SERMAYE PİYASASI KURULU
DENETLEME DAİRESİ

BİLGİ SİSTEMLERİ DENETİM SÜREÇLERİ YETERLİK ETÜDÜ

Samet YILDIRIM

Bilişim Uzman Yardımcısı

Temmuz 2017
İSTANBUL

YÖNETİCİ ÖZETİ

Günümüzde birçok işletme ve kuruluşun süreç ve operasyonlarında bilgi sistemlerinden faydalanması, bu işletme ve kuruluşlara teknolojik yeniliklerin yanı sıra kendine özgü riskleri de beraberinde getirmiştir. Doksanlı yılların sonuna doğru dünya genelinde büyük yankı uyandıran Enron ve WorldCom gibi finansal skandallar sebebiyle ABD'de 2002 yılında yürürlüğe giren Sarbanes-Oxley Kanunu ile halka açık şirketler ve finansal tablo denetimine tabi diğer tüm kuruluşlar için bilgi sistemlerine ilişkin kontrollerin denetimi zorunlu tutulmuştur. Bilgi sistemleri denetimi, kamu ve toplum güveninin azalmasına neden olan bu skandalların ileride yaşanmasını önlemek ve finansal raporlamanın doğruluğunu ve bütünlüğünü sağlamak adına kritik bir mekanizma haline gelmiştir.

Bilgi sistemleri denetiminin en önemli unsuru bilgi sistemleri denetçisidir. Ancak bilgi sistemleri denetçisi, denetimlerinde bilgi sistemlerine ilişkin uluslararası kabul görmüş standartlara verdiği referanslar ölçüsünde denetimine olan güvenin objektifliğini ve bulgularının kabul edilebilirliğini artırabilir. Uluslararası kuruluşlar ve ülke otoriteleri, gelişen teknolojilere ve bu teknolojilerin işletmelerin iş süreçlerinde ve finansal raporlamalarında kullanımının artması ile birlikte yükselişe geçen denetim ihtiyacının daha objektif ve daha güvenilir bir şekilde karşılanabilmesi için uluslararası alanda kabul gören standartlar ve uygulamalar geliştirerek kamunun yapılan denetimlere olan güvenini sağlamaya ve bu denetimlerin objektifliğini artırmaya çalışmışlardır. Bu kapsamda bilgi teknolojileri standart ve çerçevelerinin, bilgi sistemleri denetçileri tarafından en çok kullanılanları COBIT, ISO/IEC 27000 Standart Serisi, COSO, ITAF, ITIL olarak sayılabilir.

Bilgi sistemleri denetiminde izlenmesi gereken adımlar, denetçinin inceleme olarak bilgi sistemlerini temel alması dışında her finansal denetimde gerçekleştirilenlerle benzerlik göstermektedir. Denetim fonksiyonu, denetimin bağımsızlığı ve yeterliliğini korurken, denetim ekibi tarafından gerçekleştirilen çeşitli görevlerin denetim hedeflerini yerine getirmesini sağlayacak bir şekilde yönetilmeli ve yönlendirilmelidir.

Dünyada yaşanan büyük çaplı finansal skandallardan sonra 2002 yılında yürürlüğe giren Sarbanes-Oxley Kanunu, halka açık şirketler ve finansal tablo denetimine tabi tüm kuruluşlar için finansal raporlamayı etkileyen bilgi sistemleri kontrollerinin denetimini zorunlu kılmaktadır. Ülkemizde ise ilk olarak BDDK tarafından bankalara yönelik bilgi sistemleri denetimine ilişkin mevzuat yayımlanmış ve daha sonra Sayıştay tarafından kamu kurumlarında finansal denetimin yanı sıra bilgi sistemleri denetimine de başlanmıştır. Sermaye Piyasası Kurulu olarak ise *"Bilgi Sistemleri Yönetim İlkeleri Hakkında Tebliğ Taslağı"* ve *"Bilgi Sistemleri Bağımsız Denetim İlkeleri Hakkında Tebliğ Taslağı"*, 15 Kasım 2013 tarihinde kamunun görüşüne açılmıştır.

Kabul edilmelidir ki, finansal denetçinin mali tablolar üzerinde gerçekleştirdiği denetimin kalitesi, işletmenin kullanmış olduğu muhasebe bilgi sistemleri hakkındaki uzmanlığına ve bilgi sistemleri denetçisinin bu sistemler üzerindeki değerlendirmelerini dikkate almasına bağlıdır. İşletmenin mali tabloları ve diğer finansal veriler günümüzde çoğunlukla otomatize edilmiş bilgisayar sistemlerinin birer çıktısı olduklarından finansal denetimlerde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeleyecektir.

Finansal tablolar, işletmenin sahip olduğu bilgi sistemlerinden üretilen veriler temel alınarak hazırlanmaktadır. Finansal denetimi gerçekleştiren denetçiler ise bu veriler üzerinde inceleme yapmaktadır. Bu nedenle bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği finansal denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki eder. Bilgi sistemlerinin doğru çalışıp çalışmaması bilgi sistemlerinin denetimi ile ortaya çıkarılabilir. Bu nedenle finansal denetim ve bilgi sistemleri denetimi birbirleriyle yakından ilişkilidir.

İşletmelerin finansal raporlamalarında ve muhasebe verilerinde bilgi sistemlerini kullanmaları pek çok hata ve hilenin bu sistemler içinde gizli kalmasına sebep olmaktadır. Finansal denetçiler tarafından sadece bu sistemlerden elde edilen çıktılar ile girdileri karşılaştırmak, bu sistemlerin içinde gizlenmiş hile veya hatalara ulaşılmasını engellemektedir. Bu nedenle finansal denetimi gerçekleştiren bağımsız denetim ekibi,

denetlediği finansal bilgiyi üreten ve işleyen bilgi sistemlerinin denetimini de yürütmüş olduğu bağımsız denetimin bir parçası olarak görmelidir.

İşletmenin tüm alanlarına etki eden teknolojik gelişmeler ve yenilikler, muhasebe sistemlerinin yapısını da farklılaştırmaktadır. Sistemlerin elektronik hale gelmesine bağlı olarak bağımsız denetim içinde bilgi sistemleri denetiminin önemi her geçen gün artmaktadır. Bilgi sistemlerinin bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekmektedir. Denetçi sistem çıktılarına ek olarak bilgi sistemlerinin içyapısında bulunan önemli hata ve yanlışlıkları ortaya çıkarmalıdır ve tespit edilen hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır. Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.

Sonuç olarak, finansal denetimlerde, işletme tarafından denetçiye sunulan finansal bilgiler kadar bu bilgilere nasıl ulaşıldığı da denetimin bir parçasını oluşturmaktadır. İşletmelerin finansal tablolarının doğruluğu ve güvenilirliği konusunda yatırımcılara makul güvence vermeyi amaçlayan finansal denetimlerin günümüz şartlarında yetersiz kaldığı; sadece işletmeler tarafından sunulan girdi ve çıktıların kontrol edilmesiyle yapılan finansal denetimlerin, bu girdi ve çıktıların gizliliği, bütünlüğü ve güvenilirliği konusunda güvence vermeyi amaçlayan bilgi sistemleri denetimi ile bütünleşik bir şekilde yapılmadığı sürece tam anlamıyla bir güvence sağlayamadığı kabul görmüş bir gerçektir. İşletmelerin mali tablolarının doğru bir şekilde yansıtılması için;

- Mali tablo denetimleri bilgi sistemleri ile uyum içerisinde yürütülen bir bağımsız denetim faaliyeti olarak gerçekleştirilmelidir.
- Bilgi sistemleri genel kontrollerinin önemlilik kriterleri esas alınarak uyumluluk, etkinlik ve yeterlilik açısından incelenmelidir. Böylece denetim sırasında üzerinde detaylı çalışılmasının gerektiği alanlar belirlenebilir.
- Sistemler açısından veri giriş kontrolleri, veri işleme kontrolleri ve yetki kontrolleri detaylı olarak incelenmelidir.

- Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.
- Denetçi bilgi sistemleri üzerindeki incelemelerini tamamladıktan sonra, finansal raporların doğruluğuna yönelik karşılıklı kontroller yapmalıdır. Bilgi sistemlerinden üretilen verilerin finansal raporlara kaynak oluşturmasını teminen doğruluk, varlık ve bütünlük olarak kontrol edilmelidir. Bu noktada verilerin sistemlerden oluşturulup raporlama sonucuna kadar ki süreç içinde bozulmaya uğramadan finansal tablolara yansıtılıp yansıtılmadığı incelenmelidir.
- Sermaye Piyasası Kurulu'nun bağımsız denetim ile ilgili mevzuatları aracılığıyla, bilgi sistemleri denetimi ve finansal denetim uyumlu hale getirilmeli ve bu uyumun sağlanmasında yol gösterici olmak amacıyla bu iki denetimin nasıl birlikte yürütüleceğine ilişkin ayrıntılı bir rehber hazırlanmalıdır.
- Rehberin hazırlanmasında bilgi sistemleri denetimine ilişkin uluslararası düzeyde kabul görmüş standartlara referans verilerek, denetimlere ilişkin objektif ve kabul edilebilirliği yüksek bulgu ve öneriler içeren raporlar ortaya koyulmalıdır.

İÇİNDEKİLER

KISALTMALAR CETVELİ

AS	:	Auditing Standards
BDDK	:	Bankacılık Düzenleme ve Denetleme Kurumu
BDDT	:	Bilgisayar Destekli Denetim Teknikleri
BGYS	:	Bilgi Güvenliği Yönetim Sistemi
BS	:	British Standards
BSI	:	British Standards Institution
COBIT	:	The Control Objectives for Information and related Technology
COSO	:	Committee of Sponsoring Organizations
EDP	:	Electronic Data Processing
FAOA	:	Federal Audit Oversight Authority
IAASB	:	International Auditing and Assurance Standarts Board
IAP	:	International Auditing Practice Statement
IDW	:	The Institut der Wirtschaftsprüfer in Deutschland e.V.
IFAC	:	International Federation of Accountants
INTOSAI	:	The International Organisation of Supreme Audit Institutions
ISA	:	International Standards on Auditing
ISACA	:	Information Systems Audit and Control Association
ISACF	:	Information Systems Audit and Control Foundation
ISO	:	International Organization for Standardization
ITAF	:	The Information Technology Assurance Framework
ITGI	:	Information Technology Governance Institute
ITIL	:	Information Technologies Infrastructure Library
İDKK	:	İç Denetim Koordinasyon Kurulu
PCAOB	:	Public Company Accounting Oversight Board
SAS	:	Swiss Auditing Standards
SEC	:	Security Exchange Commission
TMSF	:	Tasarruf Mevduatı Sigorta Fonu
TSE	:	Türk Standartları Enstitüsü

1. GİRİŞ

Günümüzde birçok işletme ve kuruluşun süreç ve operasyonlarında bilgi sistemlerinden faydalanması, bu işletme ve kuruluşlara teknolojik yeniliklerin yanı sıra kendine özgü riskleri de beraberinde getirmiştir. Doksanlı yılların sonuna doğru dünya genelinde büyük yankı uyandıran Enron ve WorldCom gibi finansal skandallar sebebiyle ABD'de 2002 yılında yürürlüğe giren Sarbanes-Oxley Kanunu ile halka açık şirketler ve mali tablolar denetimine tabi diğer tüm kuruluşlar için bilgi sistemlerine ilişkin kontrollerin denetimi zorunlu tutulmuştur. Bilgi sistemleri denetimi, kamu ve toplum güveninin azalmasına neden olan benzer skandalların ileride yaşanmasını önlemek ve finansal raporlamanın doğruluğunu ve bütünlüğünü sağlamak adına kritik bir mekanizma haline gelmiştir.

Dünya genelinde yaşanan benzer skandallar sonucunda, yatırımcıların korunması ve toplum ve kamu çıkarlarının göz önünde bulundurulması amacıyla uluslararası kuruluşlar ve ülke otoriteleri gözetiminde, finansal raporlamanın doğruluğunu ve güvenilirliğini sağlayacak önemli adımlar atılmıştır. Bu kapsamda, dünyada bilgi sistemleri denetimi adına uygulamaya konulan standartların yanı sıra ülkemizde de bilgi sistemleri denetimine ilişkin bazı düzenlemeler yapılmıştır.

Çalışmamızın ilk bölümünde, konuya ilişkin geniş bir bakış açısı sağlanarak, ikinci bölümünde bilgi sistemleri denetimi kavramı, tarihçesi ve öneminden bahsedilmektedir.

Üçüncü bölümde, uluslararası kuruluşların bilgi sistemleri denetimine ilişkin geliştirdikleri standartlar ve yaptıkları çalışmalara yer verilmektedir.

Dördüncü bölümde, dünyada hâlihazırda uygulamada olan bilgi sistemleri denetimine ilişkin bilgilendirmeler yapılmış olup, Türkiye'deki uygulamalarından bahsedilmiştir.

Beşinci bölümde, bilgi sistemleri denetim süreçlerine ilişkin genel kabul görmüş yapıya yer verilmiş olup, bu yapıda denetim planlanmasının nasıl yapılması gerektiği, planlama kapsamında incelenecek kontrollerin nelerden oluştuğu ve rapor yazımının nasıl olması gerektiğine ilişkin alt başlıklara yer verilmiştir.

Değerlendirme ve öneriler bölümünde ise işletmelerde bilgi sistemleri denetiminin nasıl yürütülmesi gerektiği, finansal denetim ile uyumlu hale getirilmesi ve Kurulumuzun bağımsız denetim ile ilgili mevzuatına ilişkin öneriler yer almaktadır.

2. BİLGİ SİSTEMLERİ DENETİMİ

2.1. Bilgi Sistemleri Denetimi Kavramı ve Tarihçesi

2000'li yıllara doğru birçok işletme iş süreçlerini ve operasyonlarını bilgi sistemleri üzerinden yürütmeye başlamıştır. Başlangıçta, bilgisayarlar, yüksek satın alma ve işletim maliyetleri nedeniyle yalnızca büyük işletmeler tarafından kullanılırken, daha sonra kişisel bilgisayarların ortaya çıkması ve maliyetlerin çok hızlı bir şekilde azalması, orta ölçekli işletmelerin de süreç ve operasyonlarında bilgi sistemlerinden faydalanmasını sağlamıştır. Günümüzde ise, güçlü mikrobilgisayarların ve bunlarla ilişkili paket yazılımların yaygınlığı, küçük işletmeler tarafından bile bilgi sistemlerinin yaygın bir biçimde kullanılmasının önünü açmıştır. Buna paralel olarak, hızla gelişen bilgisayar teknolojisi ve bu teknolojilerin sunduğu imkânlardan faydalanmak isteyen işletmelerin başta finansal işlemler olmak üzere tüm iş süreçlerinde bilgi sistemlerini kullanmaya yönelmesi, bu teknolojilere özgü riskleri de beraberinde getirmiştir. Bu risklerin önlenmesine yönelik kontrol mekanizmalarını oluşturmayan işletmeler, bilişim sistemlerinde üretilen bilginin gizliliği, bütünlüğü, kullanılabilirliği ve güvenilirliği konusunda güvenlik zafiyetleri ile karşılaşabilmektedir. Söz konusu zafiyetler ise işletmeler açısından önemli miktarda para ve zaman kaybının yanı sıra, itibar kaybına da neden olabilmektedir. Bu nedenle, bilişim sistemlerinin kullanımı ile birlikte bu sistemlerin işletmelere getirdiği riskler, bilgi sistemleri denetim kavramının ortaya çıkmasına yol açmıştır.

Her ne kadar uluslararası kabul görmüş bir tanımı olmasa da, bilgi sistemleri denetimi, bir bilgisayar sisteminin, işletmenin varlıklarını ve verilerinin bütünlüğünü koruyup korumadığını, işletme hedeflerini etkin bir şekilde gerçekleştirip gerçekleştirmediğini ve kaynaklarını verimli bir şekilde tüketip tüketmediğini belirlemek için kanıt toplama ve değerlendirme süreci olarak tanımlanmaktadır (Weber, 1999: 35). İşletmenin faaliyetlerini verimli ve etkin bir şekilde gerçekleştirmek amacıyla kullandığı

tüm bilgi sistemlerinin süreç, kontrol ve varlıklarının gizlilik, bütünlük, güvenilirlik ve kullanılabilirliğine yönelik makul bir güvence sağlamak üzere yapılan inceleme ve değerlendirme süreci olarak daha genel bir tanım yapmak da mümkündür.

Kayıtlara göre bilgisayar teknolojisi muhasebe sistemlerinde ilk defa General Electric tarafından 1954 yılında kullanılmaya başlanmıştır. Bu tarihte, bilgi sistemlerinin denetimi yalnızca bilgisayar sistemlerinin çıktılarının denetlenmesi şeklinde yürütülmüştür. İş hayatında bilgisayarların kullanımının yaygınlaşması, bilgisayar kullanabilen insan sayısının artması, işletmelerin finansal verilerinin manuel olarak tutulmasının ve işlenmesinin zorlaşması ve finansal işlemlerin bilgisayarlarla daha etkin bir şekilde yapılabiliyor olması, çeşitli muhasebe sistemlerinin doğmasını sağlamıştır. Bunun sonucunda da elektronik veri işleme denetimi (EDP) ve elektronik veri işleme denetçileri ortaya çıkmıştır.

Bilgi sistemleri denetiminin büyümesi ve yaygınlaşması ise, "Equity Funding Corporation" Skandalı[1] sonrasında başlamıştır. Teknolojinin kötüye kullanımı olarak bilinen bu skandal olayda, işletme yöneticileri daha yüksek kar göstermek amacıyla muhasebe kayıtlarıyla oynamış ve bunun sonucunda pay fiyatları büyük oranda artış göstermiştir. Yapılan hile 10 yıl boyunca devam etmiş ve 1973 yılında gün yüzüne çıkarılmıştır. Bu skandaldan sonra kurumlar için bilgi sistemleri denetimine ihtiyaç duyulduğu görüşü hâkim olmuştur.

90'lı yılların sonunda ise AT&T[2] şirketinin bilgi sistemlerinin, yazılım hataları yüzünden çökmesi nedeniyle birçok kredi kartı sahibinin 18 saat boyunca fonlara ulaşamaması ve dünya genelinde ticaretin bu durumdan olumsuz etkilenmesi, bilgisayar

[1] Equity Funding Corporation of America, Los Angeles merkezli, 1960'lı ve 70'li yıllarda özel kişilere yatırım fonları ve hayat sigortası paketi satan bir şirkettir. Şirketin eski çalışanı Ronald Secrist ve menkul kıymet analisti Ray Dirks tarafından, Şirketin hayali sigorta poliçelerini oluşturduğu ve sakladığı özel olarak tasarlanmış bir bilgisayar sistemi ile birlikte devasa muhasebe dolandırıcılığı iddiası ortaya atıldıktan sonra başlatılan soruşturmada 100 kadar Şirket çalışanının organize aldatmacası ortaya çıkarılmıştır. (www.wikipedia.org/wiki/Equity_Funding)

[2] AT&T, merkezi Whitacre Tower, Dallas, Teksas, ABD'de bulunan çok uluslu bir telekomünikasyon şirketidir. Alexander Graham Bell tarafından kurulan Bell Telefon Şirketi'yle birleşmiş ve dönem dönem dünyanın en büyük telefon şirketi olmuştur. (www.tr.wikipedia.org/wiki/AT%26T)

sistemleri için güvence hizmetlerinin gerekliliğini bir kez daha göstermiştir (Yalkın (Demir), 2011: 22).

2000'li yılların başında meydana gelen Enron skandalı, hem Enron'un hem de şirketin muhasebe danışmanlığını yapan Arthur Andersen'in iflasına neden olmuş ve ayrıca birçok yatırımcı önemli tutarda para kaybederken birçok kişi de işsiz kalmıştır. Enron skandalı ve sonrasında meydana gelen diğer skandallara bir tepki olarak, 2002 yılında ABD'de çıkartılan Sarbanes-Oxley yasası, halka açık işletmeler ve denetim firmaları için yeni ve iyileştirilmiş standartlar getirmiştir (Dinç ve Cengiz, 2014: 223).

Ülkemizde ise 2003 yılında Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından T. İmar Bankası T.AŞ'ye ait bankacılık işlemleri yapma ve mevduat kabul etme izninin kaldırılması ve bu bankanın Tasarruf Mevduatı Sigorta Fonu'na (TMSF) intikaline sebep olan "çifte kayıt olayı" bilgi teknolojileri denetim kavramının öneminin her kesim tarafından iyice anlaşılması gerektiğini ortaya koymuştur (Özbilgin, 2003: 127).

2.2. Bilgi Sistemleri Denetiminin Önemi

Bilgi sistemleri denetimi, bir önceki bölümde de belirtildiği üzere, ilk olarak elektronik veri işleme (EDP) denetimi olarak ortaya çıkmıştır. İşletmelerin ticari alanda kullandıkları teknolojiler, muhasebe sistemlerinin bütünüyle otomatize bir şekilde kurulması ve işletilmesi, denetim hizmetlerinde de teknolojinin kullanılmasını zorunlu hale getirmiştir. İşletmelerin finansal raporlarının bilgi sistemleri tarafından üretilen bilgileri ihtiva etmesi, bu raporları değerlendiren ve inceleyen denetçiler için de bilgisayar becerilerinin geliştirilmesi ihtiyacı oluşmuştur. Ek olarak, bilgi sistemleri denetimi, kamu ve toplum güveninin azalmasına neden olan Enron ve WorldCom gibi dünya genelinde yaşanan skandalların gelecekte de yaşanmasını önlemek ve finansal raporlamanın doğruluğunu ve bütünlüğünü sağlamak adına kritik bir mekanizma haline gelmiştir.

Bunun yanı sıra, birçok işletme bilgi sistemlerinin operasyonlarına ve hizmetlerine sağlayabileceği avantajların farkına vardıklarından, bilgi sistemlerine büyük miktarda para harcamaktadır. Bilgi sistemleri denetimi, veri dolandırıcılığı, veri kaybı veya sızıntı riskini, hizmet kesintilerini ve bilgi sistemlerinin kötü yönetim riskini azaltmaya da

yardımcı olabilmektedir. Riskleri önleyecek etkin kontrol mekanizmalarının oluşturulmaması durumunda ise bu sistemler tarafından üretilen bilginin gizliliği, bütünlüğü ve kullanılabilirliği, dolayısıyla bu bilgiyi işleyen, saklayan ve raporlayan sistemlerin güvenliği ve güvenilirliği zarar görebilmektedir. Bu nedenle, bilgi sistemleri denetimi, işletmelerde bu sistemlerin yeterince güvenilir olduğu ve bu sistemlerden üretilen bilgilerin gizliliği, bütünlüğü ve kullanılabilirliği konusunda makul bir güvence sağlamak gibi önemli bir rol üstlenmektedir.

3. ULUSLARARASI KURULUŞLARIN BİLGİ SİSTEMLERİ DENETİMİ KAPSAMINDAKİ ÇALIŞMALARI

Bilgi sistemleri denetiminin en önemli unsuru bilgi sistemleri denetçisidir. Ancak bilgi sistemleri denetçisi, bilişim teknolojilerine ilişkin standartlara referans vererek denetimlerini icra edebildiği ölçüde, objektif ve kabul edilebilirliği yüksek bulgu ve öneriler içeren raporlar ortaya koyabilir. Bilgi teknolojilerine ilişkin standartlar, kurum yöneticilerine ve bilgi işlem birimlerinde çalışanlara yol gösterirken; bilgi sistemi 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 (Böcek, 2014: 23).

Dünya genelinde yaşanan skandallar sonucunda, yatırımcıların korunması ve toplum ve kamu çıkarlarının göz önünde bulundurulması amacıyla uluslararası kuruluşlar ve ülke otoriteleri gözetiminde, finansal raporlamanın doğruluğunu ve güvenilirliğini sağlayacak önemli adımlar atılmıştır. Bilgi sistemleri denetimi açısından söz konusu düzenlemeler ve standartlar; yasal düzenlemeleri, bilgi sistemleri denetimi standartlarını, bilgi sistemleri denetiminde mesleki yetkinliğin belirlenmesini, denetim süreci üzerinde inceleme faaliyetlerini ve yardımcı düzenlemeleri kapsamaktadır (Özbilgin, 2003: 123).

Günümüzde yalnızca bilgi sistemleri denetimine özgü olmayan, ancak bilgi sistemleri denetimi kapsamına giren risk, yönetim, kontrol ve bilgi güvenliği alanlarında uluslararası kuruluşlar tarafından geliştirilmiş standartlar ve çerçeveler de mevcuttur. Bu

standart ve çerçeveler içerdikleri usul ve esaslar itibarıyla birbirleri arasında sürekli geçişmekte ve güncellenerek daha da kapsamlı bir hale gelmektedirler.

Uluslararası kuruluşlar ve ülke otoriteleri, gelişen teknolojilere ve bu teknolojilerin işletmelerin iş süreçlerinde ve finansal raporlamalarında kullanımının artması ile birlikte yükselişe geçen denetim ihtiyacının, daha objektif ve daha güvenilir bir şekilde karşılanabilmesi için uluslararası alanda kabul gören standartlar ve uygulamalar geliştirerek, kamunun yapılan denetimlere olan güvenini sağlamaya ve bu denetimlerin objektifliğini artırmaya çalışmaktadırlar. Söz konusu standart ve iyi uygulama örneklerinden bazıları yalnızca bilgi sistemleri tarafından üretilen bilginin güvenliği üzerinde yoğunlaşırken, bazıları tüm bilgi sistemlerinin işletme ve kullanıcılar açısından az riskli olmasını ve işletmelerin yürüttüğü iş süreçlerine uygun olmasını amaçlamıştır. Bu kapsamda bilgi teknolojileri standart ve çerçevelerinin, bilgi sistemleri denetçileri tarafından en çok kullanılanları COBIT, ISO/IEC 27000 Standart Serisi, COSO, ITAF, ITIL olarak sayılabilir.

3.1. COBIT *(The Control Objectives for Information and Related Technology)*

Tanım olarak *"Control Objectives for Information and related Technology"*nin kısaltılmış hali olan COBIT'in Türkçe karşılığı *"Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri"* olarak ifade edilebilir. Türkiye'de BDDK tarafından yayınlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" uyarınca bankalara getirilen COBIT'te yer alan usul ve esasların uygulanması zorunluluğu ile ülkemizde de son yıllarda yayılmakta olan COBIT, iş ihtiyaçlarına göre bilgi sistemlerinin ne kadar hizmet verdiğinden emin olunmasını sağlayan öneriler bütününden oluşan bir çerçevedir.

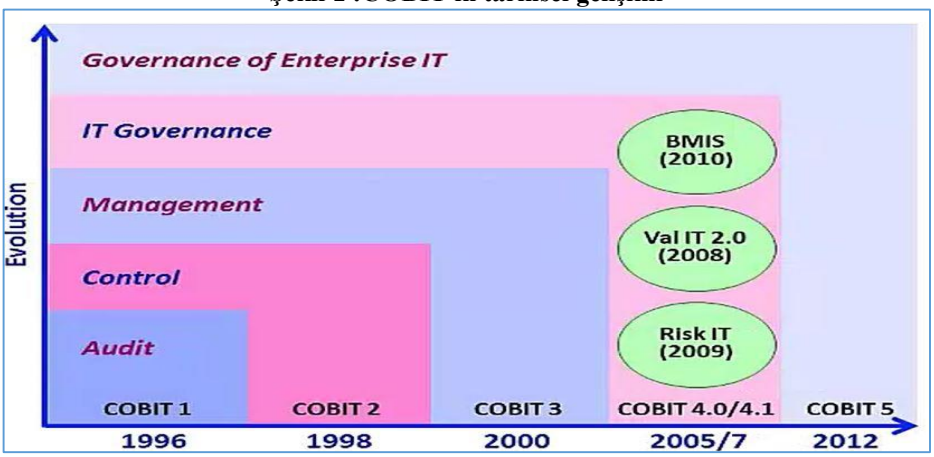
İşletmelerin operasyonlarına ve hizmetlerine fayda sağlayacak bilgilerin üretimi ve aktarımının hızlı, sürekli ve güvenli olarak sağlanabilmesi için kullandıkları bilgi sistemlerinden kaynaklanan risklerin belirlenmesi, yönetimi ve kontrolünün etkin ve verimli olarak yapılması gerekmektedir. Bu kapsamda, bilgi sistemlerinden kaynaklanan risklerin nasıl yönetileceği ve bu sistemleri nasıl daha güvenli hale getirecekleri sorularına yanıt arayan yalnızca bilgi işlem birimlerinin yöneticilerine değil, bilgi sistemlerini iş

süreçlerine entegre etmiş tüm yöneticilerin sorularına sistematik bir şekilde yanıt verecek şekilde oluşturulmuş bir çerçeve yöntem olan COBIT, aynı zamanda bilgi sistemlerinin maruz kaldıkları riskleri, bu risklerin değerlendirilmesi, yönetilmesi ve ortadan kaldırılmasına yönelik kontrolleri ve bu kontrollerin denetlenme yöntemlerini de ele alan bir bakış açısı ile oluşturulmuş bir mimariye sahiptir.

İşletmenin iş hedefleri doğrultusunda hizmet vermesini sağlamak amacıyla bilgi işlem kaynaklarını kullanmasını amaçlayan COBIT, verilen hizmetlerin istenilen kalite, güvenlik ve hukuksal ihtiyaçlara cevap vermesini sağlayan kontrol esaslı bir yaklaşımdır. Dolayısıyla, işletmelerin neler yapması gerektiği ile yetinir, bunların nasıl yapılması gerektiği ile ilgilenmez.

COBIT, Information Systems Audit and Control Foundation (ISACF)[3] tarafından ilk kez 1996 yılında oluşturulmuş ve teknolojik gelişmelere bağlı olarak son sürümü COBIT 5, Information Systems Audit and Control Association (ISACA) tarafından kurulan Information Technology Governance Institute (ITGI) tarafından 2012 yılında yayınlanmıştır. COBIT, ISACF tarafından bir denetim aracı olarak tasarlanmış olmasına rağmen, teknolojik gelişmelere bağlı olarak zamanla kontrol ve yönetim odaklı hale gelmiş, daha sonra ise bilgi teknolojilerinin yönetimi ve yönetişim odaklı kullanılan bir çerçeve olarak sunulmuştur.

Şekil 1 :COBIT'in tarihsel gelişimi



Kaynak: ISACA, 2013

[3] ISACF, ISACA'nın araştırma birimidir (Van Slyke, 2008: 1275).

Yukarıdaki şekilde görüldüğü üzere; COBIT, önceleri denetim, kontrol ve daha sonra yönetim odaklı çerçeve iken daha sonraları risk ve katma değer ile ilgili standartları da bünyesine katmış ve zamanla bir bilgi sistemleri yönetişim çerçevesi haline gelmiştir. Her versiyonunda kendisini yenilemeye devam eden COBIT, son olarak sadece bilgi sistemleri değil diğer iş süreçlerini de kapsayarak kapsamlı bir model haline gelmiştir (ISACA, 2012: 13).

Şekil 2: COBIT 5 Temel İlkeleri

Kaynak: ISACA, 2013

Yukarıdaki şekilde görüldüğü üzere; COBIT beşinci versiyonunda beş temel ilke üzerinde kurulmuştur. COBIT 5, sistem teorisinin temel varsayımlarını kullanarak birbiriyle etkileşim içerisindeki bileşkeleri dikkate alarak bütüncül bir yaklaşım sergilenmesi gerektiğini ortaya koymaktadır. Buna göre, gerçekleştiriciler kurumsal yönetişim ve yönetim açısından birbirini bütünleyen, diğer çerçeve ve standartların eksikliklerini tamamlayan, kurumun varlığını sürdürmesi için gerekli olan alt sistemlerden oluşan canlı bir sistemin birliğini tamamlamaktadır (ISACA, 2012: 13).

3.2. ISO/IEC 27000 Standart Serisi

ISO 27000 standartları her geçen gün büyüyen ISO/IEC ISMS standart ailesinin bir parçasıdır. ISO 27000 standart serisi; ISO 27001, ISO 27002, ISO 27003, vd. uluslararası standartları içeren bir standart ailesidir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ana

standardı olup diğer standartlar ise bu standardın uygulanmasına yardımcı sözlük, rehber, metrik ve ölçümler, belgelendirme ve bazı farklı sektörlere uyarlanması olarak birbirinden ayrışmıştır.

ISO/IEC 27001 standardının tarihi gelişimi, 1992 yılında İngiltere'de kamu ve özel sektörde yer alan birçok kuruluşun bilgi güvenliği standardı oluşturulmasına yönelik isteği dikkate alınarak, İngiliz Standartları Enstitüsü (BSI) desteği ile oluşturulan çalışma grubu tarafından BS (British Standart) 7779 adında bir rehber oluşturulması ve söz konusu rehberin BSI tarafından BS 7779 İngiliz Standardı olarak kabul edilmesi ile başlamıştır. İlgili standart BS 7779 – 1 ve BS 7779 – 2 olarak iki kısımdan oluşmuştur. BSI tarafından 1999 yılında BS 7779 – 2 Bilgi Güvenliği Yönetim Sistemi Gereksinimleri adı altında yayımlanmış ve ISO (International Organization for Standardization – Uluslararası Standardizasyon Kuruluşu) tarafından 2000 yılında ISO/IEC 17799 standardı olarak kabul görmüştür. İlgili standart ülkemizde de 2002 yılında Türk Standartları Enstitüsü (TSE) tarafından referans alınmıştır. Daha sonra ISO tarafından 2005 yılında ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereklilikleri adı altında yayımlanmıştır. 2006 yılında ISO/IEC 27001:2005 sürümü ve 2014 yılında ISO/IEC 27001:2013 sürümü TSE tarafından Türkçe olarak yayımlanmıştır (Haklı, 2012: 16).

Vural ve Sağıroğlu'na göre (2008: 5), ISO 27001, Bilgi Güvenliği Yönetim Sistemi (BGYS) için en iyi uluslararası uygulama ve standart olarak ifade edilmiştir. Bu standart, BGYS için gereklilikleri ortaya koyan bir standarttır ve bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur. BGYS, işletmenin gizli veya hassas kurumsal bilgilerini yönetmek için sistematik bir yaklaşım sunar ve böylece bilginin kullanılabilirliğini, gizliliğini ve bütünlüğünü koruyarak bilginin güvenliğini sağlar. Yalnızca bilgi sistemlerini değil, süreçleri ve hatta insanları da kapsar. Bir işletme bu standarda göre BGYS'yi uygulayacaksa, BGYS'nin gereklerini anlamalı ve bu alanlara dikkat etmelidir. ISO 27001'e göre BGYS aşağıdaki 10 alanda güvenliğin gerekli olduğuna odaklanmıştır.

Güvenlik Politikası: Bu çalışma, işletmenin iş hedefleri ve bilgi güvenliğine bağımlılığının kapsamlı bir şekilde anlaşılmasını içerir. Bu çalışmalara ilk olarak bilgi

sistemleri güvenlik politikasının oluşturulmasıyla başlanır. Bu son derece önemli bir görevdir ve üst yönetimin tamamı tarafından onaylanmalıdır.

Organizasyonel Güvenlik: İşletme içinde bilgi güvenliğini başlatmak, uygulamak ve kontrol etmek için bir yönetim çerçevesinin oluşturulması gerekir. Yönetim çerçevesinin oluşturulması ise, bilgi güvenliği politikasının onaylanması, güvenlik rollerinin atanması ve güvenliğin işletme içindeki koordinasyonu için uygun prosedürlere ihtiyaç duyar.

Varlık Sınıflaması ve Kontrolü: En zahmetli, ancak zorunlu görevlerden biri, bilgi varlıkları, yazılım varlıkları, fiziksel varlıklar veya benzeri diğer hizmetler olmak üzere tüm bilgi sistemlerinin varlıklarının envanterini yönetmektir.

Personel Güvenliği: Hırsızlık, dolandırıcılık veya tesislerin kötüye kullanılmasından insan hataları, ihmal ve açgözlülük sorumludur. Alınması gereken çeşitli proaktif önlemlerden önemli olanları ise, personel tarama politikalarını belirlemek, gizlilik anlaşmaları yapmak, istihdam şartlarını ve koşullarını oluşturmak, bilgi güvenliği eğitimini almak ve bu konuda personeli sürekli eğitmektir. Güvenlik konusunda nelere dikkat edeceğinin farkında olan iyi eğitim almış çalışanlar, gelecekteki güvenlik ihlallerini önlemekte kilit rol oynayabilir.

Fiziksel ve Çevresel Güvenlik: Fiziksel güvenlik ortamı, fiziksel giriş kontrolü, güvenli ofisler, odalar, tesisler, fiziksel erişim kontrolleri, ateşten elektromanyetik radyasyona kadar çeşitli riskleri en aza indiren ve güç kaynaklarına ve veri kablolarına koruma cihazları sağlayan bazı faaliyetlerden oluşur. Bu faaliyetlerin uygun maliyetlerle tasarlanması ve sürekli izlenmesi, yeterli derecede fiziksel güvenlik denetimini korumanın iki temel özelliğidir.

İletişim ve Operasyon Yönetimi: Tüm bilgi işlem tesislerinin yönetimi ve işletilmesi için doğru dokümante edilmiş prosedürler oluşturulmalıdır. Buna ayrıntılı çalışma talimatları ve olaylarla ilgili müdahale prosedürleri dâhildir.

Erişim Kontrolü: Bilgi ve iş süreçlerine erişim, iş ve güvenlik gereklilikleri çerçevesinde kontrol edilmelidir.

Sistem Geliştirme ve Bakım: Güvenlik, bir sistemin başlangıcında ideal bir şekilde oluşturulmalıdır. Bu nedenle güvenlik düzenlemeleri, bilgi sistemlerinin geliştirilmesinden önce belirlenmeli ve üzerinde anlaşmaya varılmalıdır. Güvenlik düzenlemeleri ise, güvenlik ihtiyaçlarının analizi ve spesifikasyonu ile başlar ve her aşamada, veri girişi, veri işleme, veri saklama, veri alma ve veri çıkışı gibi kontroller sağlar. Örnek vermek gerekirse, bir işletmede şifreleme denetimleri ile uygulamalar oluşturmak gerekebilir. Şifreleme, dijital imza, şifreleme anahtarlarının korunması ve kriptografi için kullanılacak standartların kullanılabileceği bu kontrollerin kullanımı hakkında tanımlanmış bir politika olmalıdır.

İş Sürekliliği Yönetimi: Felaketlerden kaynaklanan ve güvenlik arızalarının neden olduğu aksaklıkları azaltmak için bir iş sürekliliği yönetim süreci tasarlanmalı, uygulanmalı ve periyodik olarak test edilmelidir.

Uyum: Fikri mülkiyet hakları, yazılım telif hakları, kurumsal kayıtların korunması, kişisel bilgilerin korunması ve gizliliği, bilginin kötüye kullanımının önlenmesi gibi hususlara ilişkin ulusal ve uluslararası bilgi teknolojileri yasalarına sıkı sıkıya bağlı kalınması esastır.

Bu standartta ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm işletmelere uygulanabilir olması hedeflenmiştir (TS ISO/IEC 27001, 2013). Ayrıca, ISO 27001, teknik ve teknoloji bağımlı bir standart değildir ve belli bir ürün veya bilgi teknolojisi ile ilgilenmez. Hatta bilgi teknolojileri güvenliği de söz konusu standart içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir. Teknik detaylara inmeden kuruluşların bilgi güvenliği hususunda neler yapması gerektiğini açıklar.

3.3. ITAF *(The Information Technology Assurance Framework)*

ITAF, bilgi sistemleri denetim ve güvence uzmanlarının rol ve sorumluluklarına, bilgi ve becerilerine, gayret, davranış ve raporlama gereksinimlerine yönelik standartlar oluşturan, bilgi sistemleri güvencesine özgü terim ve kavramları tanımlayan, bilgi sistemleri denetim ve güvence raporlarının planlanması, tasarlanması, yürütülmesi ve

raporlanması konularında gerekli araçları, teknikleri ve rehberliği sağlayan kapsamlı ve iyi uygulama odaklı bir referans modelidir.

ITAF, ISACA'nın bilgi sistemleri denetim ve güvence standartları üzerine yoğunlaşmıştır ve bilgi sistemleri denetim ve güvence uzmanlarının rehberlik, araştırma politikaları ve prosedürleri talep edebilmesi, denetim ve güvence programları edinebilmesi ve etkili raporlar geliştirebilmesi için tek bir kaynak sunmaktadır.

ITAF metni; "Bilgi Sistemleri Denetim ve Güvence Standartları", "Bilgi Sistemleri Denetim ve Güvence Kılavuzları" ve "Bilgi Sistemleri Denetim ve Güvence Araç ve Teknikleri" ana başlıklarını içeren üç bölümden oluşmaktadır. İlk iki bölüm Genel, Performans ve Raporlama olarak yine üç bölüme ayrılmıştır. Birinci bölüm bilgi sistemleri denetimi ve güvencesi alanlarında olması gereken standartları tanımlarken, diğer iki bölüm standartların uygulanmasına ilişkin rehberleri, araç ve teknikleri sunmaktadır.

ITAF, bilgi sistemleri denetim ve güvence uzmanları tarafından uygulanan bilgi sistemleri uygulamaları ve altyapısının bileşenleri üzerinde güvence sağlayan bir standartlar bütünüdür. Söz konusu standartların, bu standartlara yol gösterici rehber, araç ve tekniklerin tasarlanmasında bilgi sistemlerinin denetim ve güvence raporlarının kullanıcıları da dâhil olmak üzere, daha geniş bir yelpazeye fayda sağlayacak şekilde olmasına bilhassa dikkat edilmiştir. Çerçevenin uygulanması, bilgi sistemleri denetim ve güvence işinin yürütülmesi için bir önkoşuldur. Denetimlerinde ITAF'ı uygulayan bilgi sistemleri denetçisi, ITAF içerisinde yer alan bilgi sistemleri denetim ve güvence standartlarını uygulamak zorundadır. Rehberler, araçlar ve teknikler denetim ve güvence raporlaması sürecinde zorunlu olmayan bir destek sağlaması için tasarlanmıştır (ITAF, 2014:5).

3.4. COSO *(Committee of Sponsoring Organizations)*

1980'li yılların başında ortaya çıkan muhasebe skandalları nedeniyle Hileli Finansal Raporlamalar Komisyonu (Treadway Komisyonu) bugün halen aktif faaliyet gösteren COSO'yu kurmuştur (Karakaya, 2016: 160). Açılımı, "Committee of Sponsoring

Organizations" olup, Amerikan Mali Müşavirler Odası'nın da içinde bulunduğu bu yapının amacı, iç kontrol kavramının net olarak anlaşılmasını sağlamak ve işletmelerde uygulanabilmesi için yol gösterici önerilerde bulunmaktır.

COSO tanımına göre iç kontrol, yönetim kurulu, üst düzey yönetim ve işletmenin diğer çalışanlarınca etkilenen ve işletme operasyonlarının etkinliği ve verimliliği, finansal raporlamanın güvenilirliği ve yasal düzenlemelere uyum hedeflerinin yerine getirildiğine dair makul bir güvence sağlamak amacıyla tasarlanan bir süreçtir.

İşletmelerde iç kontrol yapısının var olması iç kontrol bileşenleri ile mümkündür. Bu bileşenler, "Kontrol Ortamı", "Risklerin Değerlendirilmesi", "Kontrol Faaliyetleri", "Bilgi Paylaşımı ve İletişim" ve "İzleme" olmak üzere beş adettir (Moeller, 2014: 36). COSO'nun ilk baştaki tasarımında iç kontrol unsurları, yukarıda bahsedilen beş ana unsurdan oluşan bir piramit olarak tasvir edilmiştir. Yenilenmiş COSO'da ise, iç kontrol yapısı üç boyutlu bir küp şeklinde tasvir edilmiştir. Küpün üzerinde üç boyut bulunmaktadır; bunlar "unsurlar", "iç kontrol amaçları" ve "örgüt yapısı"dır. Unsurlar, yukarıda bahsedilen beş ana kategoriden oluşmaktadır. İç kontrol amaçları üç ana kategoride incelenmektedir: "faaliyetler", "mali raporlama" ve "uygunluk". Küpün üçüncü boyutundaki örgüt yapısında ise, işletmenin genel kurumsal yapısı, alt bölümleri, varsa iştirakleri ve detay fonksiyonları yer almaktadır. Aşağıda öncelikle COSO modelinin yukarıda sayılan beş unsuru özetlenmiştir.

Kontrol Ortamı

Kontrol ortamı, iç kontrolün ne kadar başarılı olabileceğini belirleyen temel unsurudur. İşletmenin faaliyetlerini yapma biçimini ifade eder. İşletmedeki iç kontrol ortamının sağlıklı ve etkin çalışabilmesi için üst yönetim ve çalışanların sorumluluk ve yetkilerinin sınırını iyi bilmesi gereklidir. Bir kurumun çalışma disiplinin oluşumunda esas belirleyici olan yönetim kurulu ile üst yöneticilerdir. Dolayısıyla kontrol ortamının ana belirleyicisi olan kurum çalışanlarının kontrol bilincinin üst yönetim tarafından etkilenebilme derecesidir (McNally, 2013: 5).

Risklerin Değerlendirilmesi

İşletmeler, kendilerine tahsis edilen kaynakları amaç ve hedeflerine ulaşmak için kullanırlar. Bu kaynakların kullanımı için alınan kararlar yürütülen faaliyet, süreç ve projeler beraberinde riskleri de getirir. Risk yönetimi, işletmelerin amaç ve hedeflerine ulaşmalarına yardımcı olan bir araçtır. Risk yönetimi, risk stratejisinin belirlenmesi, risklerin tespit edilmesi, değerlendirilmesi, risklere cevap verilmesi, risklerin gözden geçirilmesi ve raporlanması aşamalarını kapsar (McNally, 2013: 5).

Kontrol Faaliyetleri

Kontrol faaliyetleri, öngörülen bir riskin etki ve/veya olasılığını azaltmayı ve böylece işletmenin amaç ve hedeflerine ulaşma olasılığını artırmayı amaçlayan eylemlerdir. Kontrol faaliyetlerinin belirlenmesi, risk değerlendirmesinin tamamlanmasına bağlıdır. Yönetim, görevlerin ve hedeflerin gerçekleştirileceğine dair makul güvence elde etmek için risk yönetimini esas almak suretiyle kontrol faaliyetlerini planlamalı, bunları organize etmeli ve yönlendirmelidir. Kontrol faaliyetleri mali olan ve olmayan kontrolleri kapsamakta olup işletmenin tüm faaliyetleri için bir bütün olarak tasarlanıp uygulanmalıdır (McNally, 2013: 5).

Bilgi Paylaşımı ve İletişim

İç kontrol yapısı, diğer dört unsur arasındaki ilişkiyi bilgi paylaşımı ve iletişim yoluyla sağlar. İşletme genelinde bilgi akışını düzenlenmesi, kurumsal amaç ve hedeflere ulaşma yolunda bir araç olarak görülen iç kontrol yapısının işlerliği ve uygulanma kabiliyetinin artmasında önemli bir role sahiptir. İletişim, bilginin işletme içinde gerek yatay ve dikey olarak, gerekse işletme dışında uygun mekanizmalarla ilgili kişi, idare ve mercilere iletilmesini ve dönüşümünü ifade eder (McNally, 2013: 5).

İzleme

İzleme, işletmenin amaç ve hedeflerine ulaşma konusunda iç kontrol yapısının beklenen katkıyı sağlayıp sağlamadığının, iç kontrol standartlarına uyum çerçevesinde değerlendirilmesi ve sistemin iyileştirmeye açık alanlarına yönelik eylemlerin belirlenmesidir. İzleme ile, işletmenin faaliyetlerinin misyon doğrultusunda, hedeflerle uyumlu olarak yürütülüp yürütülmediği, risk yönetimi esasları çerçevesinde gerekli

kontrollerin öngörülüp öngörülmediği, söz konusu kontrollerin uygulanıp uygulanmadığı, iletişimin açık ve yeterli olup olmadığı gibi hususlar tespit edilip değerlendirilmektedir (McNally, 2013: 5).

COSO iç kontrol modelinin, içeriğinin kapsayıcılığı, kurumlara uygulama rehberi sunması ve çağın gereklerine göre yenilenerek yaşayan bir model olması gibi nedenlerle dünya çapında en yaygın olarak kabul görmüş model olduğu görülmektedir.

3.5. ITIL *(Information Technologies Infrastructure Library)*

ITIL, Information Technologies Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi) sözlerinin baş harflerinden oluşmuş bir kısaltmadır. ITIL servis yönetim metodolojisi, bilgi teknolojileri servislerini eksiksiz ve en iyi kalitede yönetmek için geliştirilmiştir. ITIL, servis yönetimini en iyi şekilde sürdürmek için kullanıcılarına rehberlik etmektedir.

ITIL'ın ilk versiyonu 1985 yılında yayınlanmıştır ancak bu yayınlar hakkında o döneme ait pek fazla bir bilgi bulunmamaktadır. ITIL'ın, ikinci versiyonu ise 2001 yılında 8 kitap olarak yayınlanmış olup, bu versiyonda servis disiplinini ön plana çıkarmıştır. Son versiyonu olan ITIL v3 ise, 2007 yılında yayımlanmış ve bahse konu versiyonda bir önceki sürüme göre modülerden yaşam döngüsü yapısına geçilmiştir. Özetle, bir servisin planlanmasından sonlandırılmasına kadar ki süreci kapsamaktadır (ICAI, 2017: 4).

Bilgi sistemleri hizmet yönetimi, iş ihtiyaçlarına uygun bilgi sistemleri hizmetlerini planlama, tedarik etme, tasarlama, uygulama, işletme, destekleme ve geliştirme ile ilgilidir. ITIL, bilgi sistemleri hizmet yönetimi ve ilgili süreçler için kapsamlı ve tutarlı bir en iyi uygulama çerçevesi sağlar ve bilgi sistemleri hizmet yönetiminde etkinlik ve verimlilik sağlamak için yüksek kaliteli bir yaklaşım sunar. ITIL uygulayan işletmeler, maliyetleri düşürmeyi, erişilebilirliği artırmayı, kapasiteyi ayarlamayı, iş gücünü artırmayı, kaynakların verimli kullanılmasını sağlamayı ve ölçeklenebilirliği artırmayı hedeflemektedir. ITIL'ın işletmelerin sistemlerine başarılı bir şekilde entegre edilmesi durumunda bu hedefler kendiliğinden gerçekleşecektir.

Bu kapsamda ITIL'ın bilgi sistemleri hizmetleri için oluşturduğu bir yaşam döngüsü mevcuttur. ITIL bu hizmet yaşam döngüsünü 5 aşamada açıklar. Bu aşamalar,

hizmet stratejisi, hizmet tasarımı, hizmet geçişi, hizmet operasyonu ve devamlı hizmet iyileştirme olarak belirlenmiştir. Özetlemek gerekirse, ITIL ile servis yönetim metodolojisi gerçekleştiren işletmeler, bir hizmet stratejisi ile uzun dönem hedeflerini belirlemiş olurlar. İşletmeler, bu doğrultuda bilgi sistemleri hizmetlerini tasarlar ve bu hizmetin canlı ortama geçişini gerçekleştirirler. Daha sonra bu servisin sürekli ayakta kalması ve daha iyi hizmet verebilmek için daha iyiye doğru yol alması yönünde çalışmalar yaparlar.

ITIL, bir işletmenin iş süreçlerini desteklemeyi amaçlamakla birlikte dikte etmeyi amaçlamaz. ITIL çerçevesinin rolü, işletmelerin kendi uygulamalarını temel alabilecekleri yaklaşımları, işlevleri, rolleri ve süreçleri tanımlamaktır. ITIL'ın rolü, genel olarak uygulanabilir olan en düşük seviyede rehberlik vermektir (ITGI, 2008: 5).

3.6. ISA *(International Standards on Auditing)*

Muhasebecilik alanında dünyadaki en büyük mesleki birlik olan IFAC (International Federation of Accountants), denetime yönelik koyduğu standartlar ve bunların sürekli olarak geliştirilmesiyle ilgili olarak faaliyet gösteren en büyük kuruluştur. IFAC'ın bünyesinde bulunan IAASB (International Auditing and Assurance Standarts Board) tarafından yayımlanan ISA yani uluslararası denetim standartları ve IAP (International Auditing Practice Statement-Uluslararası Denetim Uygulamaları), denetim uygulamaları konusunda birlik sağlanması bakımından son derece önemlidir. ISA, genel olarak mali tabloların denetiminde kullanılan standartlardan meydana gelse de, bu standartlar işletmenin diğer bilgi, hizmet ve süreçlerinin denetimlerinde de kullanılabilirler (Özbilgin, 2003: 124).

ISA altında yer alan bazı standartlarda bilgi sistemleri denetimine ilişkin kontroller yer almaktadır. Bu maddelerin bazıları denetçinin işletmenin finansal raporlamasında yer alan bilgi sistemleri yapısı hakkında bilgi sahibi olması gerektiğine vurgu yaparken, bazıları ise risk değerlendirmesinde bilgi sistemi uzmanlığına ihtiyaç duyulduğuna ve denetim kanıtları elde edilirken bilgi sistemleri genel kontrollerine bakılması gerektiğini ifade eder. İçerisinde bilgi sistemleri denetimine ilişkin maddeler bulunan ISA standartları aşağıda özetlenmiştir.

ISA 240: Bu standart finansal tabloların denetiminde, denetçinin hileye ilişkin sorumluluklarını ele almaktadır. Anılan standardın 34'üncü paragrafında özetle, denetçinin, denetim sırasında adli bilişim ve bilgi sistemleri gibi teknik bilgi ve beceri gerektiren alanlarda, bu alanda bilgi ve deneyim sahibi kişi veya kişileri görevlendirerek finansal raporlama denetimlerinde karşılaşılan hile kaynaklı risklerin önüne geçebileceği ifade edilmiştir. Aynı standardın 42'nci paragrafında ise, otomatik süreç ve kontrollerin dikkatsizlikten kaynaklı hata risklerini azalttığı görülse de, denetçinin, bu kontrollerin dışarıdan müdahale risklerini barındırdığını göz önünde bulundurması gerektiği ifade edilmiştir.

ISA 265: Bu standart denetçinin finansal tabloların denetimi sırasında tespit ettiği iç kontrol eksikliklerini uygun bir biçimde işletmenin yönetimden sorumlu kişilere bildirmesine yönelik sorumluluğunu düzenler. Bu standardın ilgili paragraflarında özetle, bilgi sistemleri kullanılarak oluşturulan otomatik kontrollerce önlenemeyen risklerin yönetimin bilgisi dâhilinde olup olmadığının tespit edilmesi gerektiği, otomatik kontrollerin eksikliği durumunda ise, eğer önemli bir kontrol olduğu kanaatine varılırsa üst yönetimde yer alan kişilere bu kontrol eksikliğinin bildirilmesi gerektiği ifade edilmiştir.

ISA 300: Finansal tabloların denetiminin planlanmasına ilişkin denetçinin sorumluluğu üzerinde duran bu standarda göre, denetim stratejisinin oluşturulması aşamasında verilerin erişilebilirliği ve bilgisayar destekli denetim tekniklerinin kullanımı dâhil olmak üzere, bilgi sistemlerinin planlanan denetim metodolojisi üzerindeki etkisinin belirlenmesi gerektiği ifade edilmiştir.

ISA 315: Bahse konu standart, denetçinin işletmenin iç kontrolleri dâhil olmak üzere, finansal tablolardaki önemli yanlışlık risklerini belirleme ve değerlendirme sorumluluğunu düzenler. Bu standarda göre, denetçi işletmenin ilgili iş süreçleri dâhil finansal raporlamayla ilgili bilgi sistemi ve işletmenin bu bilgi sistemlerinden kaynaklanan risklere nasıl karşılık verdiği hakkında bilgi edinmelidir.

ISA 330: Bu standart, finansal tabloların denetimi sırasında, denetçi tarafından ISA 315'e uygun olarak belirlenen ve değerlendirilen önemli yanlışlık risklerine karşı

yapılacakları tasarlamakla ve uygulamakla yükümlü olan denetçinin sorumluluğunu açıklar. Bu standarda göre, denetçi önceki denetimlerden elde edilen denetim kanıtlarının kullanılmasının uygun olup olmadığına karar verirken genel bilgi sistemleri kontrollerinin halen etkin olup olmadığına bakması gerekmektedir.

ISA 402: Bu ISA standardı dışarıdan hizmet alan bir işletmenin bir veya daha fazla hizmet kuruluşu kullanması halinde, denetçinin bu hizmet sağlayıcılar hakkında da yeterli ve uygun denetim kanıtı elde etme sorumluluğunu düzenler. Bu standarda göre, işletmenin finansal raporlamaya ilişkin bilgi sistemleri faaliyetleri destek hizmeti kapsamında dışarıdan bir kuruluş tarafından sağlanıyorsa, söz konusu kuruluşun da sağladığı hizmete yönelik kontrollerinin, denetim kapsamında değerlendirilmesi gerekmektedir (ISA, 2017).

4. DÜNYADA VE TÜRKİYE'DE BİLGİ SİSTEMLERİ DENETİMİ

Bilgi sistemlerinin işletmelerin temel iş süreçlerinde ve finansal raporlama sistemlerinde büyük oranda bütünleşmiş bir şekilde kullanılmaya başlanmasıyla birlikte, ülke uygulamalarında bilgi sistemleri denetimi, denetim faaliyetlerinde etkin bir rol oynar hale gelmiştir. Özellikle, işletmelerin finansal raporlamalarındaki yanlışlıklar nedeniyle yaşanan skandallar, ülke otoritelerini bilgi sistemleri denetim faaliyetlerine ilişkin düzenlemeler yapmaya yöneltmiştir. Bu kapsamda bazı ülkelerin denetim faaliyetleri düzenlemeleri ve yetkili kuruluşlarının bilgi sistemleri denetim süreçlerine ilişkin yayımladıkları standartlar ile Türkiye'de uygulanan bilgi sistemleri denetim süreçlerine ilişkin mevzuat ve standartlar incelenmiştir.

4.1. ABD'de Bilgi Sistemleri Denetimi

2000'li yılların başında ABD'de yaşanan ENRON ve WorldCom gibi finansal tabloların yanlış beyan edilmesinden kaynaklanan skandallar sonrası yayımlanan Sarbanes-Oxley Yasası, işletmelerin finansal raporlamasına ve yönetimsel kontrollere ilişkin düzenlemeleri içermektedir. Bu yasa ile kurulan PCAOB - Public Company Accounting Oversight Board (Halka Açık Şirketlerin Muhasebe Gözetimi Kurulu), kamunun bağımsız denetime olan güvenini geri kazanmak için denetim, kalite kontrol ve denetçinin bağımsızlığına ilişkin süreçlerin gerçekleştirilmesinden sorumlu SEC (Security Exchange Commision) gözetimine tabi bir kuruluştur (Gökalp, 2005: 109).

PCAOB tarafından yayımlanan standart setinde, işletmenin iç kontrol sisteminin finansal tablo denetimleri ile birlikte yürütülmesi gerektiği ve bu kapsamda iç kontrol sisteminin tasarım ve işleyiş açısından etkinliğinin belirlenmesi gerektiği belirtilmektedir. Bu kapsamda, denetlenen işletmenin bilgi sistemleri süreçlerine ilişkin kontrollerin yer aldığı PCAOB tarafından yayımlanan AS - Auditing Standards (Denetim Standartları) aşağıda özetlenmiştir.

AS 2100: Bu denetim standardı grubu, denetimin planlanması ve risk değerlendirmesi üzerine bazı kontroller sunmaktadır. Bu standarda göre denetçinin, işletmenin finansal raporlama ile ilgili süreçleri de dâhil olmak üzere işletmenin bilgi sistemi hakkında bilgi sahibi olmasının yanı sıra, işletmenin bilgi sistemlerini kullanmayı bilmesi ve bu bilgi sistemlerinin finansal tabloları nasıl etkilediğini anlaması gerekmektedir.

AS 2200: Finansal raporlamada yer alan iç kontrol sisteminin denetimi hakkında kontroller sunan bu standart grubunda denetçinin, bilgi sistemleri de dâhil olmak üzere tüm ilgili iş süreçleri aracılığıyla üretilen belgeleri ve kullanılan bilgi teknolojilerini, işletmenin finansal tablolarına yansıtılana kadar takip etmesi gerektiği ifade edilmiştir.

4.2. İsviçre'de Bilgi Sistemleri Denetimi

İsviçre'de 2005 yılında bağımsız denetim faaliyetlerine ilişkin denetçilerin yetkilendirilmesi ve gözetiminden sorumlu bir kuruluş olarak yetkilendirilen FAOA - Federal Audit Oversight Authority (Federal Denetim Gözetimi Kurumu), işletmelerin finansal tablolarının denetiminde bütünleşik olarak yürütülen bilgi sistemleri denetim süreçlerine ilişkin standart ve rehberleri yayımlama yetkisine de sahiptir. FAOA denetim süreçlerinde, ISA standart setlerinin yanı sıra kendi ulusal denetim standartları olan SAS - Swiss Auditing Standards (İsviçre Denetim Standartları) standart setlerini de kullanmaktadır. Bu standart setlerinden bilgi sistemleri denetim süreçleriyle ilgili olanlar aşağıda yer almaktadır.

ISA/SAS 200: Bağımsız denetçinin genel hedefleri ve ulusal denetim standartlarına göre denetim yaptırılmasına ilişkin kontroller sunan bu standartta, denetimin konusunu oluşturan tüm alanlarda, bilgi sistemleri denetçisinin denetlenen

işletmeye karşı tamamıyla bağımsız olması ve denetim faaliyetini sürdürebilecek teknik bilgi ve yeteneğe sahip olması gerektiği belirtilmiştir.

ISA/SAS 300: İşletmenin finansal tablolarının denetiminin planlanmasına ilişkin maddelerin yer aldığı bu standartta, denetim planının oluşturulması aşamasında verilerin erişilebilirliği ve bilgisayar destekli denetim tekniklerinin kullanımı dâhil olmak üzere, bilgi sistemlerinin planlanan denetim yöntemi üzerindeki etkisinin belirlenmesi gerektiği ifade edilmiştir.

ISA/SAS 500: Bu standartta, denetim sonucunda elde edilen kanıtların, denetimin amacına ulaşabilmesini sağlayacak derecede yeterli, güvenilir ve makul bir güvence sağlayabilmesi için denetim sürecinde finansal raporlama dâhil işletmenin iş süreçlerini etkileyen bilgi sistemlerinin de denetlenmesi ve bilgi sistemleri denetçisinin bulgularını destekleyen denetim kanıtlarının belgelendirilmesi gerektiği belirtilmiştir.

SAS 890: Bu standarda göre, denetlenen işletmenin iç kontrol sisteminin varlığının doğrulanması gerekmektedir ve bu kapsamda işletmenin bilgi sistemleri genel kontrollerinin de denetçi tarafından test edilmelidir.

4.3. Almanya'da Bilgi Sistemleri Denetimi

Almanya'da denetim standartlarının yayımlanmasından sorumlu kuruluş olan IDW - The Institut der Wirtschaftsprüfer in Deutschland e.V. (Almanya Denetçiler Enstitüsü), Almanya'nın Avrupa Komisyonu'nun Denetim Direktifi'ne tabi olmasından dolayı ISA standart setini uygulamaya koymasının yanı sıra, bu standart setinin ulusal anlamda eksik kaldığı düşünülen noktalarda kendi denetim standartlarını oluşturmuştur. Bu kapsamda, IDW'nin, işletmelerin finansal tablolarının denetimi ile bütünleşik bir şekilde sürdürülen bilgi sistemleri denetim sürecinde uygulanmasını istediği standartlar aşağıda yer almaktadır.

IDW PS 261: Bu standart seti, ISA'nın 315, 330 ve 265 sayılı standartlarının birleştirilmesiyle oluşturulmuştur. Buna göre denetçinin, işletmenin ilgili iş süreçleri dâhil finansal raporlamayla ilgili bilgi sistemleri ve bu bilgi sistemlerinden kaynaklanan risklere işletmenin nasıl karşılık verdiği hakkında bilgi edinmesi ve önceki denetimlerden elde edilen denetim kanıtlarının kullanılmasının uygun olup olmadığına karar verirken genel

bilgi sistemleri kontrollerinin halen etkin olup olmadığına bakması gerekmektedir. Söz konusu standartta ayrıca, bilgi sistemleri kullanılarak oluşturulan otomatik kontrollerce önlenemeyen risklerin, yönetimin bilgisi dâhilinde olup olmadığının tespit edilmesi gerektiği, otomatik kontrollerin eksikliği durumunda ise eğer önemli bir kontrol olduğu kanaatine varılırsa işletmenin üst yönetimine bu kontrol eksikliğinin bildirilmesi gerektiği ifade edilmiştir.

IDW PS 330: Bilgi sistemleri ortamında işletmenin finansal tablolarının denetimi üzerinde duran bu standardın, işletmenin bilgi sistemleri genel kontrollerinin değerlendirilmesine ilişkin prosedürleri içerdiği ve bu kapsamda standartta, işletmenin bilgi sistemleri kontrol riskleri, bu kontrollerin test edilmesi, bilgi sistemlerine ilişkin kontrol testlerinin yürütülmesi konularına ağırlık verildiği görülmektedir.

IDW PS 331: Bu standart seti ise, ISA'nın 402 sayılı standardı ile aynı kapsamda olup, bahse konu standartta, işletmenin finansal raporlamaya ilişkin bilgi sistemleri faaliyetleri destek hizmeti kapsamında dışarıdan bir kuruluş tarafından sağlanıyorsa, söz konusu kuruluşun da sağladığı hizmete yönelik kontrollerinin denetim kapsamında değerlendirilmesi gerektiği belirtilmiştir.

4.4. Türkiye'de Bilgi Sistemleri Denetimi

Ülkemizde de 2003 yılında bankacılık sektöründe yaşanan ve çifte kayıt olayı olarak da bilinen "İmar Bankası Skandalı" sonucunda bilgi sistemleri denetimi konusu gündemi meşgul etmiştir. Özbilgin, ülkemizde yaşanan bu skandalın bilgi sistemleri denetimi açısından önemini şu şekilde açıklamaktadır: *"Gerek dünyada 2001 yılında yaşanan "Enron Skandalı" gerekse ülkemizde 2003 yılında Bankacılık Düzenleme ve Denetleme Kurulu tarafından T.İmar Bankası T.A.Ş'e ait bankacılık işlemleri yapma ve mevduat kabul etme izninin kaldırılması ve bu bankanın Tasarruf Mevduatı Sigorta Fonuna intikaline sebep olan "çifte kayıt olayı" bilgi teknolojileri denetim kavramının öneminin her kesim tarafından iyice anlaşılması gerektiğini ortaya koymuştur"* (Özbilgin, 2003: 123).

Yaşanan bu skandaldan sonra ülkemizde bankacılık sektöründe düzenleme ve denetleme yetkisini elinde bulunduran BDDK, bilgi sistemleri denetimine ilişkin temelleri

oluşturduğu 5411 sayılı Bankacılık Kanunu'na ek olarak bazı ikincil düzenlemelerde bulunmuştur. İlk olarak *"Bankaların İç Sistemleri Hakkında Yönetmelik"* ve *"Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"* ile Bankacılık Kanunu'na tabi tüm kuruluşların iç denetim sistemlerinin oluşturulması ve bu sistemlerin periyodik olarak denetiminin sağlanması için düzenleme yapan BDDK, bankaların tedarikçilerden alacakları hizmetler için uymaları gereken kuralları ise *"Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik"* ile düzenlemiştir. BDDK ayrıca 2006 yılında yayımladığı *"Bankalarda Bağımsız Bilgi Sistemleri Denetimi Hakkında Yönetmelik"* ile bilgi sistemleri denetiminde bankalar üzerinde banka iç denetimi, bağımsız dış denetim ve kamu denetimleri olmak üzere üç yapılı bir denetim sistemi oluşmasını sağlamıştır (Varlı, 2007: 33). BDDK, bu yönetmelik ile bankaların bağımsız bilgi sistemleri denetiminde COBIT'in uygulanmasını benimsemiştir.

Ülkemizde özellikle son yıllarda kamu kurumlarının bilgi sistemlerinden ve bu sistemlerin sunduğu imkânlardan yararlanmak amacıyla başta finansal süreçleri olmak üzere tüm iş süreçlerinde giderek daha yaygın bir şekilde bilgi sistemlerini kullanmaları, Sayıştay denetimlerinin bilgi sistemleri alanını da kapsayacak şekilde yeniden yapılandırılmasını sağlamıştır. Bu kapsamda Sayıştay tarafından denetlenen kurumların mali denetiminin etkin bir şekilde yapılmasına katkı sağlamak amacıyla, 2013 yılında Bilgi Sistemleri Denetim Rehberi yayımlanmıştır. Bu rehber ile Sayıştay, kamu kurumlarında yürütmüş olduğu mali denetim sürecine destek vermeyi, bilgi sistemlerinin kontrol zayıflıklarının tespit edilmesini ve kamuoyuna ve parlamentoya bilgi sunulmasını amaçlamaktadır (Sayıştay, 2013: 1).

Söz konusu rehberin hazırlanmasında Bilgi Güvenliği Standartları, INTOSAI – The International Organisation of Supreme Audit Institutions (Uluslararası Sayıştaylar Birliği) rehberleri ve standartları, ISACA standartları ve çerçeveleri ile diğer ülkelerin uygulamalarından yararlanılmıştır. Rehberde, Sayıştay'ın mali denetim için hazırlamış olduğu Mali Denetim Rehberi'nde belirtilen süreçler dikkate alınarak, denetçinin hangi aşamada hangi işleri yapacağını gösteren süreç odaklı bir yaklaşım benimsenmiş olup

genel olarak bilgi sistemleri genel kontrollerinin nasıl değerlendirileceği düzenlenmiştir (Sayıştay, 2013: 2).

Ülkemizde, sermaye piyasaları konusunda düzenleme ve denetleme yetkisi olan Sermaye Piyasası Kurulu (SPK)'nun, 6362 sayılı Sermaye Piyasası Kanunu, *"Faaliyet Esasları"* başlıklı 62'nci maddesinin ikinci fıkrası hükümlerinden, *"Borsa ve piyasa işleticilerinin mali ve bilgi sistemleri denetimi"* başlıklı 72'nci maddesinin üçüncü fıkrası hükümlerinden ve *"Kurulun görev, yetki ve sorumlulukları"* başlıklı 128'inci maddesinin birinci fıkrasının (c) ve (h) bentlerinden, SPK'nın düzenleme ve denetleme kapsamına giren işletmelerde bilgi sistemlerinin işletimi, denetimi ve bu denetimi yapacak kuruluşlara ilişkin usul ve esasların belirlenmesi konularında yetkili olduğu anlaşılmaktadır. Bu kapsamda, yukarıda belirtilen hükümlere dayanılarak hazırlanan *"Bilgi Sistemleri Yönetim İlkeleri Hakkında Tebliğ Taslağı"* ve *"Bilgi Sistemleri Denetim İlkeleri Hakkında Tebliğ Taslağı"*, 15 Kasım 2013 tarihinde kamu görüşüne açılmıştır (Meral, 2016: 91).

5. BİLGİ SİSTEMLERİ DENETİM SÜREÇLERİ

Bilgi sistemleri denetiminde izlenmesi gereken adımlar, denetçinin inceleme olarak bilgi sistemlerini temel alması dışında her finansal denetimde gerçekleştirilenlerle benzerlik göstermektedir.

Denetim fonksiyonu, denetimin bağımsızlığı ve yeterliliğini korurken, denetim ekibi tarafından gerçekleştirilen çeşitli görevlerin denetim hedeflerini yerine getirmesini sağlayacak bir şekilde yönetilmeli ve yönlendirilmelidir (ISACA, 2014: 29).

Bilgi sistemleri denetimi, iç veya dış denetim olarak sağlanabilir. Bilgi sistemleri denetimi iç denetimin içinde bağımsız bir grup tarafından yürütülebildiği gibi finansal ve uygunluk denetimleri ile bütünleşik bir şekilde de yürütülebilir. Bunun yanı sıra, dışarıdan bir firma tarafından sağlanan bilgi sistemleri denetim hizmeti de işletme tarafından uygulanabilir.

Bilgi sistemleri denetiminin önemli bir parçası olan bilgi sistemleri denetçisinin, teknolojinin hızla geliştiği ve değiştiği bir dünyada yeni teknolojilere ve denetim

tekniklerine ayak uydurması ve var olan teknik bilgi ve yeteneklerini sürekli olarak güncellemesi gerekmektedir.

Bilgi sistemleri denetim süreçleri hazırlanırken çeşitli ülkelerin hazırlamış olduğu rehberlerden, ISACA'nın rehberlerinden ve bazı kaynaklardan yararlanılmıştır. Bilgi sistemleri denetim süreçleri denetim hedefine uygun olarak, "Planlama", "Kontrollerin Değerlendirilmesi" ve "Raporlama ve Takip" olarak 3 adımdan oluşur (Sayıştay, 2013: 2).

5.1. Bilgi Sistemleri Denetiminin Planlanması

Bilgi Sistemleri Denetim ve Güvence Standartları, 5 No'lu Standarda göre *"Denetçi, denetiminin hedeflerini karşılayacak bilgi sistemleri denetim kapsamını yürürlükteki kanun ve mesleki denetim standartlarıyla uyumlu olarak planlamalıdır. Bilgi sistemleri denetçisi risk bazlı bir denetim yaklaşımı geliştirmeli ve belgelendirmelidir"* (ISACA, 2010: 13).

ISACA'ya göre, bilgi sistemleri denetiminin etkin bir şekilde gerçekleştirilebilmesi için ilk olarak denetim hedefinin net bir şekilde ortaya konması gerekmektedir. Bilgi sistemleri denetiminin hangi amaçla yapılacağının belirlenmesi ve denetim ekibinin bu denetim hedefi doğrultusunda bilgilendirilmesi ve yönlendirilmesi çok önemlidir. İşletmenin üst yönetiminin, yatırımcılarının, personellerinin ve en önemlisi bağlı bulunduğu ülke otoritelerinin bu denetimle ilgili beklentilerinin denetim ekibi tarafından tam olarak anlaşılması gerekmektedir.

Denetçinin denetimi, ekonomik, verimli, etkin ve zamanında bitirilecek şekilde planlaması gerekmektedir. Denetim kadrosundaki her kademenin çalışması ve denetim aşaması, denetim sırasında doğru bir şekilde denetlenmesi ve denetim personelinin üst düzey bir üyesi tarafından gözden geçirilmesi, bir denetimin en önemli faaliyeti olan planlama açısından oldukça önem arz etmektedir ve denetimin etkinliğini artırmaktadır. Denetimin türü ne olursa olsun, bir denetimin en önemli faaliyeti planlamadır. Planlama aşamasında gösterilen özen ne kadar büyük olursa, denetim o kadar kesin ve etkili olacaktır.

Bir bütünleşik denetimin etkin bir şekilde yürütülebilmesi için, denetimi etkileyen bilgi sistemlerinin anlaşılması çok büyük önem taşımaktadır. Örnek vermek gerekirse, işletmenin finansal denetimlerinde finansal tabloların raporlanmasına etki eden bilgi sistemlerinin doğru bir şekilde çalışıp çalışmadığı, güvenilir veriler üretip üretmediği önemliyken, sistem denetimlerinde işletmenin iş süreçlerinin düzgün bir şekilde işleyebilmesi için kurulan bilgi sistemlerine erişim kontrolleri ve görev paylaşımlarının kontrolü daha fazla önem verilen unsurlar olmaktadır.

Bilgi Sistemleri Denetim ve Güvence Standartları 11 No'lu Standarda göre *"Bilgi sistemleri denetçisi, bilgi sistemleri denetim planının tamamını geliştirmede ve bilgi sistemleri denetim kaynaklarının etkili dağıtımı için önceliklerin belirlenmesinde kullanılabilecek uygun bir risk değerlendirme tekniği veya yaklaşımı kullanmalıdır. Bilgi sistemleri denetçisi, kişisel denetim planlamasında, denetlenen alanla ilgili riskleri tanımlamalı ve değerlendirmelidir"* (ISACA, 2010: 20).

Daha önce ifade edildiği üzere; günümüzde her işletme iş süreçlerini veya finansal raporlama süreçlerini yürütebilmek için birçok bilgi sistemi kullanmaktadır. Bu sistemler, birbirlerinden farklı işlevleri veya etkinlikleri olan uygulamalar barındırabilir ve bu uygulamalar kimi zaman farklı lokasyonlarda yerleşik olabilirler. Denetçi bu durumda, hangi sistemi ne zaman, ne sıklıkla ve nasıl denetleyeceği gibi sorularla karşılaşabilmektedir. Bunun cevabı ise riske dayalı bir yaklaşım benimsemektir.

Denetçinin bir denetim planı hazırlarken benimsediği risk bazlı bir yaklaşım için izleyebileceği adımlar şunlardır (Sayana, 2002: 2):

- İşletmede kullanılan bilgi sistemlerini kayıt altına almak ve kategorilere ayırmak,
- Hangi sistemlerin, para, malzeme, müşteriler, karar verme gibi kritik işlevleri veya varlıkları etkilediğini belirlemek,
- Bu sistemleri hangi risklerin etkilediğini ve iş üzerindeki ağırlığını değerlendirmek,
- Sistemleri yukarıdaki değerlendirmeye dayalı olarak sıralamak ve denetim önceliği, kaynaklar, zaman çizelgesi ve sıklığa karar vermek.

Yukarıda sayılı adımları uygulayan denetçi daha sonra, oluşturmuş olduğu bu çizelgeye göre yıl boyunca yapılacak denetimlerin yanı sıra gerekli kaynakları listeleyen bir yıllık denetim planı hazırlayabilir.

Risk bazlı bir denetim yaklaşımı, genellikle, sürekli denetim sürecini geliştirmek ve iyileştirmek için uyarlanmıştır. Bu yaklaşım, riskin değerlendirilmesi ve bir bilgi sistemleri denetçisinin uygunluk testi veya maddi doğruluk testleri yapıp yapmamasına karar vermesinde yardımcı olması için kullanılır (ISACA, 2014: 49).

Denetçi tarafından bilgi sistemleri denetimine ilişkin risk analizi yapılmadığında, bilgi sistemleri denetçisi muhtemelen içgüdüsel bir yol izleyip risklerin daha yüksek olduğunu düşündüğü alanlarda ilave incelemeler yapabilir veya düşük riskli alanlara ve yüksek risk alanlara eşit kaynaklar ayırarak, denetimin tüm alanlarına eşit ağırlık verebilir (Gregory, 2010: 15).

Bilgi sistemlerinin işletme içerisindeki önemi, işletmenin iş süreçlerini ne derecede etkilediği, bilgi sistemlerinin yapısı ve karmaşıklığı, işletmenin stratejisi, paydaşların beklentisi ve diğer dış etkenleri de dikkate alan risk değerlendirmesi, bilgi sistemleri denetim planlamasının en önemli adımlarından biridir.

Hazırlanan risk değerlendirmesi hangi sistemlerin bilgi sistemleri denetimi kapsamına alınacağını belirlerken denetçiye yol göstermektedir. İşletmenin bilgi sistemlerine ilişkin risk değerlendirmesini gerçekleştiren denetçinin, bilgi sistemleri denetiminin kapsamını denetim türüne göre belirlemesi gerekmektedir.

Bilgi sistemleri denetçisinin seçebileceği birçok risk değerlendirme metodolojisi vardır. Riskleri azaltmak için uygulanan politikalar, prosedürler, uygulamalar ve organizasyonel yapılar, iç kontroller olarak adlandırılır. Kontrollerin değerlendirilmesi sırasında göz önüne alınması gereken kontrol elemanları, Önleyici, Tespit edici ve Doğrulayıcı kontroller olarak sınıflandırılabilir.

Denetçi, kontrolleri geçici olarak değerlendirmeli ve bu değerlendirme temelinde denetim planını geliştirmelidir. Denetçinin, bilgisayar temelli kontrollerin ön değerlendirmesi de dâhil olmak üzere, doğal ve kontrol risklerinin değerlendirilmesine dayanarak, denetim sırasında etkili olabilecek genel kontrol tekniklerini tanımlaması

gerekir. Ayrıntılı denetimin başlatılması için denetim amaçlarını net bir şekilde ortaya koymak zorunlu olmasına rağmen, denetim sırasında bu hedeflerin değişikliğe uğrayabileceğini veya daha ayrıntılı açıklamalar yapılabileceğini anlamamız gerekir.

Planlama, denetçinin denetlenen kuruluşun bilişim sistemlerine ilişkin kontrolleri değerlendirmek için maddi kanıt toplamanın etkin ve verimli metotlarını belirlemesine yardımcı olur.

5.2. Bilgi Sistemleri Denetim Çalışmalarının Değerlendirmesi

Bilgi sistemleri denetimlerinde, kontrollerin tasarım ve işletim etkinliklerinin iç içe geçmiş olmasından dolayı direkt olarak bu kontrollere ilişkin politika veya prosedür gibi dokümanların incelenmesi yeterli olmayabilir. Böyle bir durumda denetçinin, sistemi bizzat yerinde inceleyip söz konusu sistem veya kontrollerin kullanıcısı olan bilgi işlem personeliyle iletişim halinde olması gerekmektedir (İDKK, 2014: 50).

Bilgi Sistemleri Denetim ve Güvence Standartları 6 No'lu Standarda göre *"Bilgi sistemleri denetim kadrosu, denetim hedeflerinin başarıldığının ve yürürlükteki mesleki denetim standartlarının karşılandığının makul güvencesini sağlamak amacıyla denetim işinin yürütülmesi esnasında gözden geçirilmelidir. Denetim süreci boyunca bilgi sistemleri denetçisi, denetim hedeflerini başarmak için gereken yeterli, güvenilir ve ilişkili bulgu sağlamalıdır. Denetim bulguları ve çıkarılan sonuçlar, bu kanıtların uygun analizi ve yorumuyla desteklenmelidir. Denetim süreci, yapılan denetimi ve bilgi sistemleri denetçisinin bulgu ve sonuçlarını destekleyen denetim kanıtını gösterir bir biçimde dosyalanmak zorundadır."* (ISACA, 2010: 14)

Bilgi sistemleri denetimi planlaması tamamlandıktan sonra, işletmenin incelenecek bilgi sistemlerine özgü kontrollerin değerlendirilmesi gerekmektedir. Denetçinin denetim programı kapsamında inceleyeceği bilgi sistemleri kontrollerini, kontrol varlığının belirlenmesi, kontrolün etkinliğinin değerlendirilmesi ve bulguların değerlendirilmesi olarak 3 aşamada incelemesi gerekmektedir.

Denetçi, bilgi sistemleri kontrollerini incelerken ilk olarak kontrol alanları itibarıyla olması gereken kontrollerin olup olmadığı konusunda araştırma yapmalıdır. Bu araştırmanın yapılabilmesi için işletme tarafından denetçiye sunulan kontrol setleri baz

alınarak işletmede yetkili kişilerle toplantı yapılması gerekir. Bu toplantılarda kontrollerin varlığına ilişkin işletmenin cevapları belgelendirilmelidir. Bunun sonucunda alınan cevaplar ve belgeler ışığında ilgili kontrollerin varlığı ve bu kontrollere ilişkin risklerin önlenmesine yönelik ekstra kontrollerin varlığı belirlenmelidir.

Bilgi sistemlerine yönelik olması gereken kontrolün var olup olmadığı belirlendikten sonra, bu kontrolün etkinliğinin değerlendirilmesi gerekir. Denetçinin, kontrollerin etkin bir şekilde çalışıp çalışmadığını değerlendirdikten sonra, eğer tespit edilen bir kontrol eksikliği varsa, bunu kanıtlarıyla birlikte belgelendirmesi gerekir. Eğer ilgili kontrollerin eksikliğinin değerlendirilmesinde teknik bir desteğe ihtiyaç duyulursa, bu konuda tecrübeli bir uzmandan destek alınabilir.

Yapılan incelemeler sonucunda denetçi tarafından elde edilen bulgular, denetim sonucunu etkileyecek kadar yeterli kanıt toplanıp toplanmadığı açısından değerlendirilerek ek incelemeye ihtiyaç olup olmadığı belirlenmelidir. Böyle bir ihtiyacın varlığı durumunda denetçi inceleme sürecini tamamlamadan ek incelemelerde bulunmalıdır.

Denetçinin bu sistemler üzerinde tespit ettiği kontrol eksikliği veya bu kontrollerin etkin çalışamaması neticesinde gördüğü kontrol zayıflığı bulgu olarak ifade edilir ve her bir bulgu işletmenin bilgi sistemlerine ilişkin riskler barındırır. Sistemde karşılaşılan her kontrole yönelik bulguların risk seviyelerinin belirlenmesi gerekir. Bu, bulgular arasında derecelendirme yaparak bulguların denetçi tarafından genel bir değerlendirme yapılmasına imkân sağlar. Bulguların risk değerlendirmesi, tespit edilen bulgunun ortaya çıkardığı riskin etki düzeyi ile risk gerçekleşme olasılığı birlikte değerlendirilerek yapılmaktadır.

Sistem kontrollerinin değerlendirilmesi, kontrol alanları itibarıyla yapılmaktadır. Kontrol alanları, genel ve uygulama kontrolleri olmak üzere iki ana başlık altında gruplandırılır.

A. Genel Kontroller

Genel kontroller, işletmenin tüm bilgi sistemleri altyapısı ve destek hizmetleri dâhil olmak üzere faaliyetlerinin sürekliliğinin sağlanmasına yönelik politika, prosedür ve uygulamalara yönelik kontrollerdir. Genel kontroller şunları içerir:

- 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).

Yönetim kontrolleri; güvenli ve yeterli bir bilgi sistemleri ortamının sağlanması için uygun politika, prosedür ve uygulamalar oluşturarak işletmenin bilgi sistemlerinin işletme amaçlarına uygun çalışmasını ve işlevlerini doğru bir şekilde yerine getirmesini sağlayacak tedbirleri almakla sorumlu olan işletme yönetimi tarafından oluşturulan bu kontroller, denetçiye alt düzeydeki ayrıntılı kontrollerin varlığı ve etkinliği konusunda 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).

Denetçi ise yönetim kontrolü olarak ifade edilen bu kontrolün varlığını ve etkinliğini sorgulamalıdır. Örneğin; işletmenin organizasyon alanındaki yönetim kontrolüne ilişkin değerlendirmesini yaparken denetçi, işletmenin bilgi sistemlerinin etkin bir şekilde yönetilmesini sağlayacak bir bilgi işlem biriminin olup olmadığını, bu birimin bilgi güvenliğini sağlayacak şekilde bilinçlendirilip bilinçlendirilmediğini değerlendirmelidir. Bir başka örnek vermek gerekirse, denetçi tarafından bilgi sistemlerinin kanun ve düzenlemelere uygun şekilde işletilip işletilmediğinin değerlendirildiği bir işletmede, bu kanun veya düzenlemelere uyulmadığı takdirde meydana gelecek risklerin önlenmesine yönelik olarak denetçinin, bilgi sistemlerinin kurulması, yönetilmesi ve kullanılması ile ilgili var olan mevzuata ilişkin

belgelendirmenin yapılıp yapılmadığını, bilgi sistemlerini ilgilendiren konularda (fikri mülkiyet hakları, kayıtların saklanması, kişisel bilgilerin gizliliği vb.) bağlı olduğu idari otorite tarafından konulan yasal düzenlemelerin gereklerini yerine getirecek prosedürlerin hazırlanıp hazırlanmadığını sorgulaması gerekir.

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, elektrik, voltaj dalgalanmaları veya güç yetersizlikleri gibi çevresel tehlikelere karşı ise, bunlara ilişkin uygun önlemler alınarak korunmalıdır (Sayıştay, 2013: 28).

Denetçi tarafından bu kontrollerin varlığının ve etkinliğinin sorgulanması gerekir. Şöyle ki; işletmenin bilgi sistemlerinin bulunduğu bina ve odalarda yangına karşı herhangi bir önlem alınıp alınmadığı ve yangın esnasında bu sistemleri kurtarmaya yönelik belirlenmiş bir prosedürün olup olmadığının sorgulanması, denetçinin denetlediği işletmenin fiziksel ve çevresel kontrollerine ilişkin bir hususun değerlendirmesini yapmış olacağı anlamına gelmektedir.

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 (Sayıştay, 2013: 36).

İşletmenin ağ yapılarına ilişkin güvenliği göz ardı etmesi sonucunda meydana gelebilecek veri kaybı, çalınması, bozulması veya değişikliğe uğraması veya ağ üzerindeki gizli bilgilerin yetkisiz kişiler tarafından ele geçirilmesi gibi risklerin önlenmesi amacıyla işletmenin ağ hizmetlerini sağlayan cihaz ve yazılımlarının yönetimine ilişkin politika ve prosedürlerin olup olmadığını sorgulayan denetçi, ağ yönetimi ve güvenliğine ilişkin kontrollerden birinin değerlendirmesini yapmış olacaktır. Ancak bu değerlendirme tek başına yeterli değildir.

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 sistemin korunmasıdır. Mantıksal erişim kontrolleri, hem sistem hem de uygulama düzeyinde ortaya çıkabilir. Bilgi sistemleri 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).

Denetçi, işletmenin yetkili ve güvenli erişimi içeren bir mantıksal erişim kontrollerinin varlığını ve etkinliğini değerlendirmek zorundadır. Örneğin, işletmenin yazılı bir şifre oluşturma ve değiştirme politikasının varlığını, sistem kullanıcılarının yetki ve sorumluluklarına bağlı olarak erişim haklarına yönelik kuralların varlığını veya kullanıcıların sistem erişimlerine ilişkin günlük kayıtları (log) tutulup tutulmadığını sorgulayan denetçi, bu kontrolün varlığına ve etkinliğine ilişkin değerlendirmelerde bulunmuş olacaktır. Ancak bu değerlendirmeler tek başlarına yeterli olmayacaktır.

İşletim kontrolleri; İşletim kontrollerinin amacı bilgi sistemlerinin kendinden beklenen faaliyetlerin sürekliliğini ve güvenliğini sağlayacak şekilde işletilmesidir (Sayıştay, 2013: 74). İşletmenin ana faaliyetleri için kullandığı işletim sistemlerinin gerektiği gibi çalışmasını ve bu sistemler üzerinde çalışan uygulamaların ve işlemlerin sorunsuz ve eksiksiz bir şekilde yürütülmesini sağlamak amacını taşıyan bu kontrollerin yeterli seviyede kurulamaması veya yanlış kurulması; işlemlerin zorlaşması, yetkisiz erişimler, sistem çökmesi ve kaynak yetersizlikleri gibi risklerin meydana gelmesine sebep olabilir.

Denetçi ise işletmenin faaliyetlerinde kullandığı işletim sistemlerinin düzenli bakımına ve kontrolüne ilişkin prosedürlerin olup olmadığını sorgulayarak kontrolün varlığını ve etkinliğinin bir kısmını inceleyebilir.

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).

Denetçi tarafından işletmenin bilgi sistemlerine yönelik değişikliklerine veya yeni sistem geliştirme projelerine yönelik politikalarının, hazırlanan projeyi yönetecek ekibin yeterli nitelik ve deneyime sahip olup olmadığının, projenin işletme hedeflerine uygun olup olmadığının, projenin gerçekleşebilirliğine yönelik önceden hazırlanmış teknik, mali ve sosyal analizlerin yapılıp yapılmadığının sorgulanması gerekir. Söz konusu sorgulamalar denetçinin bu kontrole yönelik olarak değerlendirmesini yaparken yardımcı olacaktır.

Acil durum ve iş sürekliliği planlaması kontrolleri; Bu kontrollerin amacı acil durum nedeniyle bilgi 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 (Sayıştay, 2013: 99).

İşletme, bir felaketle karşı karşıya kaldığında herhangi bir acil durum ve iş sürekliliği planını devreye sokamadığı takdirde, yasal sorumluluklarını veya üçüncü kişilere karşı olan sorumluluklarını yerine getirememe, ana faaliyetlerine makul bir süre içerisinde geri dönememe, felaketin sebep olduğu kayıplarda artış gibi risklere maruz kalabilir. İşletme, bu riskleri en aza indirebilmek için iç veya dış faktörler sebebiyle meydana gelme ihtimali olan acil ve beklenmedik durumlara karşı hazırlıklı olmalı ve acil durum ve iş sürekliliği planına sahip olmalıdır. Ayrıca, işletmenin ana faaliyetlerini kesintiye uğratacak çevresel faktörleri belirlemek için risk değerlendirmesi yapmalı, bu riskleri en aza indirmek için uygun maliyetle gerekli tedbirler alınmalıdır.

Denetçi ise, işletmenin acil durum ve iş sürekliliği planının varlığını, acil ve beklenmedik durumlara ilişkin işletmenin risk analizlerini inceleyerek bu kontrollere ilişkin değerlendirmelerini yapmış olacaktır.

B. Uygulama Kontrolleri

"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: 107).

Uygulama kontrolleri denetçi tarafından değerlendirilirken, uygulamaların güvenilirliğine ilişkin makul bir güvence elde edebilmek amacıyla uygulamalarda olması gereken kontroller test edilerek kanıt toplanır. Bu aşamada bilgisayar destekli denetim tekniklerinden (BDDT) de yararlanılır.

Uygulama kontrolleri aşağıdaki başlıklar altında incelenebilir:

- Girdi Kontrolleri
- Veri Transfer Kontrolleri
- İşlem Kontrolleri
- Çıktı Kontrolleri

Girdi kontrolleri; Bu kontrollerin hedefi verilerin inceleme konusu bilgi sistemlerine tam, doğru ve yetkili bir kişi tarafından girilip girilmediğinin sağlamasını yapmaktır. Bu kapsamda, yetkisiz kişilerce veri girişini engellemek, hatalı veya eksik veri girişlerini önlemek veya mükerrer kayıtların önüne geçmek amacıyla, denetim sırasında incelenen bilgi sistemlerinde çalışan uygulama programlarına ilişkin teknik dokümanlar veya kullanım rehberleri hazırlanmalı, hatalı veri girişlerini engelleyecek otomatik kontrol mekanizmaları uygulamanın arka planında yürütülmeli ve hatalı veya yetkisiz veri girişleri raporlanmalıdır. Denetçi ise, bu kontrollere ilişkin denetimini yaparken, söz konusu uygulama programlarına ilişkin teknik dokümanların ve kullanıcı rehberlerinin varlığını ve hatalı veya yetkisiz veri girişlerinin raporlanıp raporlanmadığını sorgulamalıdır.

Veri transfer kontrolleri; Bu kontrollerin amacı bilgi sistemleri arasında bir uçtan başka bir uca transferi gerçekleştirilen verilerin tam, doğru ve zamanında yapıldığının sağlamasını yapmaktır. Transfer edilen verilerin transfer esnasında

bozulması, kaybolması, çalınması veya değiştirilmesi mümkün olabilir. Bunun yanı sıra verinin ulaşması gereken yere ulaşamaması veya birkaç kez gönderilmesi gibi sorunlar da meydana gelebilir. Bu gibi risklerin önüne geçebilmek amacıyla sistemler arasında yapılan veri transferlerinin tam ve doğru olarak yapılmasını sağlayan manuel veya otomatik kontroller oluşturulabilir. Bu süreçteki en önemli husus ise, veri transferinden sorumlu personele rehberlik edecek politika ve prosedür setlerinin tanımlanmış olmasıdır.

İşlem kontrolleri; Bu kontrollerin amacı, uygulama içerisinde kullanılan verinin tam, doğru ve işletmenin iş süreçlerine uygun olarak işleme tabi tutulmasını ve denetlenebilir olmasını sağlamaktır. İşletmenin iş süreçlerinin uygulama kontrolleri üzerinden yanlış bir şekilde işletilmesi, sistematik hataların oluşması, yanlış verilerin işleme tabi tutulması, denetim izinin kaybolması veya işlemlerin doğrulanamaması gibi riskler meydana gelebilir. Bu riskler kapsamında işletmenin yönetimi tarafından, söz konusu işlemlerin doğru ve zamanında işletildiğinin sağlamasını gerçekleştiren yeterli seviyede otomatik ve manuel kontrollerin kurulması gerekir. Ayrıca, süreçte yaşanan başarısızlık veya problemler karşısında, işlemi yapanın, onaylanan veya doğrulanan en son noktadan işleme devam edebilmesi gerekmektedir.

Çıktı kontrolleri; Bu kontrolün amacı, çıktıların tam, doğru ve zamanında üretilmesini, doğru yere/kişilere dağıtılmasını, gizliliklerinin korunmasını, tespit edilen hataların detaylı olarak incelenmesini ve gereğinin yapılmasını sağlamaktır. Bu kontrollerin yetersizliği nedeniyle, çıktıların tam ve doğru olmaması, yetkisiz kişilerin eline geçmesi, elde edilen çıktıların muhafaza edilememesi gibi riskler meydana gelebilir. Bu risklerin azaltılması amacıyla işletmenin çıktıların elde edilmesine ve muhafaza edilmesine ilişkin yazılı bir prosedürünün olması, çıktılarda meydana gelen hatalara ilişkin gözden geçirme ve doğrulama işlemlerinin yetkili personelce yapılması gerekmektedir.

5.3. Bilgi Sistemleri Denetim Sonuçlarının Raporlanması ve İzlenmesi

Bilgi Sistemleri Denetim ve Güvence Standartları 7 No'lu Standarda göre *"Bilgi sistemleri 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. Bilgi sistemleri denetçisinin denetimle ilgili olarak bulgularını, sonuçlarını ve önerilerini, sahip olduğu çekincelerini, niteliklerini veya sınırlandırmalarını belirtmelidir. Bilgi sistemleri denetçisi, raporlanan sonuçları destekleyecek uygun ve yeterli denetim kanıtlarına sahip olmalıdır. Bilgi sistemleri denetçisi, raporunu bitirdiği zaman raporunu imzalamalı, tarih atmalı ve denetim yönetmeliği veya hizmet sözleşmesine göre sunmalıdır" (ISACA, 2014: 15). Detaylı ana rapor ise aşağıda belirtilen bölümler itibarıyla oluşturulur:

Rapor özeti: Özet, detaylı denetim raporundan önce yer alan ve denetçinin temel bulgularına dair görüş ve önerilerine yer verilen kısımdır. Rapor özeti, raporu detaylı bir şekilde okuması mümkün olmayan ilgililerce raporda yer alan temel bulguların hızlıca anlaşılmasını sağlar.

Giriş bölümü: Raporun ana bölümünün girişinde bulunan bu bölüm, denetlenen işletme, inceleme yapan denetçiler, denetimin kapsamı ve denetimin nasıl yapıldığı konusunda bilgiler içeren bölümdür.

Ana rapor gövdesi bölümü: Raporun ana gövdesi, detaylı denetim bulgularını içermelidir. Raporun bu bölümünde yer verilen tespitler mantıklı ve tutarlı bir yapıda ve sistematik bir şekilde ele alınmalıdır. Denetim hedeflerine uygun bir şekilde konularına göre bölümleme yapılmalı ve kontrol yetersizlikleri ve kontrol etkinliğine ilişkin denetçi bulguları her bir konu için ayrı ayrı belirtilmelidir.

Öneriler bölümü: Bu bölümde, tespit edilen kontrol eksikliklerinden doğan riskleri düşürecek önerilerde bulunulmalıdır. Denetçi, ileri sürdüğü önerilerin mantıklı, uygulanabilir ve işletmenin yapısına uygun olmasına dikkat etmelidir.

İşletmenin denetim bulgularına ilişkin yorumları: Bu bölümde, denetçi tarafından bilgi sistemleri denetimi gerçekleştirilen işletmenin, denetçinin denetim bulgularına yönelik cevaplarına ve varsa bunlara ilişkin belgelerine yer verilmelidir.

Bilgi Sistemleri Denetim ve Güvence Standartları 8 No'lu Standarda göre *"Bulguların ve önerilerin raporlanmasından sonra, bilgi sistemleri denetçisi yönetim*

tarafından zamanında ve uygun bir şekilde harekete geçilip geçilmediğini belirlemek için ilgili bilgileri istemeli ve değerlendirmelidir" (ISACA, 2010: 16).

"Eğer işletme yönetimi, rapordaki uygulama önerilerine dair eylem planını bilgi sistemleri 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, bilgi sistemleri 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 bilgi sistemleri 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 bilgi sistemleri denetçileri, kendilerinin üzerinde anlaştıkları önerileri izlemek için bir iç bilgi sistemleri denetim birimine güvenebilirler. Önerileri uygulamak için yapılan etkinliklerle ilgili olarak yönetimin bilgi sağladığı ve bilgi sistemleri 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 bilgi sistemleri denetçisi eğer uygulanmadıysa bulguların hala geçerli olup olmadığını değerlendirmek durumundadır" (Yurdagül, 2010: 16).

6. DEĞERLENDİRME VE ÖNERİLER

ABD ve dünyada yaşanan büyük çaplı finansal skandallardan sonra 2002 yılında yürürlüğe giren Sarbanes-Oxley Kanunu, halka açık şirketler ve mali tablolar denetimine tabi tüm kuruluşlar için finansal raporlamayı etkileyen kontrol ve bilgi sistemleri

kontrollerinin denetimini zorunlu kılmaktadır. Ülkemizde ise ilk olarak BDDK tarafından bankalara yönelik bilgi sistemleri denetimine ilişkin mevzuat yayımlanmış ve daha sonra Sayıştay tarafından kamu kurumlarında finansal denetimin yanı sıra bilgi sistemleri denetimine de başlanmıştır. Sermaye Piyasası Kurulu ise, *"Bilgi Sistemleri Yönetim İlkeleri Hakkında Tebliğ Taslağı"* ve *"Bilgi Sistemleri Bağımsız Denetim İlkeleri Hakkında Tebliğ Taslağı"*nı, 15 Kasım 2013 tarihinde kamu görüşüne açmıştır.

Bilgi sistemleri kullanımının özellikle finans sektöründe yaygınlık kazanması ve hatta bir zorunluluk haline gelmesi ile finans kuruluşlarında yalnızca finansal denetimin değil, bilgi sistemleri denetiminin de gerekli olduğu fikri her kesim tarafından kabul görmüştür. Kabul edilmelidir ki, finansal denetçinin mali tablolar üzerinde gerçekleştirdiği denetimin kalitesi, işletmenin kullanmış olduğu muhasebe bilgi sistemleri hakkındaki uzmanlığına ve bilgi sistemleri denetçisinin bu sistemler üzerindeki değerlendirmelerini dikkate almasına bağlıdır. İşletmenin mali tabloları ve diğer finansal veriler günümüzde çoğunlukla otomatize edilmiş bilgisayar sistemlerinin birer çıktısı olduklarından, finansal denetimlerde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeleyecektir.

"Finansal bilgiler, kuruluşun sahip olduğu sistemler üzerinde ve bu sistemlerde yer alan raporlar temel alınarak hazırlanır. Finansal denetimin üzerinde çalıştığı bu veriler bilgi sistemleri tarafından üretilir. Bu nedenle bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği finansal denetim çalışmasının doğruluğuna ve anlamlılığına doğrudan etki eder. Bilgi sistemlerinin doğru çalışıp çalışmadığı ise bilgi sistemleri denetimi ile belirlenir. Bu nedenle finansal denetim ve bilgi sistemleri denetimi yakından ilişkilidir" (Cantürk, 2016: 49).

İşletmelerin finansal raporlamalarında ve muhasebe verilerinde bilgi sistemlerini kullanmaları, pek çok hata ve hilenin bu sistemler içinde gizli kalmasına sebep olmaktadır. Finansal denetçiler tarafından sadece bu sistemlerden elde edilen çıktılar ile girdileri karşılaştırmak, bu sistemlerin içinde gizlenmiş hile veya hatalara ulaşılmasını engellemektedir. Bu nedenle finansal denetimi gerçekleştiren bağımsız denetim ekibi,

denetlediği finansal bilgiyi üreten ve işleyen bilgi sistemlerinin denetimini de yürütmüş olduğu bağımsız denetimin bir parçası olarak görmelidir.

"Finansal tabloların finansal raporlama standartları ve/veya genel kabul görmüş muhasebe ilkelerine uygunluğunu denetleyen ve işletmede depolanan finansal ve finansal olmayan verilerin doğruluğu ve güvenilirliğine ilişkin makul güvence veren bağımsız denetimin bilgi teknolojilerinden yararlanması gerekir. Bağımsız denetçiler, denetim riskini belirleme aşamasında işletmenin iç kontrol yapısını da değerlendirmekte ve kontrol riskini ortaya çıkarmaktadırlar. Bir başka ifade ile bağımsız denetçiler; işletmenin kurmuş olduğu bilgi teknolojilerinde yer alan iç kontrol prosedürlerinin olası hata ve hileleri ortaya çıkarmaya yetecek düzeyde olup olmadığını belirlemektedirler. Bu bakımdan, bağımsız denetimin işleyişinde bilgi teknolojilerinin incelenmesi ve denetlenmesi önemli bir yer tutmaktadır." (Yalkın, 2011: 112)

İşletmenin tüm alanlarına etki eden teknolojik gelişmeler ve yenilikler, muhasebe sistemlerinin yapısını da farklılaştırmaktadır. Sistemlerin elektronik hale gelmesine bağlı olarak bağımsız denetim içinde bilgi sistemleri denetiminin önemi her geçen gün artmaktadır. Bilgi sistemlerinin bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekmektedir. Denetçi sistem çıktılarına ek olarak bilgi sistemlerinin içyapısında bulunan önemli hata ve yanlışlıkları ortaya çıkarmalıdır ve tespit edilen hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır. Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.

Sonuç olarak, finansal denetimlerde, işletme tarafından denetçiye sunulan finansal bilgiler kadar bu bilgilere nasıl ulaşıldığı da denetimin bir parçasını oluşturmaktadır. İşletmelerin finansal tablolarının doğruluğu ve güvenilirliği konusunda yatırımcılara makul güvence vermeyi amaçlayan finansal denetimlerin günümüz şartlarında yetersiz kaldığı; sadece işletmeler tarafından sunulan girdi ve çıktıların kontrol edilmesiyle yapılan finansal denetimlerin, bu girdi ve çıktıların gizliliği, bütünlüğü ve güvenilirliği konusunda güvence vermeyi amaçlayan bilgi sistemleri denetimi ile bütünleşik bir şekilde

yapılmadığı sürece tam anlamıyla bir güvence sağlayamadığı kabul görmüş bir gerçektir. İşletmelerin mali tablolarının doğru bir şekilde yansıtılması için;

- Bilgi sistemleri denetimi mali tablo denetimleri ile uyum içerisinde yürütülen bir bağımsız denetim faaliyeti olarak gerçekleştirilmelidir.
- Bilgi sistemleri genel kontrolleri önemlilik kriterleri esas alınarak uyumluluk, etkinlik ve yeterlilik açısından incelenmelidir. Böylece denetim sırasında üzerinde detaylı çalışma gerektiren alanlar belirlenebilir.
- Sistemler açısından veri giriş kontrolleri, veri işleme kontrolleri ve yetki kontrolleri detaylı olarak incelenmelidir.
- Finansal tablolara kaynak olan verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.
- Denetçi bilgi sistemleri üzerindeki incelemelerini tamamladıktan sonra, finansal raporların doğruluğuna yönelik karşılıklı kontroller yapmalıdır. Bilgi sistemlerinden üretilen verilerin finansal raporlara kaynak oluşturmasını teminen doğruluk, erişilebilirlik ve bütünlük olarak kontrol edilmelidir. Bu noktada verilerin sistemlerden oluşturulup raporlama sonucuna kadar ki süreç içinde bozulmaya uğramadan finansal tablolara yansıtılıp yansıtılmadığı incelenmelidir.
- SPK'nın bağımsız denetim ile ilgili mevzuatları aracılığıyla, bilgi sistemleri denetimi ve finansal denetim uyumlu hale getirilmeli ve bu uyumun sağlanmasında yol gösterici olmak amacıyla bu iki denetimin nasıl birlikte yürütüleceğine ilişkin ayrıntılı bir rehber hazırlanmalıdır.
- Rehberin hazırlanmasında bilgi sistemleri denetimine ilişkin uluslararası düzeyde kabul görmüş standartlara referans verilerek, denetimlere ilişkin objektif ve kabul edilebilirliği yüksek bulgu ve öneriler içeren raporlar ortaya koyulmalıdır.

KAYNAKÇA

BÖCEK, Bilal

2014 “Bilgi Teknolojileri Denetiminin İçeriği ve Mali Denetimde Karşıladığı Riskler” T. C. Gazi Üniversitesi İşletme Anabilim Dalı Yüksek Lisans Tezi.

CANTÜRK, Sinem

2016 “Günümüzün Görünmez Kahramanı Bilgi Sistemleri Denetimi” Denetimin Değeri, KPMG Türkiye

DİNÇ, Yusuf ve CENGİZ, Selim

2014 “Muhasebe Denetiminde Hata ve Hilenin Denetçi Etiği Açısından İncelenmesi: Enron Skandalı Örneği” T. C. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.

GÖKALP, Füsun

2005 “Genel Hatları İle Sarbanes Oxley Kanunu ve Türkiye'deki Şirketlere Etkisi”

GREGORY, Peter H.

2010 “The Audit Process” Certified Information Systems Auditor All In One Exam Guide

HAKLI, Tuğba

2012 “Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi” T.C. Süleyman Demirel Üniversitesi Fen Bilimleri Üniversitesi Yüksek Lisans Tezi

ICAI

“Information Systems Auditing Standards, Guidelines, Best Practices” Erişim: 09.07.2017 http://www.icaiknowledgegateway.org/littledms/folder1/chapter-8-information-systems-auditing-standards-guidelines-best-practices-pm.pdf

ISA - International Standards of Auditing

2014 “Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements” IAASB

ISACA

2010 “Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araç ve Teknikleri” ISACA

2012 “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT” ISACA.

2014 “CISA Review Manual 2014” ISACA.

ITAF

2014 “ITAF: A Professional Practices Framework for IS Audit/Assurance”, 3rd Edition

ITGI

2008 “Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit” A Management Briefing From ITGI and OGC

İDKK

2014 “Kamu Bilgi Teknolojileri Denetimi Rehberi” T.C. Maliye Bakanlığı İç Denetim Koordinasyon Kurulu

KARAKAYA, Gencay

2016 “Çalışan Hileleri ve İç Kontrol İlişkisi” Vergi Sorunları Dergisi Sayı: 330

MCNALLY, J. Stephen

2013 “The 2013 COSO Framework & SOX Compliance”

MERAL, Erkan

2016 “Türkiye’de Bilgi Sistemleri Denetimi Ve Kamu Gözetimi Kurumu’nun Bilgi Sistemleri Denetiminde Üstlendiği Misyon” Muhasebe ve Denetim Dünyası, Yıl:1 S:1

MOELLER, Robert R.

2014 “Executive’s Guide to COSO Internal Controls-Understanding and Implementing the New Framework” John Wiley & Sons Inc.

ÖZBİLGİN, İzzet Gökhan

2003 “Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar” Sayıştay Dergisi.

SAYIŞTAY

2013 “Bilişim Sistemleri Denetim Rehberi” T.C. Sayıştay Başkanlığı

SAYANA, S. Anantha

2002 “The IS Audit Process” Information Systems Control Journal, Volume 1

TS ISO/IEC 27001

2013 “TS ISO/IEC 27001” ISO/IEC

VAN SLYKE, Craig

2008, “Information Communication Technologies: Concepts, Methodologies, Tools, and Applications”

VARLI, Ahmet Türkay

2007 “Bankacılıkta Bilgi Sistemleri Yönetimi ve Denetimi/Mevzuat Çerçevesinde BDDK Perspektifi Sunumu” Türkiye İç Denetim Enstitüsü 11. İç Denetim Kongresi

VURAL, Yılmaz ve SAĞIROĞLU, Şeref

2008 “Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme” T. C. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi.

WEBER, Ron

1999 “Information Systems Control and Audit”, Prentice Hall.

YALKIN (DEMİR), Lütfiye Defne

2011 “Bilgi Teknolojileri Denetimi Kavramsal Çerçeve, Aşamaları, Sınırları, Sorunları” T. C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Doktora Tezi.

YURDAGÜL, Ömer

2010 “Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araçları ve Teknikleri” ISACA

Yararlanılan İnternet Siteleri

www.rab-asr.ch

www.idw.de

www.isaca.org

www.ifac.org

www.vikipedia.org