde denetlenmesi için yeni denetim araçlarına ihtiyaç duyulmaktadır. Günümüzde bakıldığında bu denetim araçlarının gelişmesinin teknolojinin gerisinde kaldığı görülmektedir. Bu nedenlerle denetçiler kanıt toplamada bir takım tavizler vermek durumunda kalmaktadırlar.

Bilgisayar sistemlerinin ve iç kontrol teknolojilerinin karmaşıklığı karşısında denetçilerin sistemlerin güvenilirliğine ilişkin değerlendirme yapabilmesi ve kontrol

mekanizmalarının güçlü ve zayıf yönlerini ortaya koyabilmesi güçleşmiştir. Şöyle ki denetçiler ilk olarak bir kontrolün düzgün çalışıp çalışmadığına karar vermek durumundadır. İkinci olarak, denetçi kontrolün güçlü ve zayıf yanlarının sistem içindeki etkilerini izleyebilmesi ve değerlendirmesi gerekir. Örneğin ortak paylaşıma açık verilerin etkilerinin boyutunu belirlemek güçtür. Yine, tek bir veri girişi sistemde birçok veri tabanı etkileyebilir, güncellemeye ve değişime neden olabilir. Denetçinin yanlış bir veri girişinin bütün kullanıcılar için ne sonuçlar doğuracağını ve nereleri etkilediğini hesaplayabilmesi gerekir.

Bilgisayar sistemlerine ilişkin kanıtların değerlendirilmesi de denetçiler için zordur. Çünkü bu sistemlerdeki bir hatanın sonucu manuel sistemlerdeki bir hatanın sonucundan çok daha büyüktür. Yine gerçekleşmiş bir hatanın düzeltilmesi veya hata veren bir programın düzeltilmesi manuel sistemlere göre daha maliyetlidir. Bu nedenlerle yüksek kaliteli bilgisayar sistemlerinin kurulması ve düzgün işletilmesi sağlam bir iç kontrol ortamı için gereklidir. Denetçi, kontrollerin veri bütünlüğünün sağlanması, varlıkların korunması, etkin ve verimli şekilde işletilmesi amaçlarına uygun olup olmadığı konusunda çalışma yapmak ve güvence elde etmek zorundadır.

2.4.10. Bilgisayarların İç Kontroller Üzerindeki Etkisi

Kurum varlıklarının korunması, veri bütünlüğünün sağlanması, sistemlerin etkin ve verimli işlemesine yönelik hedeflere ulaşılması ancak kurum yönetiminin etkin bir iç kontrol sistemini kurması ile mümkündür. “Genel olarak bakıldığında iç kontrol sistemi görevlerin ayrılığını, yetkilendirmenin ve sorumlulukların net olarak yapılmasını, yüksek kaliteli personel istihdamı ve eğitimini, yetkilendirme sistemini, yeterli düzeyde dokümantasyon ve kaydı, kurum varlıkları ile kayıtları üzerinde fiziksel erişim kontrollerini, yönetimin gözetimini, performansa yönelik bağımsız kontrolleri ve periyodik olarak fiili durum ile kaydi durumun karşılaştırılmasını içerir.” (Weber, 2013: 37).

Bilgisayar sistemlerinde de etkin bir iç kontrol ortamı için yukarıda sayılan iç kontrol ortamının bütün bileşenlerinin olması ve uygulanması gerekir; ancak bilgisayar ortamlarında fiziksel ortamlardan farklı olarak anılan bileşenlerin uygulamaya

geçirilmesi birkaç açıdan farklılık göstermektedir. Dolayısıyla bu bileşenler bilgisayar kullanılan çevrelere göre uyarlanarak uygulanmaktadır.

2.4.10.1. Görevlerin ayrılığı

Manuel sistemlerde işlemlerin gerçekleştirilmesi, kaydedilmesi ve varlıkların korunması gibi işlemlerin her biri için ayrı bir personel görevlendirilir. Temel bir kontrol yöntemi olarak görevlerin ayrılığı ilkesi hata ve yolsuzlukları önler veya ortaya çıkmasını sağlar; ancak bilgisayar sistemlerinde geleneksel görevler ayrılığı ilkesi uygulanamaz. Örneğin bir bilgisayar programı tedarikçiden alınan fatura karşılığında gerekli hesaplama ve mahsupları yaparak muhasebe kayıtlarını gerçekleştirebilir ve kalan tutar için borç kaydedebilir veya çek düzenleyebilir. Böylece manuel sistemlerde birden fazla personelin katılımını gerektiren işler otomatik sistemlerde tek bir program ile gerçekleştirilebilir.

Görevlerin ayrılığı ilkesi gereği örnekte anılan her bir işlem ayrı programlar tarafından gerçekleştirilse bu defa sistemler yavaş işleyen, verimsiz, insan kaynağına ihtiyaç duyan sistemler haline dönecektir. Bu gibi durumlarda görevlerin ayrılığı ilkesi farklı formlarda uygulanmalıdır. Eğer bir program doğru şekilde işliyorsa ve denetçi programın doğru işlediğine kanaat getirdiyse görevlerin ayrılığı ilkesi için bakılacak husus programı işleten ile programın yazılımını yapan veya programda değişiklik yapma yetkisine sahip olan kişilerin aynı kişiler olup olmadığına dikkat etmek olacaktır. Eğer bu işleri yapma yetki ve sorumluluğu aynı kişilerdeyse görevlerin ayrılığı ilkesi ihlal edilmiş olur, iç kontrol ortamının sağlamlığı konusunda şüphe oluştur. Denetçinin bu durumu risk değerlendirmesinde dikkate alması ve bulgu olarak değerlendirmesi gerekir.

Mini bilgisayar ve mikro bilgisayar ortamlarında görevlerin ayrılığı ilkesinin uygulanması daha da zordur. Çünkü bu bilgisayarlar bazen kullanıcılarına programlar üzerinde değişiklik yapma yetkisi verebilir ve kullanıcılar verileri kolayca değiştirebilirler. Ayrıca yapılan değişikliklerin kayıtları da tutulmayabilir.

2.4.10.2. Yetki ve sorumlulukların dağıtılması

Manuel ve bilgisayar sistemlerinde yetki ve sorumlulukların çizgilerinin net olarak belirlenmesi temel bir kontrol hedefidir. Ne var ki bilgisayar sitemlerinde yetki ve sorumlulukların net belirlenmesi çok zordur; çünkü kaynaklar birçok kullanıcı tarafından ortak olarak paylaşılmaktadır. Örneğin veri tabanı yönetim sisteminin amaçlarından biri birçok kullanıcıya aynı anda aynı verilere ulaşma imkanını sağlamaktır. Böylece birden fazla yerde aynı verileri saklama ve korumada karşılaşılan zorluklar azaltılmış olur. Birden çok kullanıcının erişiminde olan verilerin herhangi bir şekilde bütünlüğü bozulursa bu bozulmalara sebep olanları belirlemek, sorumluluklarını tespit etmek ve hataları düzeltmek genellikle zordur. Bazı kurumlar bir kullanıcıyı veya belirli kullanıcıları bu verilerin sahibi olarak belirleyerek bu sorunu aşmışlardır. Böylece verinin sahibi olan kullanıcı veriyi değiştirme, kaldırma, paylaşıma açma gibi yetkileri elinde bulundurarak verinin bütünlüğüne ilişkin tüm sorumluluğu üzerlerinde taşımaktadırlar.

2.4.10.3. Uzman ve güvenilir personel

Bilgisayar tabanlı bilgi sistemlerinin geliştirilmesi, uygulamaya konulması, yürütülmesi, bakım ve destek çalışmalarının yapılması çalışmalarını yürüten personeller genellikle ağır sorumluluk altında olan personellerdir. Örneğin bir sistem analisti, ileri teknoloji içeren ve yüksek maliyetli makinelerin kurum için uygun olup olmadığı konusunda yönetime görüş vermek durumundadır. Benzer şekilde bir bilgisayar operatörü, sistem yedeklerini alırken veya sistemi işletirken kritik yazılımların, verilerin korunması konusunda önemli sorumluluk almaktadır.

Bilgi sistemlerinden sorumlu personelin taşıdıkları sorumluluk ve yük manuel sistemlerden sorumlu personelin taşıdığı yük ve sorumluluktan daha fazladır. Kuruluşların bu alanlarda uzman ve güvenilir personeli bulmaları ve istihdam etmeleri genellikle zordur. Çoğu ülkede uzman bilişim sistemleri personeli yıllarca yetersiz kalmıştır. Ayrıca uzman ve güvenilir personeli belirlemek ve yetkinliklerini ölçmek kuruluşlar için kolay da olmamaktadır. Bilişim sistemleri sektöründe yüksek miktarda bir devinim vardır, dolayısıyla yöneticilerin doğru personeli seçmek için fazla vakitleri

yoktur. Diğer taraftan bilişim sektöründe çalışan personelin etik anlayışlarının az olduğu, bazılarının da üzerlerinde fazla kontrolü istemedikleri bilinmektedir.

2.4.10.4. Yetkilendirme sistemi

Yönetimler işlemlerin yürütülmesinde iki çeşit yetkilendirme usulüne başvurmaktadır. Birinci usul, kuruluş çalışanlarının uyması için genel politikalar geliştirerek yetkilendirme yapmaktır. Örneğin, ürün satışında çalışan personel için fiyat listesi belirlenerek personelin bu fiyat listesine göre satış işlemlerini gerçekleştirmesi sağlanır. İkinci usul, belli işlemler için özel yetkilendirme uygulamasıdır. Örneğin önemli yatırım varlıklarının alınması yönetim kurulunun kararına bağlanabilir.

Manuel sistemlerde denetçi, personelin çalışmalarını gözlemleyerek yetkilendirme prosedürlerinin yeterli olup olmadığını değerlendirir. Bilgisayar sistemlerinde yetki prosedürleri bilgisayar programlarının içine gömülüdür. Örneğin satış bölümünde yer alan sipariş giriş modülü herhangi bir müşterinin hangi fiyattan ürünü alacağını belirleyebilir. Bu durumda denetçi personelin çalışmalarını izlemenin yanında sistemin doğru işleyip işlemediğine de bakmak ve incelemek zorundadır.

Bilgisayar sistemlerinde personele verilen yetkilerin yönetimin istediği bir düzeyde bir yetki olup olmadığına karar vermek denetçi açısından zordur. Örneğin genel erişim diliyle yetkilendirilmiş bir kullanıcının hangi verilere ulaşabileceğini veya hangi verilere ulaşamayacağını belirlemek zordur. Kullanıcılar bir takım sorgulamalar formülüze ederek veri tabanında erişememesi gereken bilgilere veya gizli bilgilere ulaşabilirler.

2.4.10.5. Yeterli belge ve kayıt

Manuel sistemlerde gerçekleştirilen denetim faaliyetlerinin izlerinin yeterli belge ve kanıtlarla desteklenmesi gerekir. Ancak bilgisayar sistemlerinde işlemler belgeye dayanmadan gerçekleştirilebilir. Örneğin online sipariş sistemlerinde müşteriler siparişlerini internet veya telefon aracılığıyla doğrudan sisteme girebilir ve ürünlerini alabilirler. Benzer şekilde bazı işlemler bilgisayar sistemleri tarafından gerçekleştirilebilir. Örneğin stok ikmal programı stok seviyesinin belirlenen miktarın altına düşmesi durumunda otomatik olarak alım siparişi verebilir. Dolayısıyla denetim

açısından bakıldığında bu tür işlemlerde belgeye rastlamak ve bu belgeler üzerinden denetim yapmak mümkün değildir.

Belgeye dayalı kanıtların olmaması denetim açısından bir sorun teşkil etmemektedir; ancak denetçinin bu alanlarda denetim yaparken bilgisayar sistemlerinin tüm işlemleri kayıt altına aldığı ve kayıtlara erişimin kolaylıkla mümkün olması konusunda güvence elde etmelidir. Doğru tasarlanmış bilgisayar sistemlerinde elde edilen denetim kanıtı manuel sistemlerde elde elde edilen denetim kanıtına göre daha geçerlidir; ancak bütün bilgisayar sistemleri düzgün kurgulanmamıştır. Bazı yazılımlar doğru ve tam bir denetim izi için yeterli erişim kontrolleri ve log donanımlarını içermemekte ve kontrol problemleri doğurmaktadır.

2.4.10.6. Varlık ve kayıtlar üzerinde fiziksel kontroller

Gerek manuel sistemlerde gerekse bilgisayar sistemlere varlık ve kayıtlara fiziksel erişimin kontrol altında tutulması kritik öneme sahiptir. Bilgi sistemi varlıkları yoğun olarak belli bir bölgede tutulan kuruluşlarda manuel sistemlerden farklı olarak bütün kritik bilgiler tek bir bölgede bulunur. Manuel sistemlerde suç işlemek isteyen bir kişi farklı fiziksel bölgelerde bulunan kayıtlara erişmek zorundadır. Dolayısıyla bilgisayar sistemlerinde yeterli fiziksel kontroller olmazsa kayıtlara usulsüz erişim daha kolay olabilmektedir.

2.4.10.7. Yönetimin yeterli gözetimi

Manuel sistemlerde yönetim tarafından personelin faaliyetlerinin gözlemlenmesi genellikle basit düzeydedir; çünkü yönetici ve personel aynı fiziksel mekan içinde bulunmaktadır. Bilgisayar sistemlerinde veri iletişim araçları personelin müşterilere daha yakın olmasını sağlayacak şekilde kullanılmakta ve yönetim tarafından personelin gözetimi daha uzaktan yapılabilmektedir. Bu sistemlerde yönetimin gözetim görevini yerine getirmesi için yazılımlar geliştirilerek programlar içine yerleştirilmekte ve personelin gözetimi sağlanmaktadır.

Birçok işlem elektronik ortamda gerçekleştirilmesi ve yapılan işlemlerin takibi için yöneticinin sık sık sisteme giriş yapması gerekmesi nedeniyle bilgisayar sistemlerinde personelin çalışmalarını izlemek daha zordur.

2.4.10.8. Performans üzerinde bağımsız kontrol

Manuel sistemlerde bağımsız kontrole ihtiyaç duyulmaktadır; çünkü bu sistemlerde personelin prosedürleri unutması, hata yapması, dikkatsiz davranması veya art niyetli olarak yazılı kurallara uymaması olasılığı her zaman vardır. Bilgisayar sistemlerinde ise durum biraz daha farklıdır. Şöyle ki bir bilgisayar sisteminde program kodları doğruluk, tamlık, yetkilendirme açısından düzgün kurgulanmışsa sistem donanım ve yazılım hataları verse bile program düzenlenmiş prosedürleri yerine getirmeye devam edecektir. Dolayısıyla programların performansı üzerinde yapılacak bağımsız ölçümlerin pek önemi kalmamaktadır. Görüldüğü gibi performans üzerinde bağımsız ölçümlerin pek yararı olmadığından denetçi program geliştirmelerine ilişkin kontrolleri, modifikasyonları, programların işletilmesi ve desteklenmesine yönelik faaliyetleri iyi değerlendirmelidir.

2.4.10.9. Muhasebe kayıtları ile varlıkların karşılaştırılması

Kayıtlara ilişkin verilerle varlıklar tamlık ve doğruluk açısından karşılaştırılmalı ve kaydi durum ile fiili durum arasındaki olumlu veya olumsuz farklar araştırılmalıdır. Manuel sistemlerde bağımsız bir görevli karşılaştırma amacıyla verileri hazırlar ve karşılaştırmayı yapar. Bilgisayar sistemlerinde ise bu karşılaştırmalar için geliştirilmiş yazılımlar kullanılır. Örneğin, envanter listesi envanterin bulunduğu depoya göre yazılım aracılığıyla ayrıştırılarak sayım işleri kolaylaştırılabilir. Burada dikkat edilmesi gereken programın kullandığı veri dosyalarının yetkisiz erişimlerin engellenmiş olmasıdır. Eğer veri dosyalarına yetkisiz erişimler ve çeşitli modifikasyonlar yapılırsa yolsuzlukların ortaya çıkması mümkün değildir. örneğin belli bir depodan envanterin çalınması durumunda eksik envanter yetkisiz erişimlerle kapatılabilir. Vurgulamak gerekirse, program kodlarının geçerliliğine ilişkin iç kontrol mekanizmasının olması gerekir; çünkü geleneksel görevlerin ayrılığı ilkesini karşılaştırma maksadıyla verilerin hazırlanmasına uygulamak mümkün değildir.

2.4.11. Mali Denetim ve Bilgi Teknolojileri Denetimi İlişkisi

Bilgisayar sistemlerinin iş hayatında yoğun şekilde kullanılması bir takım teknolojik riskleri de beraberinde getirmekte ve bu yeni sistemlerde üretilen çıktıların doğruluğunun kontrol edilmesi ihtiyacını ortaya çıkarmaktadır. “Denetçilerin etkin bir denetim yapmak için ihtiyaç duydukları bilgi ve belgeleri sanal ortamdan elde etmeleri sonucunda, denetimde kullanılacak olan bu bilgilerin doğruluğu hakkında güvence verilmesi gerekmektedir. Bu güvence olgusu bilgi teknolojileri denetiminin gerekliliğini ortaya çıkartmıştır.” (Topkaya, 2011: 118).

Denetçinin üzerinde çalıştığı verilerinin güvenilirliği ve tamlığı denetim sonuçlarına olan etkisi nedeniyle önemlidir. Eksik, hatalı, gereksiz veriler üzerinden yapılacak bir denetim tarafsızlığını ve güvenilirliğini yitirecektir. Bilginin tamlığına ve güvenilirliğine ilişkin bilişim sistemlerinden kaynaklanacak risklerin kabul edilebilir seviyeye indirilebilmesi bilgi teknolojilerinin denetimi ile mümkün olmaktadır.

Bilgi teknolojileri denetimi asıl olarak mali denetim çalışmalarının bir parçası durumundadır. Mali denetim çalışmalarının planlama aşamasında, kurumun bilişim sistemleri varlıklarının tanınması ile başlatılacak temel düzeyde bilişim sistemleri denetimleri sonucunda kurum tarafından tesis edilen kontrollerin, kurumun sahip olduğu bilgilerin güvenliğe, güvenilirliğe ve tamlığa ilişkin gerekli nitelikleri sağlayıp sağlamadığını ortaya koyar. Mali denetim çalışmaları sırasında denetim yaklaşımını etkileyebilecek sonuçlar ortaya konduğu takdirde, bu sonuçlar dikkate alınarak denetim çalışmalarının yürütülmesi gerekliliği doğacaktır. Mali denetim ekiplerinin, kurumun sahip olduğu bilgileri güvenli bir şekilde koruduğunu tespit etmeleri tek başına yeterli değildir. Kurumun sahip olduğu ve mali denetime esas teşkil edecek bilgilerin aynı zamanda güvenilir ve tam olduğunun da tespit ve teyit edilmesi gerekecektir. Aksi takdirde bilgiye ulaşmanın güç olduğu veya eksik bilginin var olduğu durumlarda yapılacak her türlü denetim çalışmasının sonuçları sorgulanmaya açık hale gelecektir. (Akbaş, 2011: 14).

Teknolojide yaşanan gelişmelerin sağladığı faydalardan istifade etmek amacıyla günümüzde bilişim sistemleri hemen hemen tüm kurumlar tarafından yoğun bir şekilde

kullanılmakta olup, gerçekleştirilen tüm işlemlerde dijital veriler kullanılmaktadır. Bilişim sistemlerinin bu şekilde yaygın kullanımı beraberinde teknolojik riskleri de getirdiğinden bu riskleri minimize edecek, bilgisayarlaştırılmış verilerin güvenilirliğini kontrol edecek ve verileri sağlayan, işleyen ve raporlayan bilişim sistemleri denetimi bir zorunluluk haline gelmiştir. Çünkü yapılan denetimlerde bu veriler kullanılmakta olup verilerin hatalı veya yanlış olarak sistemden alınması sonucunda tüm denetim süreci sekteye uğrayabilecektir.

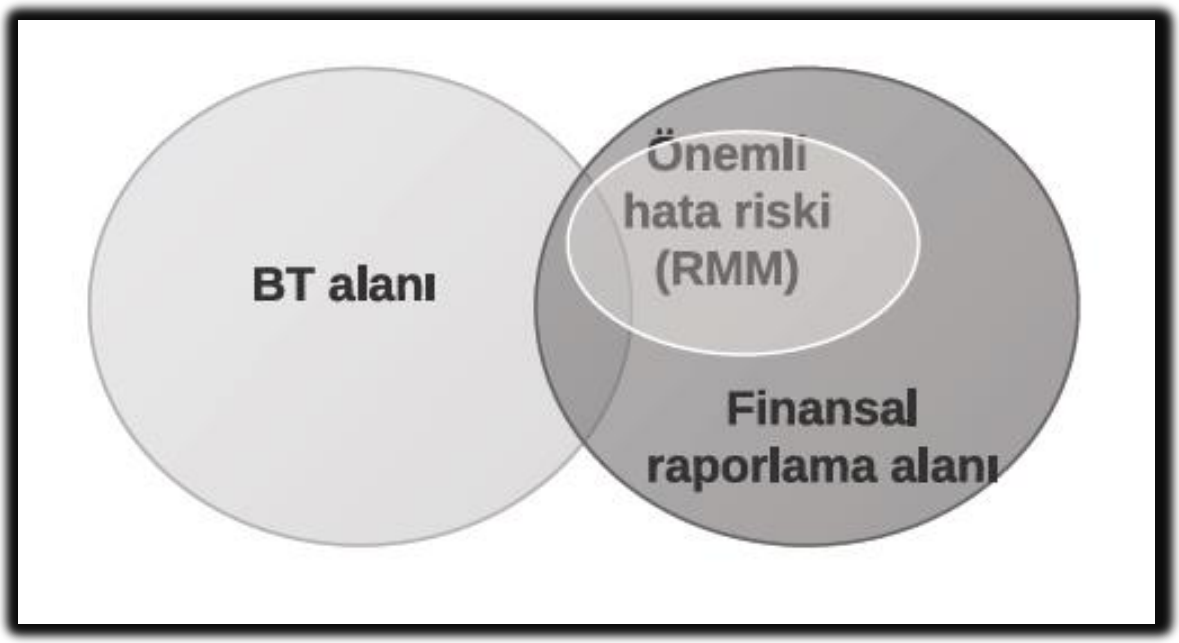
2.4.12. Mali Denetimde Bilgi Teknolojileri Denetimi Kapsamı Sorunu

İç denetim fonksiyonunun bir parçası olarak BT denetçisi bir kuruluşun BT portföyünü denetler. Kuruluş ne kadar büyükse BT alanı da o kadar çeşitli ve karmaşıktır ve ona göre farklı denetim teknikleri uygulanır. Bağımsız denetimlerde BT denetçileri, BT alanının sadece mali raporlamayı etkileyen hususlarını denetim konusu yaparlar. Sarbanes-Oxley Kanunun 404 üncü bölümüne göre halka açık şirketler ve mali tablolar denetimine tabi tüm kuruluşlar için finansal raporlamayı etkileyen kontrol ve BT kontrollerinin denetimi zorunludur.

Mali tablolar denetiminde, BT denetim kapsamının belirlenmesinde ortaya çıkan zorluk BT denetçilerinin BT alanı ve bileşenlerine ilişkin geniş kapsamlı bilgi edinme çabalarından kaynaklanmaktadır. Bu bilgi edinme çalışmaları iyi uygulama örneklerinin uygulanmasını, kriterlere, standartlara uyumun araştırılmasını, bileşenlerle ilgili modellerin geliştirilmesini ve çeşitli teknolojilere ilişkin kapsamlı bir bilgi birikiminin uygulanmasını gerektirir. BT denetçileri sistem geliştirme yaşam döngüsü, BT yönetişimi, erişim kontrolleri/BT genel kontrolleri, proje yönetimi, ağ, yazılım, iş sürekliliği gibi birçok alanda bilgi sahibidirler. Duruma göre BT denetçileri yazılı plan, görev paylaşımı, veri yedekleme gibi birçok noktaya bakmak ve test etmek durumundadır. Eğer BT denetimi BT denetimi için yapılıyorsa ve kuruluş karmaşık bir BT alanına sahipse çok sayıda denetim teknik ve prosedürlerin uygulanması gerekir ve bu şekilde yapılacak bir denetim genellikle iç denetim faaliyeti veya danışmanlık kapsamında yapılan bir denetim faaliyeti olur. Ancak söz konusu mali tablolar denetimi ise ve mali tablolar denetimi kapsamında bir BT denetimi yapılacaksa BT denetiminin kapsamı da ona göre farklı olacaktır.

Mali tablolar denetimi için yapılacak BT denetiminin kapsamının belirlenmesinde zorluk uygun bir denetim kapsamının belirlenmesidir. BT denetçileri mali tablolar denetiminde görevlerini yerine getirirken bütün bilgi birikimlerini ve teknikleri kullanmak isteyeceklerdir. Eğer mali tablolar denetimi için yapılan BT denetiminde denetçi mali tablolar denetimi yapıldığı gerçeğini dikkate almazsa gereksiz yere birçok prosedür ve test uygulayacaktır. “Denetimin kapsamını belirlemenin en iyi yolu ne çok ne de çok az denetim prosedürü belirleyerek risk odaklı bir denetim yaklaşımını benimsenmesidir (Risk-Based Audit- RBA).” (Singleton, 2009: 2)

Risk odaklı denetim yaklaşımı mali denetim alanını belirlemekle başlar. “Finansal raporlamada hangi manuel ve otomatik sistemler kullanılır, hangi hesaplar, işlemler ve açıklamalar finansal raporlamayı etkiler, finansal raporlama süreç döngüsünde hangi manuel ve otomatik süreçler işler” gibi sorular risk odaklı denetim yaklaşımında denetim kapsamının belirlenmesine yardımcı olur.



Şekil 2.3. Mali tablolar denetimde BT denetimi kapsamının belirlenmesi (Singleton, 2009: 3)

Mali tablolar denetimi kapsamında yapılacak bir BT denetiminde öncelikle BT alanında hangi bileşenlerin denetim kapsamı içinde olduğuna karar vermek gerekir. Mali denetim bütün BT alanlarını (IT Space) kapsamaz. Yukarıdaki şekilde görüldüğü gibi mali denetim alanı (Financial Reporting Space) BT alanının sadece bir kısmını kapsar.

Pratik bir bakış açısıyla, mali denetimin BT alanını kapsayan kısmı finansal raporlamaya ilişkin olan verilerin kaydedilmesi, işlenmesi, saklanması, verinin transferi gibi hususlar olmaktadır.

Mali denetimde BT denetiminin kapsamının belirlenmesi ilk önemli adımdır. Uygun denetim kapsamın belirlenmesinde mali tabloların taşıdığı yanlış beyan riski belirleyici rol oynar (risk of material misstatement-RMM). Yanlış beyan riski (RMM), denetlenen kurumun iç kontrol mekanizmasına bağlı olmaksızın, mali tabloların önemli olabilecek bir hata içerme olasılığı olan yapısal risk (inherent risk) ve mali tabloları etkileyebilecek önemli bir hatanın, kurumun iç kontrol sistemi tarafından zamanında önlenememesi, tespit edilememesi veya düzeltilememesi olasılığı olan kontrol riskinden (control risk) oluşur. Temel olarak BT denetçisinin sorumluluğu iki yönlüdür:

1. BT'nin finansal raporlama üzerindeki etkilerinden kaynaklanan riskleri tespit etmek ve
2. BT kontrollerinden kaynaklanan riskleri belirlemek.

Eğer bir kuruluş kendi yazılım uygulamalarını geliştirmişse ve bu uygulamalardan biri finansal raporlama sürecinde kullanılıyorsa BT denetim alanında finansal tablolara ilişkin bir risk var demektir (yazılım uygulamalarının geliştirilmesi riski). Bu risk finansal tablolarda bir yanlış bilgiye sebep oluyorsa mali denetim içinde değerlendirilmesi gerekecektir, aksi halde mali denetim için önemsiz bir risk olacaktır. Örneğin, BT denetimi için bilgi sistemlerin internet bağlantılarında sistemi dış saldırılara karşı koruyacak güvenlik duvarlarının olması ve güvenlik duvarının ataklara karşı düzgün işlemesi önemlidir. Finansal raporlama ile ilgili sistemlerin de internet yoluyla dış bağlantısı olduğundan mali denetim ile BT denetimi bu alanda kesişirler. Fakat finansal veriler etrafında erişim ve diğer gerekli kontroller varsa ve bu kontroller test edilmiş ve veri bütünlüğüne ilişkin güvence veriyorsa güvenlik duvarının olup olmaması ve test edilmesi mali denetim açısından bir anlam ifade etmeyecektir. Dolayısıyla BT denetim alanı ve mali denetim alanının kesişmesi yukarıdaki şekilde gözüken yanlış beyan alanına indirgenmiştir (RMM). Bu kesişme alanı finansal tablolarda yanlış beyana neden olabilir ve yüksek risk taşımaktadır.

Risk odaklı denetim yaklaşımı mali denetimin planlanmasında BT denetçisine uygun seviyede alt küme seçmesini ve daha az denetim prosedürünün uygulamasını gerektirir. Şekilde gözüken BT denetim alanı ile mali denetim alanındaki kesişme ne kadar genişse uygulanacak denetim prosedürleri de o kadar çok olacaktır.

2.4.13. Bilgi Teknolojileri Denetiminin Mali Denetime Katkısı

BT denetçileri, kuruluşların mali nitelikli iş süreçlerinde bilgisayar kullanmaya başladıkları zamandan beri mali denetimlere katkıda bulunmaktadırlar. İlk zamanlarda BT denetçilerinin kullandığı denetim prosedür ve teknikleri denetim alanında öncülük etmiş ve yaygın olarak kullanılmaya başlamıştır. Örneğin BT'nin bir denetim aracı olarak kullanılması (envanterin digital ortama geçirilmesi 1956), BT görev ayrımı-*segregation of IT duties* (1961), entegre test araçları-*integrated test facilities*, genelleştirilmiş denetim yazılımı-*generalized audit software* (bilgisayar destekli denetim teknikleri olarak da bilinir-BDDT-CAATs, 1967) gibi teknik ve yöntemler yoğun olarak mali denetimlerde kullanılmaktadır.

Uzun zamandan beri mali denetim konusundaki literatür, mali denetimlerde BT denetçilerine olan ihtiyacın önemine vurgu yapmıştır. 2001 yılında AICPA tarafından yayınlanan 94 No'lu denetim standartı-SAS 94, bilgi teknolojileri sistemlerindeki iç kontrolleri değerlendirmede uygun türde değerleme araçları kullanılması konusunda denetçilere yol göstermek üzere yürürlüğe girmiştir. Söz konusu denetim standardı, bilgisayar destekli denetim tekniklerinin belli bilgi teknolojileri ortamlarında belli bilgi teknolojileri kontrol türlerini test etmesi gerektiğini belirtmektedir. 2002 yılında yürürlüğe giren Sarbanes-Oxley Kanunu ile mali denetimlerde BT denetçilerine olan ihtiyaç artmıştır. Bu Kanunu göre halka açık şirketler ve mali denetime tabi tüm kuruluşlar için finansal raporlamayı etkileyen kontrol ve BT kontrollerinin denetimi zorunludur. 2006 yılında risk odaklı standartların benimsenmesinden sonra (Denetim Standartları-SAS 104-111) BT denetçilerine olan ihtiyaç daha da artmıştır.

BT denetiminin mali denetime olan ilk katkısı kontrol testleri alanındadır (test of controls). Mali denetim ekibi mali denetim sürecinde kontrol testlerinden elde ettikleri sonuçlara göre güvence vermektedirler. Güvence verebilmek için bilgisayar

ortamındaki otomatik kontrollerin etkili çalışıp çalışmadığının test edilmesi gerekir ki bu da BT denetçilerinin yardımıyla gerçekleşir. Otomatik kontrol testlerinin uygulanmasının denetime önemli katkısı vardır:

- İlk olarak otomatik kontrol testlerinin uygulanması denetimde etkinliği ve verimliliği arttırır (yüzde yüz test etme, daha az iş gücü emek kullanımı gibi).
- İkinci olarak bu testler sonucunda mali denetçi genel kontrollerin etkinliği konusunda yeterli güvence elde etmiş olur.
- Üçüncü olarak risk odaklı denetim standartları mali raporlama sürecindeki BT kontrollerinin düzgün tasarlanmasını ve uygulanmasını gerektirdiğinden bu standarda uyum araştırılmış olur.

Kontrol testleri, denetlenen kuruluşun yazılımlarının bir kopyası alınarak ayrı bir bilgisayar ortamında bir test verisi girerek sistemin nasıl işlediğini, kontrollerin düzgün işleyip işlemediğini araştırmak şeklinde de gerçekleştirilebilir; ancak yazılımlar kopyalanamıyorsa bu yöntemi uygulamak mümkün olmayacaktır.

BDDT'lerin kullanımı, mali denetimde BT denetçilerinin sıkça kullandığı bir diğer geleneksel bir yöntemdir. BDDT'lerin kullanımı genellikle veri madenciliği ve veri analizi ile ilişkilidir. Veri analizi (örneğin genellikle belirli anomaliler için test etme) hem kanıt toplama hem de belirli denetim amaçları için test uygulaması ile ilişkilidir. BDDT'ler BT denetçileri için en değerli denetim teknikleridir ve BDDT'ler daha da gelişmekte ve denetimde işlevliğini arttırmaktadır. Örneğin PDF dosyaları ve digital belgeleri artık BDDT'ler ile okunabilmekte ve güvenilir bir ekstraksiyon işlemi verileri ayrıştırarak analize tabi tutulabilmektedir.

Temel BT prosedürleri, BDDT ile yakın ilişkilidir ve temel denetim prosedürlerini desteklemek, tamamlamak ve geliştirmek için kullanılabilir. Örneğin BT denetçisi, mali yılın herhangi bir ayında ödenen faturaları çıkararak bir önceki ayda borç kaydedilmiş tutarlarla karşılaştırarak eksik kaydedilen borçların olup olmadığını ve doğru kaydedilip edilmediğini kısa zamanda ortaya çıkarabilir. Normalde böyle bir işlemin manuel olarak yapılması uzun zaman ve emek gerektirirken BT denetçisi bu işlemleri BT teknikleri ile kısa zamanda yapabilmekte ve yüzde yüz doğrulama sağlayabilmektedir.

BT denetimi, kurum yönetimine değer katar. Mali denetim sürecinde gerçekleştirilen BT denetimleri mali tabloları etkileyen işlem ve süreçler üzerine yoğunlaşır. Bu denetim sürecinde mali tabloları etkilemeyen BT ile ilgili aksaklıklar olabilir. Mali tablolara etkisi olmasa da yönetim bu tür aksaklıkları bilmek ve düzeltmek isteyecektir. Örneğin bir kuruluş uygulama ve sunucu/ağ düzeyinde mükemmel erişim kontrollerine sahipken zayıf çevresel ve fiziksel kontrollere sahip olabilir. Ancak mali verileri etkileyen başka kontroller varsa ve diğer kontroller düzgün işliyorsa BT denetçisi ve mali denetim ekibi için çevresel/fiziksel kontrollerin zayıf olması mali denetim için önemsiz olacaktır. Fakat kuruluş yönetimi, böyle bir zayıflığın olduğunu bilmeyi ve gerekli önlemleri almayı isteyecektir.

BT denetçileri mali tablolarda olabilecek yanlış beyan konusunda, BT ile ilgili yapısal risklerin ve kontrol risklerinin değerlendirilmesinde mali denetimlere her zaman katkıda bulunabilirler. Risk temelli denetim standartları, hesap bakiyelerinin incelenmesinde, muhasebe işlemlerinin sınıflandırılmasında ve raporlanmasındaki risk seviyesinin tespit edilmesinde denetçinin titiz çalışmasını gerektiren bir yaklaşım öngörmektedir ve her bir hesap alanı kendi risk seviyesi ile değerlendirilmektedir. BT denetçisi yüksek risk görülen alanlar için daha güçlü testler geliştirir, orta sevide riskli alanlar için orta düzeyde testler, düşük düzeyde riskli alanlar için de düşük düzeyli testler uygular.

Sonuç olarak BT denetçisi mali denetimlere emek tasarrufu sağlar, mali denetimin kalitesini arttırır ve kuruluş yönetimine değer katar.

2.4.14. Risk Değerlendirmesi, Bilgi Sistemleri ve Mali Denetim

ISA 400 No'lu Standarta göre, "Denetimin planlanması ve etkin bir denetim için, denetçinin muhasebe ve iç kontrol sistemi hakkında yeteri kadar bilgisi olması gerekir. Bu bilgiler denetçinin denetim riskini hesaplamasını sağlar. Denetçi denetim riskinin kabul edilebilir bir seviyeye düşürülmesi için gereken denetim işlemlerini mesleki kanaatini kullanarak belirler." ISA 400 ve 401 No'lu standartlar "İşletmenin İç Kontrolü Dâhil İşletme ve Çevresini Tanımak Suretiyle, Finansal Tablolardaki "Önemli Yanlışlık" Risklerini Belirlemesi ve Değerlendirilmesi" ne ilişkin 315 No'lu ISA standartı ve "Bağımsız Denetçinin Değerlendirilmiş Risklere Karşı Yapacağı İşler"e ilişkin ISA 330

No'lu Standart ile birlikte kaldırılmıştır ve ülkemizde Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından yayınlanarak 01.01.2013 sonrasında başlayacak hesap dönemlerinden itibaren uygulanmak üzere BDS 315 ve 330 olarak yürürlüğe girmiştir.

ISA 315 No'lu Standarta göre; İç kontrolde manuel veya otomatik unsurların kullanılması işlemlerin başlatılma, kaydedilme, işlenme ve raporlanma biçimlerini etkiler:

- Manuel bir sistemdeki kontroller, işlemlerin onaylanması ve incelenmesi gibi prosedürleri, mutabakatları ve mutabakata konu olan kalemlerin takibini içerebilir. Alternatif olarak bir işletme, işlemlerin başlatılması, kaydedilmesi, işlenmesi ve raporlanması için otomatik prosedürler kullanabilir; bu durumda elektronik ortamdaki kayıtlar kâğıt belgelerin yerini alır.
- BT sistemlerindeki kontroller, otomatik kontrollerin (örneğin, bilgisayar programlarına yerleştirilen kontroller) ve manuel kontrollerin bileşiminden oluşur. Ayrıca, manuel kontroller BT'den bağımsız olabilir, BT'nin ürettiği bilgileri kullanabilir veya BT'nin ve otomatik kontrollerin etkin şekilde işlemesini izlemekle ve istisnaları ele almakla sınırlı olabilir. Finansal tablolarda yer alacak işlem veya diğer finansal verilerin başlatılmasında, kaydedilmesinde, işlenmesinde veya raporlanmasında BT'nin kullanılması durumunda, BT sistem ve programları, önemli hesaplara karşılık gelen yönetim beyanlarına ilişkin kontrolleri içerebilir veya BT'ye dayanan manuel kontrollerin etkin şekilde işlemesi açısından kritik önem taşıyabilir.

Bir işletmenin iç kontrolündeki manuel ve otomatik unsurların bileşimi, söz konusu işletmenin BT'yi kullanım niteliğine ve karmaşıklığına göre farklılık gösterir. Genel olarak BT, işletmenin:

- Önceden tanımlanmış iş kurallarını tutarlı biçimde uygulamasına ve büyük hacimli işlem veya verileri işlerken karmaşık hesaplamaları yapmasına,
- Bilgilerin güncelliğini, erişilebilirliğini ve doğruluğunu artırmasına,
- Bilgilere ilişkin ek analizler yapmasını kolaylaştırmasına,

- İşletmenin politikalarını, prosedürlerini ve performansını izleme kabiliyetini geliştirmesine,
- Kontrollerin engellenmesi riskini azaltmasına,
- Uygulamalara, veri tabanlarına ve işletim sistemlerine güvenlik kontrolleri yerleştirerek görevlerin ayrılığı ilkesini etkin bir şekilde uygulama kabiliyetini artırmasına,

imkân sağlayarak işletmenin iç kontrolüne katkıda bulunur.

Bununla birlikte BT, işletmenin iç kontrolü açısından belirli riskler de barındırır. Bu risklere aşağıdakiler örnek olarak verilebilir:

- Verileri hatalı işleyen, hatalı verileri işleyen veya her ikisini de yapan sistem veya programlara güvenilmesi.
- Verilerin zarar görmesine veya veriler üzerinde uygun olmayan değişikliklerin yapılmasına yol açabilecek şekilde verilere yetkisiz erişim (yetkisiz veya var olmayan işlemlerin kaydedilmesi veya işlemlerin hatalı kaydedilmesi dâhil). Birden fazla kullanıcının ortak bir veri tabanına eriştiği durumlarda belirli riskler ortaya çıkabilir.
- BT personelinin, görevlerin ayrılığı ilkesinin bozulmasına sebep olacak şekilde, görev alanları çerçevesinde ihtiyaç duyduklarının ötesinde erişim ayrıcalıkları elde etme ihtimâli.
- Ana dosyalardaki verilerde yetkisiz değişiklikler.
- Sistem veya programlarda yetkisiz değişiklikler.
- Sistem veya programlarda yapılması gereken değişikliklerin yapılmaması.
- Uygun olmayan manuel müdahaleler.
- Veri kaybı ihtimâli veya gerektiğinde verilere erişilememesi

İşletmenin faaliyetlerini BT kullanarak yürütmesi ve BT sistemi ortamı dışında, işlemlere dair hiçbir dokümanın üretilmemesi veya saklanmaması durumunda denetçi, tek başlarına yönetim beyanı düzeyinde yeterli ve uygun denetim kanıtı sağlayabilecek etkin maddi doğrulama prosedürleri tasarlamanın mümkün olmadığını düşünebilir. Böyle durumlarda denetçi ilgili kontrollerin işleyiş etkinliklerine ilişkin yeterli ve uygun

denetim kanıtı elde etmek amacıyla kontrol testlerini tasarlar ve uygular. Denetçi kontrol testlerini tasarlarken ve uygularken, ilgili kontrolün etkinliğine daha fazla güvenmek istiyorsa daha fazla ikna edici denetim kanıtı elde etmelidir.

Denetçi kontrol testlerini tasarlarken ve uygularken:

a) Aşağıdakiler de dahil kontrollerin işleyiş etkinliğine ilişkin denetim kanıtı elde etmek için sorgulamayla birlikte diğer denetim prosedürlerini uygular:
   I. Denetlenen dönem boyunca kontrollerin ilgili zamanlarda nasıl uygulandığı,
   II. Kontrollerin uygulanmasındaki tutarlılık ve
   III. Kontrollerin kimler tarafından veya hangi vasıtalar kullanılarak uygulandığı.
b) Test edilecek kontrollerin diğer kontrollere (dolaylı kontrollere) bağlı olup olmadığına, diğer kontrollere bağlı olması durumunda ise, söz konusu dolaylı kontrollerin etkin şekilde işlediklerini destekleyen denetim kanıtı elde etmenin gerekip gerekmediğine karar verir.

Denetçi, kontrollere ilişkin planladığı güvenmeye uygun bir dayanak sağlamak amacıyla güvenmek istediği kontrolleri belirli bir zamanda veya dönem boyunca test eder. Bu aşamada önceki dönemlerde elde edilen denetim kanıtlarından yararlanılabilir.

BT işleyişinin doğasında var olan tutarlılık sebebiyle, otomatik bir kontrole ilişkin testin kapsamını genişletmek gerekli olmayabilir. Program değiştirilmediği sürece (programın kullandığı tablolar, dosyalar veya diğer sabit veriler dâhil) otomatik bir kontrolün tutarlı şekilde çalışması beklenebilir. Denetçi, otomatik kontrolün amacına uygun olarak çalıştığına bir kez karar vermesi hâlinde (kontrolün ilk uygulandığı zamanda veya daha sonraki bir tarihte karar verilebilir), kontrolün etkin şekilde çalışmaya devam edip etmediğini belirlemek amacıyla testler yapmayı düşünebilir. Bu testler; (BDS 330 No'lu standart)

- Programlarda yapılan değişikliklerin, uygun program değişiklik kontrollerine tabi tutulmaksızın yapılmadığının,

- İşlemlerin yürütülmesi için programın onaylı versiyonunun kullanıldığının,
- İlgili diğer genel kontrollerin etkin olduğunun belirlenmesini içerebilir.

Ayrıca bu tür testler, programlarda değişikliklerin yapılıp yapılmadığının (işletmenin değiştirilmeden veya bakım yapılmadan kullanılan paket yazılım uygulamalarını kullanması durumunda söz konusu olabileceği gibi) belirlemesini içerebilir. Örneğin denetçi, dönem içinde izinsiz erişim olup olmadığına dair denetim kanıtı elde etmek için BT güvenliğinden sorumlu birimin kayıtlarını tetkik edebilir.

Bilgisayarlı ortamlarda yapısal risk ve kontrol riski maddi yanlışlık olasılığı üstünde hem yaygın hem de özel bir etkiye sahiptir. Bu riskler; program geliştirilmesi ve korunmasını sistemlerin yazılım desteği, işletilmesi, bilgisayarlı bilgi sistemlerinin fiziksel güvenliği ve özel programlara giris üzerindeki kontrol gibi bilgisayarlı faaliyetlerdeki eksikliklerden kaynaklanmaktadır. Bu eksiklikler, bilgisayar tarafından yürütülen uygulamalara yönelecektir. Bu riskler; özel uygulamalarda, özel veri tabanları ya da dosyalarda veya özel faaliyetlerin islenmesinde hata ya da hile olasılığını artırabilir.

Bilgi teknolojilerinin yoğun kullanıldığı ortamlarda muhasebe verilerinin güvenilirliği BT sistemlerinin ve BT kontrollerinin güvenilirliğine bağlıdır. Verilerin bilgisayar tabanlı sistemlere doğru bir biçimde girilmesi, burada tam olarak işlenmesi ve güçlü bilgisayar kontrollerinin olması mali denetçilerin kontrol güvencesi elde etmelerini ve daha az bağımsız test uygulamalarını sağlamaktadır. Bunun aksine veri girişlerinde ve işlenmesinde aksaklıkların olması ve bunlar üzerindeki kontrollerin zayıf olması denetçilerin güvence elde etmek için daha fazla bağımsız test uygulamalarına neden olacaktır.

“Bilgi sistemleri kontrol prosedürlerinin incelenmesinde bir bağımsız denetçinin temel amacı, finansal raporlarda sunulan muhasebe verilerinin entegrasyonunun (bütünlüğünün) taşıdığı riskleri (herhangi bir kontrol zayıflığı ile ilgili) değerlendirmektir. Kontrollerin güçlü ve zayıf yönleri denetimin kapsamının belirlenmesinde etkili olmaktadır” (Yalkın, 2011).

Mali tablolar denetimi ile birlikte yürütülen BT denetiminde; denetçilerin görüş verdiği mali tablolar bilişim sistemlerinin ürettiği muhasebe verileri ile 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. İyi tasarlanmış ve uygulanmış bir BT denetimi aşağıdaki denetim hedeflerine ilişkin güvence oluşturur (Soltani, 2007: 295):

- ***Tamlık (completeness):*** Mali tabloların kapsadığı döneme ilişkin tüm muhasebe işlemleri kaydedilmeli ve ait olduğu mali tabloya yansıtılmalıdır.
- ***Doğruluk (accuracy):*** Tüm işlemler gerçek değeriyle kaydedilmiş olmalıdır ve ait olduğu mali tabloda uygun tutarlarla ifade edilmelidir.
- ***Zamanlılık (timeliness):*** Tüm işlemler meydana geldiği anda kayıt altına alınmalıdır. İşlemin meydana gelmesi ile kayıt edilmesi arasında önemli zaman farkının olması tamlık ve doğruluk kriterlerine ilişkin şüphe oluşturacaktır.
- ***Ölçülebilirlik (assessability):*** Mali tablolarda beyan edilen her konuyu ve beyanı destekleyen kaynak dokümanların olmasını ifade eder.
- ***Kronolojik sıra (chronological order):*** Bütün işlemlerin tarihi sırasına göre girilmesidir.
- ***Değişmezlik (inalterability):*** Kaydedilen işlemlerin sonradan geriye dönük olarak değiştirilememesi veya değiştirilmesine ilişkin kayıtların (log kayıtları) tutulmasıdır.

3. BÖLÜM

ÖRNEK BT DENETİM RAPORU

Bilgi teknolojileri ile ilgili örnek denetim raporu Türkiye'de faaliyet gösteren bir şirkete aittir. Bu raporun sunulmasında bilgilerin gizliliği nedeniyle şirkete ait bilgiler yer almamaktadır ve bazı bölümler çıkarılmıştır.

3.1. Giriş

Şirket hakkında özet bilgi: Kurumun yerel ağ ve İnternet üzerinden erişilebilir bilgi sistemlerinin mevcut güvenlik seviyelerinin belirlenmesini, olası problemleri ve çözüm önerilerini raporlamayı amaçlayan "Sızma Testleri" hizmeti, yukarıda önemi açıklanan sistemler için 2012 yılı Ekim ve Kasım ayları içerisinde gerçekleştirilerek bu rapor hazırlanmıştır. Gerçekleştirilen sızma testleri ve raporlama "yönetmelik" e uygun olarak ifa edilmiştir.

3.1.1. Sızma testinin hedefi

Bu çalışmanın hedefi, kapsam içerisinde yer alan şirketin altyapısını oluşturan ağ cihazları, sunucular, web uygulamaları ve diğer bilgi teknolojileri bileşenlerinin güvenliklerinin denetlenmesi ile şirket çalışanlarına yönelik düzenlenen sosyal mühendislik saldırıları ile söz konusu öğelerin güvenlik seviyesinin artırılmasını sağlayacak çıktıları ortaya koymaktır.

Denetimler yerel ağ ve İnternet üzerinden gerçekleştirilmiş olup, sosyal mühendislik gibi teknik olmayan saldırı yöntemleri de kullanılmıştır.

3.1.2. Sızma testi kapsamı

Şirket alt yapısında aşağıda belirtilen sistemler için sızma testleri gerçekleştirilmiştir;

- İletişim Altyapısı ve Aktif Cihazlar

- DNS Servisleri
- Etki Alanı ve Kullanıcı Bilgisayarları
- E-posta Servisleri
- Veritabanı Sistemleri
- Web Uygulamaları
- Dağıtık Servis Dışı Bırakma Testleri
- Sosyal Mühendislik Testleri

3.1.3. Yönetici özeti

3.1.3.1. Bulgular

- Bir saldırgan şirket altyapısındaki bilgilere yetkisiz erişebilir mi? Bilgiler bozulabilir mi? şirket bilgi sistemlerinde gerçekleştirilen değişikliklerin kaydı tutuluyor mu? Bu soruların cevabını bulmak için, bir saldırgan (hacker) tarafından gerçekleştirilebilecek yöntemlerle güvenlik önlemlerinin denenmesi sonucu ortaya çıkan bilgiler bu raporda yer almaktadır.

- Şirket bünyesindeki sistemler üzerinde yapılan incelemelerde acil aksiyon alınması gereken bulgular tespit edilmemiştir. Kapsam dâhilindeki sistemlerin bazılarının üzerindeki uygulama ve işletim sistemlerinde güncelleme eksikliğinden kaynaklanan uzaktan kod çalıştırma açığının olduğu tespit edilmiştir.

- Yapılan incelemelerde kapsam dâhilindeki şirket altyapısını etkileyebilecek önemli bulgular tespit edilmiştir. Güncelleştirme ve yama yönetiminden kaynaklanan eksiklikler, tespit edilen bulguların başında gelmektedir. Kurumsal yazılımların güvenlik ve işleyiş açılarından istenen seviyede kullanılabilmesi için üretici firma güncellemelerinin iyi bir şekilde yönetilmesi gereklidir. Benzer şekilde bazı sunucular için güvenlik güncelleştirmelerinin sıkı takip edilmediği ve sistemlerin ciddi güvenlik zafiyetlerine sahip olduğu görülmüştür. Güncelleştirme ve yama yönetimi planlı olarak yönetilmeli ve şirket sistemlerinin güncel ve güvenli kalması sağlanmalıdır.

- Kurumun İnternet'e açık sistemleri üzerinden yapılan testler sonucunda acil aksiyon alınması gereken bir bulgu tespit edilmemiştir. Ancak çeşitli sunucularda güncel olmayan FTP, sunucu yönetim panelinin İnternet'e açık olması, sağlayıcısı tarafından desteklenmeyen işletim sistemi kullanımı, sunucu sürüm bilgilerinin açığa çıkarılması, SSL desteği olmayan kullanıcı giriş sayfalarının olması gibi açıklar kurumun altyapısı hakkında bilgi vermektedir ve bu açıklar başka güvenlik açıklarıyla birleştirildiğinde önemli sonuçlar doğurabilir.

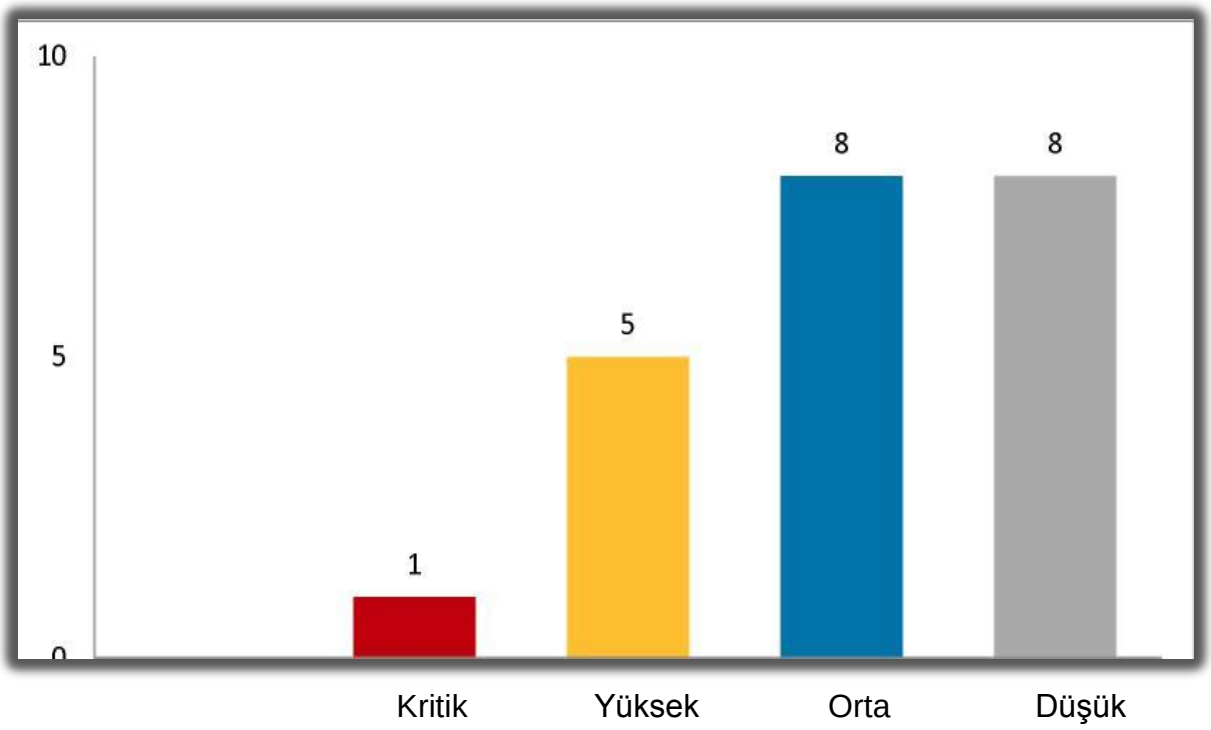
- Gerçekleştirilen çalışma kapsamında yapılan dağıtık servis dışı bırakma testleri sonucunda kapsam dahilindeki şirket sistemlerinin dağıtık servis dışı bırakma saldırılarına karşı direncinin arttırılması gerektiği tespit edilmiştir. Yine aynı kapsamda gerçekleştirilen sosyal mühendislik çalışmalarında, şirket çalışanlarının sosyal mühendisliğe karşı farkındalık ve direnç seviyelerinin geliştirilmesine ihtiyaç olduğu tespit edilmiştir.

- Yapılacak çalışmaların önceliğine yardımcı olması için, aşağıdaki grafikte de gösterildiği gibi, tüm bulgular "Acil", "Kritik", "Yüksek", "Orta" ve "Düşük" olmak üzere beş gruba ayrılmıştır.

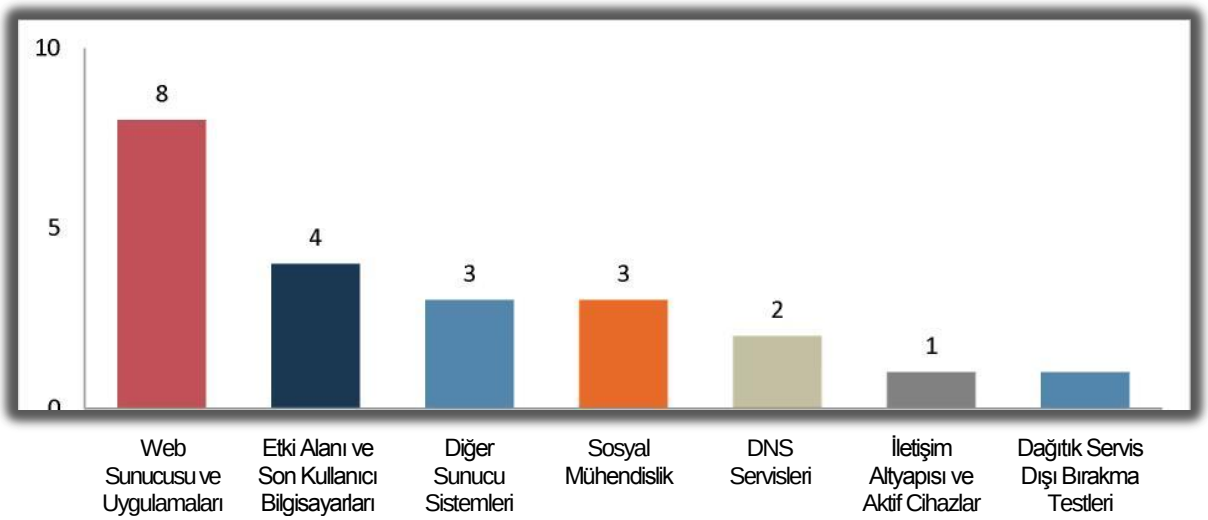
- Yapılan analiz sonucunda bulunan güvenlik açıkları 1 kritik, 5 yüksek, 8 orta ve 8 düşük seviye olmak üzere toplam 22 adettir. Raporun teknik kısmında, bulunan güvenlik açıkları ayrıntıları ile sıralanmış, yapılan saldırı örneklerine ait ekran çıktıları eklenmiş ve güvenlik açıklarının ortadan kaldırılması için yapılması önerilen işlemler belirtilmiştir.

Risk durumuna göre görsel sonuçlar aşağıda sunulmuştur:

Acil	Niteliksiz saldırgan tarafından şirket dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından şirket dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Şirket dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.



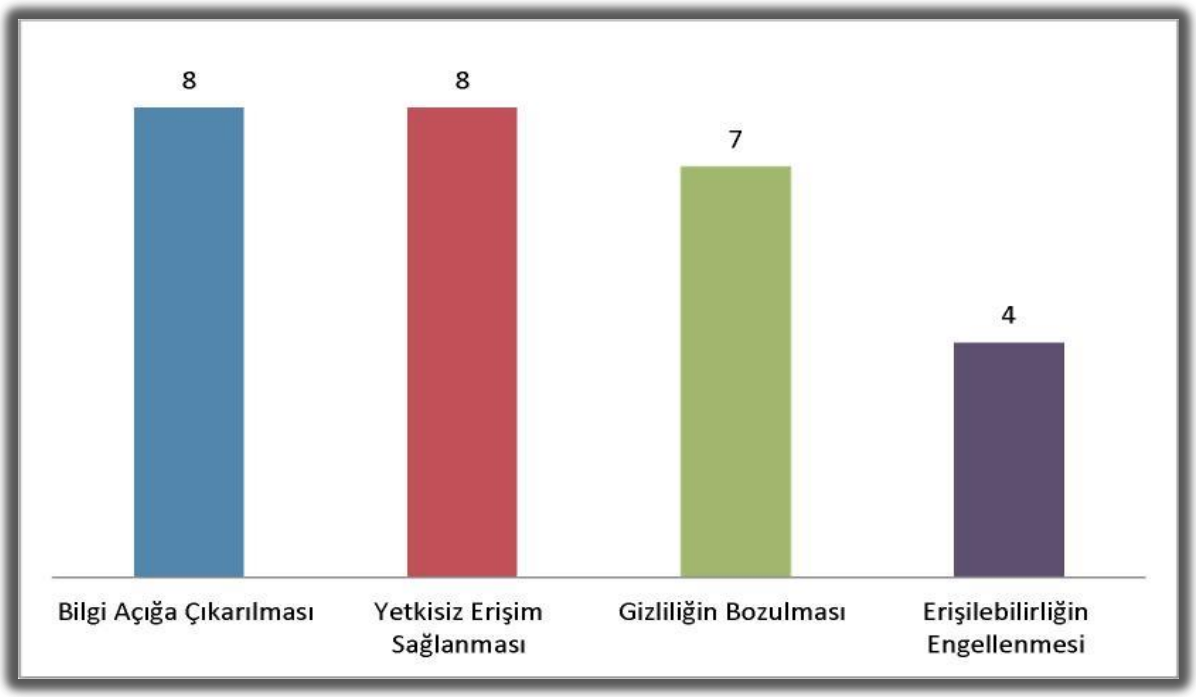
Şekil 3.1. Risk durumuna göre görsel sonuçlar



Web Sunucusu ve Uygulamaları	Web Uygulamalarından kaynaklanan açıklar.
Etki Alanı ve Kullanıcı Bilgisayarları	Etki Alanı ve Kullanıcı Bilgisayarları ile ilgili açıklar.
Diğer Sunucular ve Sistemler	Diğer Sunucular ve Sistemlerden kaynaklanan açıklar.
Sosyal Mühendislik Testleri	Sosyal Mühendislik ile ilgili açıklar.

DNS Servisleri	DNS Servislerinden kaynaklanan açıklar.
Veritabanı Sistemleri	Veritabanı Sistemlerinden kaynaklanan açıklar.
İletişim Altyapısı ve Aktif Cihazlar	İletişim Altyapısı ve Aktif Cihazlardan kaynaklanan açıklar.
Dağıtık Servis Dışı Bırakma	Dağıtık servis dışı bırakmadan kaynaklanan açıklar.

Şekil 3.2. Gruplara göre güvenlik açıkları dağılımı



Bilgi Açığa Çıkarılması	Sistem, uygulama veya altyapı ile ilgili bilgi edilmesine olanak sağlayan açıklar.
Yetkisiz Erişim Sağlanması	Sistem, uygulama ve veritabanlarına yetkisiz bir şekilde erişime sebep olan açıklar.
Gizliliğin Bozulması	Sistem, uygulama veya veritabanı üzerinden bulunan gizli bilgilerin elde edilebileceği açıklar.
Erişilebilirliğin Engellenmesi	Hizmet engellemeye yönelik açıklar.

Şekil 3.3. Muhtemel etki biçimlerine göre güvenlik açıklarının dağılımı

3.2. Teknik Rapor

Bu bölümde yapılan güvenlik taramasına ait detaylı teknik bilgiler yer almaktadır.

3.2.1. Teknik sızma testleri hedefi

Şirket sistemlerine yerel ağ ve İnternet üzerinden yapılan güvenlik denetiminin hedefi, kötü niyetli bir kişinin sistemler hakkında hangi bilgileri elde edebileceğini, sistemlerde hangi zafiyetlerin bulunduğunu ve bu zafiyetleri kullanarak sistemlere yetkisiz bağlanma, zarar verme veya hizmet dışı bırakma risklerini tespit etmek ve bunları raporlamaktır.

3.2.2. Teknik sızma testleri kapsamı

Bu çalışma aşağıdaki kapsamdan oluşmaktadır:

- Tüm Datacenter,
- İnternet'e açık tüm IP adresleri

3.2.3. Genel Test Metodolojisi

Yapılan güvenlik testleri bileşen temelli ele alınmıştır. Bu testlerde ilk olarak, tarama araçları yardımıyla, hedefler hakkında bilgi edinilmiştir. Bu bilgiler, sunucuların işletim sistemi bilgileri ve üzerinde çalışan portlar ile bu portlarda çalışan servislerdir. Daha sonra bileşenler güvenlik tarayıcı araçları ile taranmıştır. Bu araçların birçok yanlış alarmlar (false positives) verebileceği hususu göz önünde bulundurularak, tespit edilen açıklıklar detaylı olarak incelenmiştir. Bu açıklıkları kullanabilecek program kodları araştırılmış ve bulunan kodlar eğer mümkünse sisteme göre değiştirilerek denenmiştir. Sistemi devre dışı bırakabileceği düşünülen kodlar çalıştırılmamış fakat ilgili açıklıklara ve bu açıklıkların kapatılması ile ilgili çözümlere değinilmiştir.

Tespit edilen açıklıklar, açıklığın önem derecesi, sisteme olan etkisi, gerçekleştirilme şekli, açıklığın açıklaması, hangi bileşenlerde bulunduğu, açıklığın önlemi, varsa referansı içerecek şekilde detaylandırılmıştır. Açıklık önem derecesi beş kategoride ele alınmıştır. Bunlar acil, kritik, yüksek, orta ve düşük şeklindedir. Belirtilen açıklıkların önem derecesi belirlenirken varlığın değeri dikkate alınmamıştır.

3.2.3.1. Ağ haritası

Örnek bir ağ yapısı

3.2.4. Güvenlik analizi sonuçları

Raporun bu kısmında tetkikler sonucu bulunan açıkların detayları açıklanmıştır. Bulunan açıklar önem seviyesine göre acil, kritik, yüksek, orta, düşük olmak üzere 5 kategoriye ayrılmıştır. Her açık için ayrıntılı açıklama, etki biçimi, etkilenen platformlar, çözüm önerisi ve varsa ilgili açıkla ilgili referans bağlantı adreslerini aşağıdaki bölümde bulabilirsiniz.

3.2.4.1. Web Sunucusu ve Uygulamalarından Kaynaklanan Açıklar ve Çözüm Önerileri

- ***Güncel Olmayan FTP Sunucusundan Kaynaklanan Açıklar: KRİTİK SEVİYE***

Açıklama: Kurumsal bilgi teknolojileri sistemlerinde kullanılan uzaktan erişim servislerinin güncel olması, kurumsal sistemlere yetkisiz erişilmesine karşı koruma sağlar. Güncellemelerin sistemlere yüklenmeden önce test edilmesi ve sonrasında sunucu yöneticilerinin kontrolünde sistemlere yüklenmesi önerilmektedir.

Elde Edilen Bilgiler: Gerçekleştirilen çalışmalar esnasında güncel olmayan ve birçok güvenlik açığına sahip FTP sunucusu 5.03 (WS_FTP 7.5 öncesi bir sürüm) kullanıldığı tespit edilmiştir.

Mevcut durumda kurumsal bilgi teknolojileri sistemlerinin birçok saldırıya zafiyeti olması muhtemeldir. Kapatılan kritik açıklardan bazıları aşağıdaki gibidir:

- Servis dışı bırakmaya sebep olabilir,
- Arabellek aşımlarına sebep olabilir,
- Uzaktan kod çalıştırılabilir.

Etkilenen IP'deki sunucuda birçok güvenlik açığına sahip olan versiyonun yüklü olduğu tespit edilmiştir. Root yetkileri ile uygulama üzerinde uzaktan kod çalıştırılabildiği tespit edilmiştir.

Çözüm Önerisi: Uygulama hizmetlerinin güncellenmesi işlemi bir süreç olarak tanımlanmalı, süreç kapsamında otomatik veya manuel yöntemlerle gerçekleştirilmelidir. Uygulamaların güncel tehditlere karşı güvencede olması için güncellemelerin en kısa zamanda yapılması gereklidir.

- ***İnternet Üzerinden Erişilebilir Sunucu Yönetim Paneli: ORTA SEVİYE***

Açıklama: Bir sunucu üzerinde kullanılan uygulamalara ait yönetim panellerinin, dışarıdan erişilemez ve adreslerinin tahmin edilemez olması gerekir. Aksi halde, parola ve kimlik doğrulama işlemleri ile korunuyor olsalar bile; çıkacak bir açığın sömürülmesi, şifre tahmin, ele geçirme ve deneme yöntemleri gibi güvenlik riskleri dolayısıyla, yetkisiz biri tarafından erişim sağlanabilir. Sunucu üzerinde ayar yapılmasına olanak sağlamasa da üzerindeki bilgiler ile sunucu hakkında bilgi edinile bilinir.

Elde Edilen Bilgiler: Yapılan incelemeler sonucunda, aşağıdaki adreslerde İnternet'e açık yönetim panelleri tespit edilmiştir. Bu paneller sunucu hakkında bilgi toplanması ve sunucunun ele geçirilmesi gibi durumlara sebebiyet verebilir.

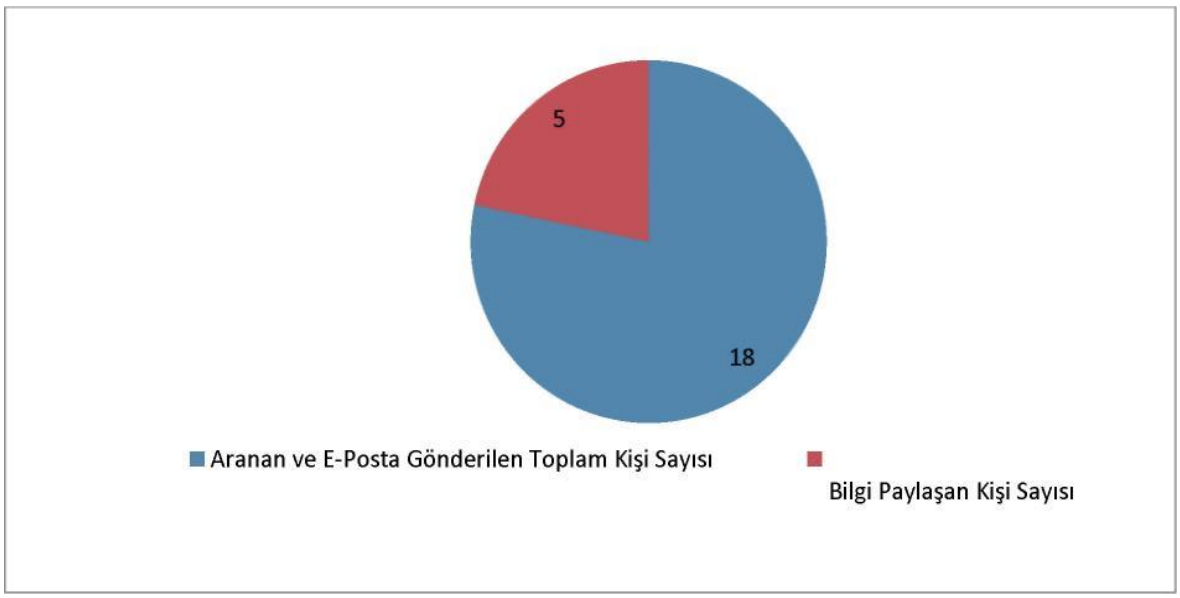
Çözüm Önerisi: Sunucu üzerinde bulunan panellerin öncelikli olarak İnternet üzerinden kontrolsüz erişime kapatılması gerekmektedir. Eğer sunucuların yönetim panellerine İnternet üzerinden erişim verilmesi zorunlu ise, bu erişim tahmin edilmesi zor bir URL üzerinden, SSL, Basic Authentication (SSL olamıyorsa), IP kısıtlama, Custom User Agent tanımlama gibi erişimi kısıtlayacak önlem alınarak sağlanmalıdır.

3.2.4.2. Sosyal mühendislik testleri sonucu

3.2.4.2.1. Uygulanan senaryoların başarısı

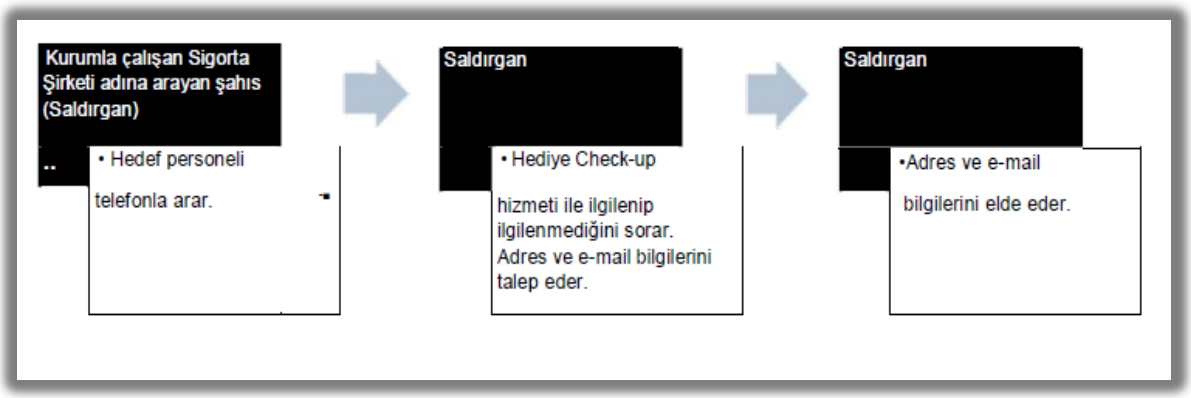
Şekil 3.4. Senaryo uygulama sonucu

3.2.4.2.2. Kapsam dahilinde iletişime geçilen personelin bilgi paylaşım dağılımı



Şekil 3.5. İletişime geçilen personelin bilgi paylaşım dağılımı

3.2.4.2.3. Uygulanan senaryolar



Şekil 3.6. Senaryo 1: Kurum iştiraki sosyal yapılarla kişisel bilgilerin elde edilmesi

Sosyal Mühendislik çalışmaları kapsamında, şirket çalışana, kendini Şirket'e sağlık hizmeti veren bir sigorta şirketinin çalışanı xxyy (var olmayan şahıs) olarak tanıtır. Daha sonra, sigorta firmasının şirket çalışanlarından bazılarına Kasım ayı içerisinde geçerli olacak ücretsiz check-up hizmeti hediye edeceğini belirterek bu hizmet ile ilgilenip ilgilenmediklerini sorar. İlgilendiğini söyleyen personelden adres ve e-posta bilgilerini talep eder. E-posta adresine bilgilendirme maili göndereceklerini ve ev/iş adresine ise ücretsiz check-up hizmetinden yararlanabilmeleri için hediye çeki göndereceklerini söyler.

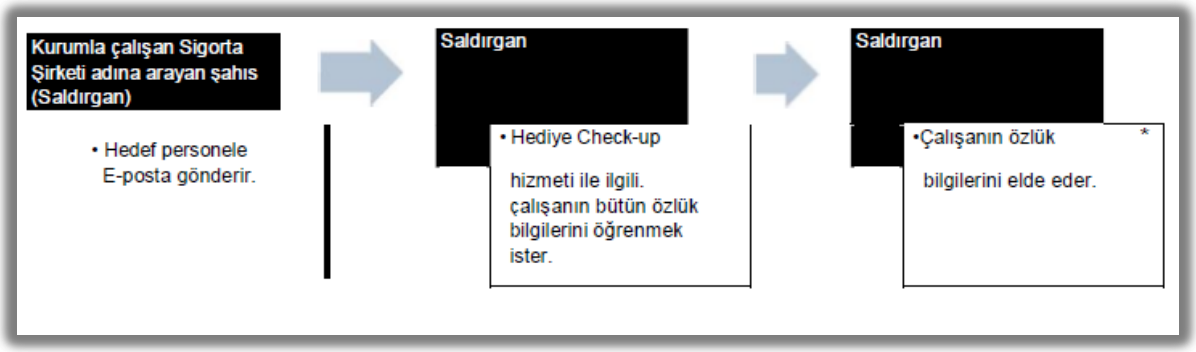
Saldırgan, telefon görüşmesi sonunda istediği bilgileri elde ederse, çalışanın bu hizmeti hangi semtteki hastanede kullanmak istediğini sorar ve cevabı aldıktan sonra teşekkür ederek görüşmeyi sonlandırır. Herhangi bir bilgi öğrenemediyse yine teşekkür ederek görüşmeyi bitirir.

Sonuç: Kasım ayı içerisinde sabah ve öğleden sonra olmak üzere iki farklı şirket çalışanı aranarak saldırgan tarafından sağlanan listedeki iki kişi ile görüşüldü. Şirket çalışanlarını hedef alan iki arama da olumlu olarak sonuçlandı.

Olumlu sonuçlanan her iki aramada da çalışanlardan ev adresleri ve işyeri e-postaları ile cep telefonu numaraları alındı. Çalışanlara, ücretsiz check-up hizmetinden hangi hastanede/poliklinikte yararlanmak istedikleri sorusu sorulduğunda, evlerine yakın olan hastanede/poliklinikte kullanmak istedikleri

cevabını alındı. Bu çalışanların oturdukları semt bilgisi öğrenildikten sonra çalışanlar en yakın hastaneye yönlendirildi.

Sonuç olarak senaryo dahilinde hizmet ile ilgilendiğini söyleyen, ev adres ve işyeri e-postaları ile cep telefon bilgilerine erişildi.



Şekil 3.7. Senaryo 2: Oltalama (Phishing) ile özlük bilgileri elde etme

Sosyal mühendislik kapsamında uygulanan bu senaryoda; şirket IT ekibi tarafından iletilen e-posta listesindeki 14 kişiye aldatma e-postası gönderir. Gönderilen e-postada, Şirket'e hizmet veren bir sigorta firması tarafından Kasım ayı boyunca ücretsiz checkup hizmeti sunulacağı ve hizmetten yararlanmak için e-posta içerisinde yer alan www.sirketsaglik.org sitesine girerek kayıt olunması gerektiği belirtilir. İnternet sitesi üzerinde şirket çalışanı, özlük bilgilerini (T.C. Kimlik No gibi) doldurması gereken bir form ile karşılaşır. Form doldurulduktan sonra "Başvurunuz alınmıştır, checkup hizmetimizle ilgilendiğiniz için teşekkür ederiz. Sizinle en kısa zamanda iletişime geçeceğiz." şeklinde teşekkür bildirisi yayınlanır ve işlem sonlanır.

Sonuç: 2012 yılı Eylül ayı içerisinde şirket tarafından sağlanan e-posta listesindeki 14 şirket çalışanına e-posta gönderildi.

Genel Müdürlük çalışanlarına yönelik gerçekleştirilen bu saldırıda, üç çalışan e-postadaki web sitesine girerek özlük bilgilerini, kullanıcı adı ve parola bilgilerini isteyen formu doldurdu. Böylece 3 şirket çalışanının özlük bilgileri ele geçirildi.

Şekil 3.8. Senaryo 3: Şirket çalışanının kullanıcı adı ve şifre bilgilerinin öğrenilmesi

Şirket IT ekibi ve saldırgan tarafından sağlanan çalışan bilgileri kullanılarak yapılan sosyal mühendislik kapsamındaki bu senaryoda, saldırgan şirket ile çalışan dışarıdan hizmet veren IT çalışanı gibi 2 şirket çalışanını arar. Saldırgan, aradığı Şirket çalışanına otomatik program kurulum sistemiyle ilgili yaşanan bir problemin onları da etkilediğini söyledikten sonra problemin çözümü için çalışandan kullanıcı adı ve parolası istenir. Ayrıntılı bilgi istendiğinde ise sistemlerde sebebi araştırılan bir sorun yaşandığı belirtilir. Arayan kişinin kim olduğunun sorgulanması durumunda kendisini gerçekte var olmayan kişi xxyy olarak tanıtır.

Saldırgan görüşme sonunda istediği bilgileri elde ederse, otuz dakika içinde kullanıcının şifresini değiştirmesi gerektiğini belirtir ve teşekkür ederek konuşmayı sonlandırır. Çalışan istenen bilgileri vermediği takdirde, saldırgan gerekli talimatlar için tekrar arayacağını ya da yazılı talep ile çalışana geri dönüleceğini belirterek konuşmayı sonlandırır.

***Sonuç*:** 2012 yılı Kasım ayı içerisinde bir Şirket çalışanı arandı.

Kurumsal Şube çalışanlarına yapılan olumlu sonuçlandı. Çalışan, bu görüşme esnasında kullanıcı adı ve parolasını saldırgan ile paylaştı. Ardından yapılan görüşmelerde şirketin ufak çaplı bir şirket olmasından ve az sayıda çalışanının bulunmasından, parolasını saldırgan ile paylaşan çalışanın diğer çalışanların durum ile ilgili uyarmasından dolayı çalışmalar sonlandırılmıştır.

3.2.4.2.4. Sosyal mühendislik yöntemlerinden kaynaklanan açıklar ve çözüm önerileri

- ***Oltalama (Phishing) ile Özlük Bilgileri Elde Etme: YÜKSEK SEVİYE***

Açıklama: Sosyal mühendislik kapsamında uygulanan bu senaryoda; Şirket IT ekibi tarafından oluşturulan listeden 14 kişi seçer ve çalışanlara E-Posta gönderir. Gönderilen E-Postada, şirkete hizmet veren bir sigorta firması tarafından Kasım ayı boyunca ücretsiz Checkup hizmeti sunulacağı ve hizmetten yararlanmak için E-Posta içerisinde yer alan xxyy sitesine girerek kayıt olunması gerektiği belirtilir. İnternet sitesi üzerinde Şirket çalışanı, özlük bilgilerini (T.C. Kimlik No gibi) doldurması gereken bir form ile karşılaşır. Form doldurulduktan sonra "Başvurunuz alınmıştır, checkup hizmetimizle ilgilendiğiniz için teşekkür ederiz. Sizinle en kısa zamanda iletişime geçeceğiz." şeklinde teşekkür bildirisi yayınlanır ve işlem sonlanır.

***Elde Edilen Bilgiler*:** Eylül ayı içerisinde saldırgan tarafından sağlanan listedeki şirketin 14 çalışanına E-Posta gönderildi. Genel Müdürlük çalışanlarına yönelik gerçekleştirilen bu saldırıda, üç çalışan e-postadaki web sitesine girerek özlük bilgilerini, kullanıcı adı ve parola bilgilerini isteyen formu doldurdu. Böylece 3 Şirket çalışanının özlük bilgileri ele geçirildi.

Çözüm Önerisi: Kurum çalışanları ise bu tür saldırılar konusunda bilinçlendirilmelidir. Bu konuda devamlı olarak tekrarlanması ve gündemde tutulması gereken uyarılar şu şekilde özetlenebilir:

- Tanınmayan kişilerden gelen e-postalar açılmamalı,
- Bilinen bir kişiden gelen şüpheli e-postalar, gönderen kişi tarafından onaylatılmalı,
- Gelen e-posta ile birlikte gelen dokümanlar veya bağlantılar bu onay olmadan açılmamalı,
- Özellikle herhangi bir e-postadaki bağlantı, eğer görünürde farklı, arkada farklı bir adrese yönlendiriyor ise bu bağlantılara kesinlikle tıklanmamalı.

- Kurum içinden gelen e-postaların onaylama işleminin otomatik olarak gerçekleştirilebilmesi için, e-posta imzalama mekanizmaları kullanılabilir.

- ***Şirket Çalışanının Kullanıcı Adı ve Şifre Bilgilerinin Öğrenilmesi: YÜKSEK SEVİYE***

Açıklama: Şirket IT ekibi ve saldırgan tarafından sağlanan çalışan bilgileri kullanılarak yapılan sosyal mühendislik kapsamındaki bu senaryoda, saldırgan Şirket ile çalışan dışarıdan hizmet veren IT çalışanı gibi 2 Şirket çalışanını arar. Saldırgan, aradığı Şirket çalışanına otomatik program kurulum sistemiyle ilgili yaşanan bir problemin onları da etkilediğini söyledikten sonra problemin çözümü için çalışandan kullanıcı adı ve parolası istenir. Detay istendiğinde ise sistemlerde sebebi araştırılan bir sorun yaşandığı belirtilir. Arayan kişinin kim olduğunun sorgulanması durumunda kendisini gerçekte var olmayan kişi xxyy olarak tanıtır.

Saldırgan görüşme sonunda istediği bilgileri elde ederse, otuz dakika içinde kullanıcının şifresini değiştirmesi gerektiğini belirtir ve teşekkür ederek konuşmayı sonlandırır. Çalışan istenen bilgileri vermediği takdirde, saldırgan gerekli talimatlar için tekrar arayacağını ya da yazılı talep ile çalışana geri dönüleceğini belirterek konuşmayı sonlandırır.

Elde Edilen Bilgiler: Kasım ayı içerisinde bir Şirket çalışanı arandı. Kurumsal Şube çalışanlarına yapılan olumlu sonuçlandı. Çalışan, bu görüşme esnasında kullanıcı adı ve parolasını saldırgan ile paylaştı. Ardından yapılan görüşmelerde Şirketin ufak çaplı bir şirket olmasından ve az sayıda çalışanının bulunmasından dolayı çalışmalar sonlandırıldı.

Çözüm Önerisi: Kurum çalışanları ise bu tür saldırılar konusunda bilinçlendirilmelidir. Bu konuda devamlı olarak parolaların her ne sebeple olursa olsun hiçbir çalışanla paylaşılmaması gerektiği tekrarlanmalı ve gündemde tutulmalıdır.

- ***<u>Kurum İştiraki Sosyal Yapılarla Kişisel Bilgilerin Telefonla Elde Edilmesi: DÜŞÜK SEVİYE</u>***

Açıklama: Sosyal Mühendislik çalışmaları kapsamında, Şirket IT ekibi tarafından ve saldırgan tarafından sağlanan listeden 2 kişi seçer. Saldırgan telefonla ulaştığı çalışana, kendini şirkete sağlık hizmeti veren bir Sigorta çalışanı xxyy (var olmayan şahıs) olarak tanıtır. Daha sonra, Sigorta firmasının Şirket çalışanlarından bazılarına Kasım ayı içerisinde geçerli olacak check-up hizmeti hediye edeceğini belirterek bu hizmet ile ilgilenip ilgilenmediklerini sorar. İlgilendiğini söyleyen personelden adres ve e-posta bilgilerini talep eder. E-posta adresine bilgilendirme maili göndereceklerini ve ev/iş adresine ise ücretsiz check-up hizmetinden yararlanabilmeleri için hediye çeki göndereceklerini söyler.

Saldırgan, telefon görüşmesi sonunda istediği bilgileri elde ederse, çalışanın bu hizmeti hangi semtteki hastanede kullanmak istediğini sorar ve cevabı aldıktan sonra teşekkür ederek görüşmeyi sonlandırır. Herhangi bir bilgi öğrenemediyse yine teşekkür ederek görüşmeyi bitirir.

Elde Edilen Bilgiler: Kasım ayı içerisinde sabah ve öğleden sonra olmak üzere farklı Şirket aranarak saldırgan tarafından sağlanan listedeki iki kişi ile görüşüldü. Şirket çalışanlarını hedef alan her iki aramada olumlu olarak sonuçlandı. Olumlu sonuçlanan her iki aramada da çalışanlardan ev adresleri ve işyeri e-postaları ile cep telefonu numaraları alındı. Çalışanlara, ücretsiz check-up hizmetinden hangi hastanede/poliklinikte yararlanmak istedikleri sorusu sorulduğunda, evlerine yakın olan hastanede/poliklinikte kullanmak istedikleri cevabını alındı. Bu çalışanların oturdukları semt bilgisi öğrenildikten sonra çalışanlar en yakın hastaneye yönlendirildi. Sonuç olarak senaryo dahilinde hizmet ile ilgilendiğini söyleyen, ev adres ve işyeri e-postaları ile cep telefon bilgilerine erişildi.

Çözüm Önerisi: Kurum çalışanları ise bu tür saldırılar konusunda bilinçlendirilmelidir.

3.2.4.2.5. Sosyal mühendislik testleri sonucu

Şirket çalışanları üzerinde uygulanan senaryolar dâhilinde yapılan sosyal mühendislik kapsamındaki çalışmada üç senaryonun tamamında başarıya ulaşılmıştır. Bazı çalışanların özlük bilgileri, bazı çalışanlarında uygulama/sistem/veritabanı giriş için kullandığı kullanıcı adı ve şifre bilgileri ele geçirilmiştir. Çalışma sonucunda kapsam dâhilindeki Şirket çalışanlarının bilgi güvenliği konusunda farkındalıklarının geliştirilmesine ihtiyaç olduğu tespit edilmiştir. Şirket personelinin farkındalıklarının verilecek eğitimler ile yukarıya çekilmesi sosyal mühendisliğe olan direnç seviyesini artıracaktır.

Güvenlik sisteminin en zayıf halkası, insan bileşenidir. Şirket personelinin uygun bir şekilde bilgilendirilmesi sosyal mühendislik saldırılarının etkisini azaltmaya yardımcı olur. Bu nedenle Şirket üst yönetiminin, bilgi güvenliği farkındalığını ve sosyal mühendisliğe karşı direncin artırılması için kurumsal gelişim programları kapsamında çalışanlarını eğitmesi ve belirli aralıklarla bu eğitimleri tekrarlaması önerilir. Aynı zamanda Güvenlik Politikalarının güncel tutulması, bu politikaların tüm çalışanlar tarafından okunduğuna ve anlaşıldığına emin olunması son derece önemlidir.

3.3. Denetim Sonucu

xxyy Bilgi Güvenliği uzmanları tarafından gerçekleştirilen Şirket sızma testleri Web Uygulamaları, E-posta Sunucuları, DNS Sunucuları, Sosyal Mühendislik Testleri, Veritabanı Sistemleri, Etki Alanı ve Son Kullanıcı Bilgisayarları, İletişim Altyapısı, Dağıtık Servis Dışı Bırakma Testleri, Diğer Sunucu Sistemleri kapsamında gerçekleştirilmiştir.

Yapılan çalışmaların sonucunda kurum bilgi teknolojileri sistemleri öğelerinin bir kısmında işletim sistemi güvenlik güncellemelerinin yönetiminde aksaklık olduğu saptanmış, bu durumun bir sonucu olarak güvenlik güncellemelerinin yüklenmediği sunucuların ciddi güvenlik zafiyetlerine sahip olduğu tespit edilmiştir. Bu nedenle güncelleme yönetimine önem verilmeli, kritik güvenlik açıkları yakından takip edilmeli ve mümkün olan en kısa sürede sistemlere yüklemelidir.

Raporda ayrıntıları belirtilmiş olan açıklar en kısa sürede kapatılmalı, kurumsal sistemlerin güvenlik seviyesi daha iyi hale getirilmelidir. Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamalıdır.

Güvenlik denetimleri dönemsel olarak devam ettirilmeli, güncel tehditler göz önüne alınarak kullanılan altyapı, yapılandırma ayarları ve uygulamalar güncelleştirilmelidir.

Bu çalışmalar kapsam dâhilindeki Şirket altyapısının denetim anındaki durumunu göstermektedir.

SONUÇ

Bilgi sistemleri kullanımının iş hayatında yaygınlık kazanması BT denetimi konusunu ön plana çıkarmaktadır. Karmaşık bilgi teknolojisinin kullanıldığı çevrelerde, mali tablolar denetimin kalitesi mali denetçinin muhasebe bilgi sistemleri hakkındaki uzmanlığına ve BT denetçisinin değerlendirmesini dikkate almasına bağlıdır. Mali denetçi kontrol riskini değerlendirirken ve maddi doğrulama testleri planlarken BT denetçisinin uzmanlığından yararlanır. Mali tablolar ve diğer mali veriler işletmelerin bilgisayar sistemlerinin bir çıktısı olduğundan mali tablolar denetiminde bilgi sistemlerinin göz ardı edilmesi denetimin güvenilirliğini zedeleyecektir. Bağımsız denetçiler mali denetim sürecinde iç kontrollerin etkinliğine göre denetim yaklaşımı belirlemekte ve hesap alanları ve örnekleme kararlarını vermektedirler. Bu nedenle işletmelerin iç kontrollerinin gözden geçirilmesi ve bilgi sistemlerinin değerlendirilmesi için bilgi teknolojileri denetimi gereklidir.

2001 yılında AICPA tarafından yayınlanan denetim standartları (SAS 94), BDDT'nin belli bilgi teknolojileri ortamlarında belli bilgi teknolojileri kontrol türlerini test etmesi gerektiğini belirtmektedir. 2002 yılında yürürlüğe giren Sarbanes-Oxley Kanunu, halka açık şirketler ve mali tablolar denetimine tabi tüm kuruluşlar için finansal raporlamayı etkileyen kontrol ve BT kontrollerinin denetimini zorunlu kılmaktadır. Yine 2006 yılında yayınlanan risk odaklı standartlar (SAS 104-111) BT denetiminin önemine işaret etmektedir. Bu standartların yanında ISA 315, 330 No'lu standartlar bilgisayarlı ortamlardan denetimin nasıl etkilendiğini belirtmekte ve denetçinin dikkate alması gerektiği hususlara işaret etmektedir. Genel olarak bakıldığında kuruluşlarda bilgisayar kullanımı şunlara etki eder:

1) İç kontrol ortamı ve kontrol testlerini,
2) Kanıt toplama tekniklerini,
3) Toplanan kanıtların değerlendirilmesini etkiler.

Mali tablolar denetimi için yapılacak bir BT denetiminde karşılaşılan sorun uygun denetim kapsamının belirlenmesidir. Denetimin kapsamını belirlemenin en iyi yolu ne çok ne de çok az denetim prosedürü belirleyerek risk odaklı bir denetim

yaklaşımının benimsenmesidir. Uygun denetim kapsamın belirlenmesinde mali tabloların taşıdığı yanlış beyan riski belirleyici rol oynar. Yanlış beyan riski, denetlenen kurumun iç kontrol mekanizmasına bağlı olmaksızın, mali tabloların önemli olabilecek bir hata içerme olasılığı olan yapısal risk ve mali tabloları etkileyebilecek önemli bir hatanın, kurumun iç kontrol sistemi tarafından zamanında önlenememesi, tespit edilememesi veya düzeltilememesi olasılığı olan kontrol riskinden oluşur. BT denetçisinin mali tablolar denetiminde sorumluluğu iki yönlüdür:

1. BT'nin mali raporlama üzerindeki etkilerinden kaynaklanan riskleri tespit etmek,
2. BT kontrollerinden kaynaklanan riskleri belirlemek.

BT denetiminin mali tablolar denetimine katkılarından biri kontrol testleri alanındadır. Mali denetim ekibi mali denetim sürecinde kontrol testlerinden elde ettikleri sonuçlara göre güvence vermektedirler. Güvence verebilmek için bilgisayar ortamındaki otomatik kontrollerin etkili çalışıp çalışmadığının test edilmesi gerekir ki bu da BT denetçilerinin yardımıyla gerçekleşir.

Otomatik kontrol testlerinin uygulanmasının denetime olan katkıları şunlardır:

- Otomatik kontrol testlerinin uygulanması denetimde etkinliği ve verimliliği arttırır (yüzde yüz test etme, daha az iş gücü emek kullanımı gibi).
- Bu testler sonucunda mali denetçi genel kontrollerin etkinliği konusunda yeterli güvence elde etmiş olur.
- Risk odaklı denetim standartları mali raporlama sürecindeki BT kontrollerinin düzgün tasarlanmasını ve uygulanmasını gerektirdiğinden bu standarda uyum araştırılmış olur.

İkinci olarak, BDDT'lerin kullanımı mali denetimde doğru ve güvenilir sonuçlara kısa sürede ulaşmayı sağlar. BT denetçisi mali tablolar denetiminde gerçekleştirilen işlemleri BT teknikleri ile kısa zamanda yapabilmekte ve yüzde yüz doğrulama sağlayabilmektedir.

Üçüncü olarak, BT denetimi kurum yönetimine değer katar. BT denetim sürecinde mali tabloları etkilemeyen BT ile ilgili aksaklıklar olabilir. Mali tablolara etkisi olmasa da yönetim bu tür aksaklıkları bilmek ve düzeltmek isteyecektir.

BT denetçileri mali tablolarda olabilecek yanlış beyan konusunda, BT ile ilgili yapısal risklerin ve kontrol risklerinin değerlendirilmesinde mali denetimlere her zaman katkıda bulunabilirler. Risk temelli denetim standartları, hesap bakiyelerinin incelenmesinde, muhasebe işlemlerinin sınıflandırılmasında ve raporlanmasındaki risk seviyesinin tespit edilmesinde denetçinin titiz çalışmasını gerektiren bir yaklaşım öngörmektedir ve her hesap alanı kendi risk seviyesi ile değerlendirilmektedir. BT denetçisi yüksek risk görülen alanlar için daha güçlü testler geliştirir, orta sevide riskli alanlar için orta düzeyde testler, düşük düzeyde riskli alanlar için de düşük düzeyli testler uygular.

Sonuç olarak BT denetimi mali denetimlerde emek tasarrufu sağlar, mali denetimin kalitesini arttırır, standartlara uyumu sağlar, kuruluş yönetimine değer katar ve mali denetim hedeflerine ulaşmada güvence verir.

KAYNAKÇA

AICPA. (1997). www.aicpa.org adresinden 13 Kasım 2013'te alındı.

Akbaş, G. (2011). Mali Denetimde Temel Düzeyde Bilişim Sistemleri Denetiminin Önemi. *Dış Denetim Dergisi*, 14.

Artinyan, E. N. (2014). *Denetim ile ilgili bilgiler.* www.denetimnet.net: http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf adresinden 17 Nisan 2014'te alındı.

Atay, C. (1999). *Devlet Yönetimi ve Denetimi.* İstanbul: Alfa Yayınları.

Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri Bankacılık Süreçlerinin Denetimi Hakkında Yönetmelik. (2010). Ankara: BDDK.

Boyacıoğlu, M. A. (2002). Operasyonel Risk ve Yönetimi. *Bankacılar Dergisi*, 43.

Cascarino, R. E. (2012). *IT Auditor's Guide to IT Auditing.* New Jersey: John Waley and Sons Inc.

Donald, T. H., & William, G. G. (1997). *Auditing: An Assertion Approach.* New York: John Wiley and Sons Inc.

Gelinas, U., Dull, R., & Wheeler, P. (2012). *Accounting Information System.* South-Western.

Güredin, E. (2010). *Denetim ve Güvence Hizmetleri.* Türkmen Kitabevi.

Houck, T. P. (2003). *Why and How Audit Must Change.* New Jersey: John Wiley & Sons.

ISACA. (2005). *BT Denetim ve Güvence Standartları.* ISACA. www.isaca.org addresinden 13 Kasım 2013'te alındı.

ISSAI 1003. http://www.issai.org/media/13208/issai_1003_e_.pdf adresinden 17 Nisan 2014 tarihinde alınmıştır.

İnternet: http://pune.cdac.in: http://pune.cdac.in/html/gist/research-areas/ocr.aspx adresinden 17 Nisan 2014'te alınmıştır.

İnternet:www.en.wikipedia.org.wikipedia:http://en.wikipedia.org/wiki/Magnetic_ink_character_recognition adresinden 17 Nisan 2014'te alınmıştır.

İnternet: *www.isaca.org*. History of ISACA: www.isaca.org adresinden 17 Nisan 2014'te alındı.

İnternet: www.kpmg.com.tr. (2014, 07 15). *audit/sayfalar/mali-tablolarin-denetimi*. www.kpmg.com:http://www.kpmg.com/tr/tr/hizmetlerimiz/audit/sayfalar/mali-tablolarin-denetimi-hizmetlerimiz.aspx adresinden 17 Nisan 2014'te alındı

Jain, A. K., Flynn, P., & Ross, A. A. (2008). *Handbook of Biometrics.* New York: Springer Science+Business Media.

Jancura, E. G. (1974). *Audit and Control of Computer Systems.* New York: Mason/Charter Publishers Inc.

Johnstone, K. M., Gramling, A. A., & Rittenberg, L. E. (2014). *Auditing: A Risk Based Approach to Conducting a Quality Audit.* South-Western: Cengage Learning.

Kaval, H. (2008). *Muhasebe Denetimi.* Ankara: Gazi Kitabevi.

Kavut, L., Taş, O., & Şavlı, T. (2009). *Uluslararası Denetim Standartları Kapsamında Bağımsız Denetim.* İSTANBUL: İSMMMO Yayın No: 130.

Kayrak, M. (2011). Avrupa Birliği Sayıştayında Mali Denetim Çerçevesinde Bilişim Sistemleri Denetimi. *Dış Denetim Dergisi*, 20-21.

Kayrak, M. (2012). Bilgi Kriterleri Çerçevesinde Denetim. *Sayıştay Dergisi*, 154.

Kumar, R., & Sharma, V. (2013). *Auditing: Principles and Practices.* Delhi: PHI Learning.

Maliye Hesap Uzmanları Derneği. (1997). *Denetim İlke ve Esasları I. Cilt.* Ankara.

Özbilgin, İ. G. (2003). Bilgi Teknolojileri ve Denetimi ve Uluslararası Standartlar. *Sayıştay Dergisi*, 123.

Özkul, D. (2002). Bilişim Sitemleri Denetimi. *Gazi Üniversitesi Sosyal Bilimler Enstitüsü*.

Puttick, G., Esch, S. v., & Kana, S. (2007). *The Principles and Practice of Auditing.* Cape Town: Juta & Co. Ltd.

Saran, U. (1995). Türk Kamu Yönetiminde Denetim Sistemi. *Türk İdare Dergisi*, 67.

Sayıştay Başkanlığı. (2014). *Düzenlilik Denetim Rehberi.* Ankara: Sayıştay Bşakanlığı.

Sayıştay. (2013). *Bilişim Sistemleri Denetim Rehberi.* Ankara: Sayıştay Başkanlığı.

Singleton, T. W. (2009). What Every IT Auditor Should Know About Scoping an IT Audit. *ISACA Journal Volume 4*, 2.

Soltani, B. (2007). *Auditing: An International Approach.* Prentice Hall.

Sürmeli, F. (2005). *Muhasebe Bilgi Sistemi.* Eskişehir: Anadolu Üiversitesi Yayını No:1644.

Topkaya, A. (2011). Bilişim Sistemleri Denetiminde Sayıştay Modeli. *Dış Denetim Dergisi*, 118-119.

Tufan, E. F. (2007). *Kamu Yönetiminde Bilişim Sistemlerinin Strateji Geliştirme Amaçlı Kullanımı:Kuram ve Selçuk Üniversitesi İktisadi İdari Bilimler Fakültesi İçin Bir Model Önerisi.* Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Weber, R. (2013). *Information Systems Control and Audit* (s. 32). içinde Upper Saddle River: Prentice Hall.

Yalkın, L. D. (2011). Bilgi Teknolojileri Denetimi. *Kavramsal Çerçeve, Aşamaları, Sınırları, Sorunları*. ANKARA.

Yıldız, Ö. R. (2007). Bilişim Sistemleri Denetimi ve Sayıştay. *Sayıştay Dergisi*, 181.

Yıldız, Ö. R. (2010). 5018 Sayılı Kanun ve Bilişim Sistemleri Denetimi. *Dış Denetim Dergisi*, 121.

Yurdagül, Ö. (2010). *Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri.* Isaca.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: BÖCEK, Bilal
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 01.07.1984, Balıkesir
Medeni hali	: Evli
Telefon	: 0 (312) 295 39 77
Faks	: 0 (312) 295 40 94
e-mail	**:** bilalbocek@hotmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Yüksek lisans	Gazi Üniversitesi / Muhasebe-Finans	Devam Ediyor
Lisans	Marmara Üniversitesi/ İşletme (İng.) B.	2007
Lise	Sırrı Yırcalı Anadolu Lisesi (Balıkesir)	2002

İş Deneyimi

Yıl	**Yer**	**Görev**
2009-Devam ediyor	T.C. Sayıştay Başkanlığı	Denetçi
2007 - 2008	Deloitte	Denetçi

Yabancı Dil

İngilizce

DİZİN

GAZİ GELECEKTİR...

Gazi geleceğiz...