IJAFR

INTERNATIONAL JOURNAL OF ACCOUNTING AND FINANCE RESEARCHES
ULUSLARARASI MUHASEBE VE FİNANS ARAŞTIRMALARI DERGİSİ

Cilt:1 Sayı:2 – Kasım 2019

BİLİŞİM TEKNOLOJİLERİ (BT) DENETİMİNDE BİLGİ GÜVENLİĞİ İLE İLGİLİ ULUSLARARASI STANDARTLAR VE TÜRKİYE'DEKİ UYUM ÇABALARININ İNCELENMESİ*

Doç. Dr. Selahattin KOÇ**
Öğr. Gör. Sevgi ŞEKER***
Öğr. Gör. Fatma ŞEKER****

Teorik İnceleme
(Theoretical Research)

Muhasebe ve Finans
Araştırmaları Dergisi
Kasım 2019; 1 (2): 121-139

ÖZ

İçinde bulunduğumuz çağda, Bilişim Teknolojilerinde (BT) yaşanan akıl almaz gelişmeler, başta bilgisayarlar olmak üzere birçok bilişim teknolojisi aracının işletme faaliyetlerinde kullanılmasına neden olmuştur. Dahası bilişim teknolojilerinin kullanımı, yoğun küresel rekabet ortamında işletmelerin hayatta kalabilmesi için bir tercih değil zorunluluk haline gelmiştir. Muhasebe ve denetim faaliyetleri de bilişim teknolojilerindeki gelişmelerden etkilenmiş, kağıtsız muhasebe ve kağıtsız denetim olarak nitelendirilen yeni bir dönem başlamıştır. Artık muhasebe bilgileri bilişim teknolojileri araçları ile üretilmekte, saklanmakta ve aynı araçlar ile ilgili kişilere raporlanmaktadır. Bilgisayar ortamında üretilen bilgiler de yine bilgisayarlar vasıtasıyla denetim yazılımları kullanılarak denetlenmektedir.

Bu aşamada muhasebe denetiminde önemi her geçen gün artan ve en kritik işletme kaynaklarından biri haline gelen "bilgi"nin üretildiği teknolojilerin de denetlenmesi zorunluluğu ortaya çıkmaktadır. Bu nedenle denetim standartları ve düzenlemelerinde belki de en çok dikkat çeken başlıklardan biri BT denetimi ve bilgi güvenliği konusu olmuştur.

Bu çalışmada, BT denetimi ve bilgi güvenliği kavramı ile BT denetiminde bilgi güvenliği konusuna yer veren ISO/IEC 27000 Serisi, COBIT, ITIL, NIST SP 800 Serisi gibi düzenleme ve standartlar inceleme konusu yapılacaktır. Ayrıca Türkiye'deki standart ve düzenlemelerdeki bilgi güvenliği ile ilgili çalışmalar hakkında bilgi verilmeye çalışılacaktır.

Anahtar Sözcükler: Bilgi Teknolojileri Denetimi, Bilgi Güvenliği, Bilgi Güvenliği Uluslararası Standartları.
JEL Kodları: M40, M42, M49.

APA Stili Kaynak Gösterimi:

Koç, S., Şeker, S., Şeker, F. (2019). Bilişim Teknolojileri (Bt) Denetiminde Bilgi Güvenliği ile İlgili Uluslararası Standartlar ve Türkiye'deki Uyum Çabalarının İncelenmesi. *Muhasebe ve Finans Araştırmaları Dergisi*. 1 (2), 121-139.

* Makalenin gönderim tarihi: 06.11.2018; Kabul tarihi: 17.04.2019, iThenticate benzerlik oranı %43
** Sivas Cumhuriyet Üniversitesi, skoc@cumhuriyet.edu.tr, ORCID: 0000-0003-4285-5632
*** Sivas Cumhuriyet Üniversitesi, sseker@cumhuriyet.edu.tr, ORCID: 0000-0001-7131-112X
**** Sivas Cumhuriyet Üniversitesi, fatmaseker@cumhuriyet.edu.tr, ORCID: 0000-0003-2118-1798

IJAFR

INTERNATIONAL JOURNAL OF ACCOUNTING AND FINANCE RESEARCHES
ULUSLARARASI MUHASEBE VE FİNANS ARAŞTIRMALARI DERGİSİ

Cilt:1 Sayı:2 – Kasım 2019

INTERNATIONAL STANDARDS FOR INFORMATION SECURITY IN INFORMATION TECHNOLOGY (IT) AUDITING AND REVIEW OF COMPLIANCE EFFORTS IN TURKEY

ABSTRACT

In the current era, intelligent developments in Information Technologies (IT) have led to the use of many information technology tools, especially computers, in business operations. Moreover, the use of information technology has become a necessity, not an option for business to survive in a highly global competitive environment. Accounting and auditing activities have also been influenced by the develeopments in information Technologies, and a new period has begun, characterized as paperless accounting and paperless auditing. Accounting information is now being produced, stored and reported to the relevant persons with the same tools. The information produced in the computer environment is also audited by means of computers via audit software.

At this stage in auditing, the necessity of supervising the technologies where the"information" which has become one of the most critical business resources and whose importance has been increasing day by day has been produced has appeared. One of the most noticeable titles in the audit standards and regulations mentioned above has been the topic of IT audit and information security.

In this study, the concept of IT audit and information security; ISO/IEC 27000 Series, COBIT, ITIL, NIST SP 800 Series which provide information security in IT audit will be discussed. Also will be given information about the work related to information security standards and regulations in Turkey.

Keywords: Information Technology Auditing, Information Security, Information Security International Standards.

JEL Codes: M40, M42, M49.

1. GİRİŞ[1]

Yaşadığımız çağın getirdiği dinamik rekabet ortamında bir işletmenin hayatta kalabilmesi, doğru bilgiye doğru zamanda ulaşabilmesi ve bunu iş süreçlerine aktarabilmesi ile mümkündür.

İşletme bakış açısıyla bilgi, en önemli üretim faktörleri arasındadır. İşletmelerin rekabet avantajı elde edebilmesi, karar almada kullanılacak olan doğru bilgiyi sistematik olarak elde etmesine, depolamasına, iş süreçlerinde kullanmasına ve gerektiğinde ilgililerle paylaşmasına bağlıdır. Dolayısıyla bilginin de yönetilmesi gerekmektedir (Önder, 2018, s.90). Bu bağlamda muhasebe sistemlerinin ürettiği bilgiler de işletmelerin başarısında kritik bir rol oynamaktadır.

Günümüzde yaşanan teknolojik gelişmelerle birlikte bilgi, bilişim teknolojisi araçları ile üretilmekte, kullanılmakta, depolanmakta ve

[1] Bu çalışma, Sivas Cumhuriyet Üniversitesi Bilimsel Araştırma Projeleri (CÜBAP) tarafından İKT-116 proje numarası ile desteklenmiştir.
Bu makale, 17-20 Ekim 2018 tarihinde İzmir'de düzenlenen 5.Uluslararası Muhasebe ve Finans Araştırmaları Kongresinde sunulmuş olan özet bildirinin genişletilmiş tam metnidir.

paylaşılmaktadır. Muhasebe sistemleri de bu teknolojik gelişmelerden etkilenmiş ve başta bilgisayarlar olmak üzere birçok bilişim teknolojisi aracı muhasebe uygulamalarında yoğun olarak kullanılır hale gelmiştir.

Bilgisayarların muhasebe faaliyetlerinde kullanılması, muhasebe denetiminde de köklü değişimlere neden olmuştur. Denetlenecek olan verilerin hacim olarak çok büyük boyutlara ulaşması ve muhasebe ile ilgili kayıtların bilgisayar ortamında tutulmaya başlanması denetim sürecini ve denetim tekniklerini de etkilemiştir (Karkacıer, 2014, s.12). Ayrıca denetime konu olan ve BT araçları kullanılarak üretilen muhasebe bilgilerinin yine aynı araçlar ile denetlenmesi BT denetimini daha da önemli hale getirmiştir. Çünkü bilgisayarlı ortama taşınan bilgiler, daha önce var olmayan siber saldırılar vb. riskler ile karşı karşıya kalmış ve BT'nde bilgi güvenliğinin sağlanması zorunluluğu doğmuştur.

Bu çalışmada, bilişim teknolojileri denetimi kapsamında bilgi güvenliği konusu inceleme konusu yapılacaktır. Bilgi güvenliğinin sağlanmasına yönelik olarak uluslararası alandaki düzenlemeler ve standartlar araştırılacak, bu bağlamda Türkiye'de bilgi güvenliğinin sağlanmasına yönelik düzenlemeler hakkında bilgi verilmeye çalışılacaktır.

2. BİLİŞİM TEKNOLOJİLERİ (BT) VE BİLİŞİM TEKNOLOJİLERİ DENETİMİ

BT ile ilgili pek çok farklı tanım yapılmaktadır. Kimi zaman "bilginin bilgisayarlar aracılığı ile elde edilerek işlenmesi, depolanması ve paylaşılması" olarak tanımlanırken, kimi zaman "bilginin elde edilmesi, işlenmesi, saklanması ve paylaşılmasında mühendislik ve yönetim tekniklerinin kullanıldığı teknolojiler ve bunlarla ilişkili sosyal ve ekonomik yapılardır" şeklinde ifade edilmektedir. (Akolaş, 2004, s.33).

En basit tanımıyla BT, verileri toplamak ve bilgiye dönüştürmek için donanım, yazılım, iletişim araçları ve bunları destekleyen kaynaklar ve personelin teknolojiye dayalı olarak işletme süreçlerinde kullanılmasıdır.

2000'li yılların başından itibaren denetime konu olan mali raporlar üretilirken BT araçlarından yararlanılmaktadır. Bu mali raporların kaynağını oluşturan muhasebe verileri de aynı araçlar kullanılarak üretilmektedir. (Meral, 2016, s.84). Dolayısıyla sadece muhasebe uygulamaları değil, muhasebe denetimi de "denetim süreci" ve "denetim teknikleri" bakımından değişikliğe uğramıştır.

BT'de yaşanan gelişmelerin, muhasebe mesleğinde etkilerini şu şekilde özetlemek mümkündür (Karkacıer, 2014, s.12):

- Geleneksel muhasebe uygulamaları olan belgelendirme, kaydetme gibi faaliyetler değişmiştir,
- Muhasebede "kayıt tutma işlevi"nin önemi azalmış, danışmanlık ve denetim önemli hale gelmiştir.
- Zamandan tasarruf sağlanmıştır,

- İşlem maliyetleri düşmüştür,
- Teknolojik hileler ortaya çıkmıştır,
- Finansal tabloların zamanında ve karşılaştırılabilir şekilde sunulmasına olanak sağlamıştır,
- E-imza, e-beyanname, e-bildirge ve fatura ve defterlerin elektronik ortamlara taşınması ile kağıtsız muhasebe olarak nitelendirilen muhasebe uygulamalarına geçilmiştir,
- "Bilişim teknolojileri denetimi" kavramının ortaya çıkmasına neden olmuştur.

İşletmelerin bilgi sistemlerine olan bağımlılığı arttıkça, bu sistemlerdeki güvenlik açıkları ve bu açıklar nedeniyle karşılaşılabilecek risklerin yönetilmesi de önem kazanmıştır. Önceleri belgeler üzerinde yapılan suistimaller BT aracılığıyla daha zahmetsiz ve kolay yapılmaktadır. Bu nedenle geleneksel yöntemler ile tespiti mümkün olmayan hile ve suistimallerin önlenebilmesi için bilgi teknolojilerinin de kontrol ve denetimi önem kazanmaktadır (Biçer ve Aydın, 2015, s.216).

Teknolojik gelişmelere bağlı olarak muhasebe bilgi sistemlerinde ortaya çıkan güvenlik tehditlerini kısaca aşağıdaki şekilde sıralamak mümkündür (Demir, 2005, s.149):

- Bilginin gizliliğinin veya mahremiyetinin kaybedilmesi,
- Bilginin çalınması,
- Bilgi ve bilgi teknolojilerinin hileli kullanımı,
- Kasti değiştirme veya veri manipülasyonu sonucu bilgi bütünlüğünün kaybı,
- Kötü niyetli davranışlar ile ortaya çıkan işlem hataları.

BT denetimi, BT denetim standartları ve çerçeve dokümanlar kapsamında sistemler üzerinde işletmelerin sahip olduğu bilgilerin korunmasına, bütünlüğünün, erişilebilirliğinin ve güvenilirliğinin sağlanmasına yönelik olarak, bu teknolojilerin kurumların amaçlarına uygun şekilde etkin ve verimli bir hizmet sağladığı konusunda makul bir güvence vermek adına yapılan incelemelerdir. BT denetiminin niteliği, kapsamı, yürütülme biçimi ve denetimin hedeflerine göre değişmektedir. Denetimde hedeflenen finansal süreçleri etkileyen BT süreçlerinin denetlenmesi, belirli bir faaliyet alanında hizmet veren BT işleyişinin yasal mevzuata uygun olup olmadığının tespit edilmesi, BT'nin bilgi güvenliği hususunda değerlendirilmesi, BT performans ve etkinliğinin değerlendirilmesi ya da farkı diğer konuların değerlendirmesi olabilir. Bu nedenle belirlenen hedefler doğrultusunda BT denetimi bağımsız bir denetim olarak yapılabileceği gibi, mali denetim, uygunluk denetimi, performans denetimi, güvenlik denetimi gibi başka denetim alanları ile birlikte de yürütülebilir (Gündoğan, 2016, s.18).

Bilindiği üzere günümüz iş ortamında bilgiye rahat ve kolay erişebilme bir takım riskleri de beraberinde getirmektedir. Bu riskler, önemli

bilgilerin kaybolması, çalınması, değiştirilmesi, ya da kötüye kullanılması gibi farklı şekillerde ortaya çıkabilmektedir. Şayet bilgi, elektronik ortama taşınmış ise, kağıtlara basılmış bilgiye nazaran daha savunmasızdır. Çünkü elektronik ortama taşınmış ve ağ üzerinde kaydedilmiş bilgiler, yine aynı bilişim teknolojisi araçları vasıtasıyla saldırı ve risklere açık olabilmektedir. Bu nedenle bilgi ve belgelerin koruma altına alınabilmesi için "*bilgi güvenliği*" kavramından söz edilir olmuştur (Alagöz ve Allahverdi, 2011, s.49).

3. BİLGİ GÜVENLİĞİ

Bilginin elektronik ortamlar üzerine taşınması ile birlikte bireyler ve örgütler açısından çeşitli güvenlik riskleri ortaya çıkmıştır. Her geçen gün artan risk ve sorunlar nedeniyle, örgütlerde bilgi güvenliğinin sağlanması hem kurum imajı, hem de kurumun güvenilirliği ve faaliyetlerinin devamlılığı açısından son derece önemli hale gelmiştir (Şahinaslan ve diğerleri, 2009, s. 597).

Bilgi güvenliği, bilgiye erişmenin sürekli olarak sağlandığı bir ortamda, bilginin göndericiden alıcıya kadar gizlilik içinde, bozulmaya ve değişikliğe maruz kalmadan ve üçüncü kişiler tarafından ele geçirilmeden bütünlüğünün sağlanarak güvenli şekilde iletilmesi süreci olarak tanımlanabilir (Vural ve Sağıroğlu, 2008, s. 509).

Bilgi güvenliğinin sağlanabilmesi için bilginin;

1- Gizlilik (Confidentiality),
2- Bütünlük (Integrity),
3- Kullanılabilirlik (Availability) olmak üzere üç unsurunun yeterli düzeyde sağlanabilmesi ile mümkündür.

Bu kavramları inceleyecek olursak, "*gizlilik*", bilginin yetkisi olmayan kişilerin erişimine kapalı olması olarak tanımlanabilir. "*Bütünlük*", yetkisi olmayan kişilerce bilginin değiştirilmesi, silinmesi, ya da başka bir şekilde tahrip edilmesine karşı içeriğinin korunması şeklinde ifade edilebilir. "*Kullanılabilirlik*" ise bilginin ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Yaşanabilecek herhangi bir sorunda bile bilginin erişilebilir olması gereklidir (Yılmaz, 2014, s. 47).

Tarihsel süreç içerisinde bilginin karakteristik özelliklerinin (gizlilik, bütünlük, kullanılabilirlik) temel olarak değişmemesine karşın, bilginin durumuna -yani bilginin işlenmesi, depolanması ve iletilmesine- ilişkin önemli değişiklikler meydana gelmiştir. Bu kapsamda alınacak güvenlik önlemlerinin çeşitliliği de değişim göstermiştir. Bilgi varlıklarının güvenliği sağlanırken teknoloji, bilgi güvenliği politikaları ve insan kaynağına yönelik eğitim/farkındalık unsurlarına dikkat edilmesi gerekmektedir (Henkoğlu, 2017, s.49).

İşletmeler açısından bilgi güvenliğinin sağlanmasının önemi kısaca şu şekilde sıralanabilir (Vural ve Sağıroğlu, 2007, s.192):

- Güvenlik ile ilgili tehdit ve risklerin önceden belirlenmesi ve etkin bir risk yönetimi sağlanabilmesi ve bu sayede kurumsal itibarın korunması,
- İş sürekliliğinin sağlanması,
- Bilgi kaynaklarına erişimin denetlenmesi,
- Bilgi varlıklarının gizlilik, bütünlük ve doğruluğunun sağlanması,
- İşletmeye ait bilgi varlıklarına ilişkin suiistimal/kötüye kullanma gibi durumların engellenmesi,
- Sahip olunan bilginin güvenli şekilde üçüncü taraf veya denetçilere açık olmasının sağlanması,
- Bilişim sistemlerini kullanan kişilerin dikkatsizlik, bilinçsizlik veya suiistimal gibi nedenlerden ötürü ortaya çıkabilecek donanım, yazılım ve ağda oluşabilecek arızalara karşı koruma sağlanması.

Muhasebe açısından bilgi güvenliği konusu incelendiğinde kağıt üzerindeki verilere dayalı olarak gerçekleştirilen geleneksel muhasebe süreci yerini elektronik veri değişimi (EDI), elektronik fon transferi (EFT), internet, intranet, extranet, genişletilebilir biçimleme dili, genişletilebilir işletme raporlama dili (XBRL), ilişkisel veri tabanı yönetim sistemleri, web araçları gibi bilişim teknolojilerinin kullanıldığı, işlemlerin bütünleşik veri tabanlarında ve web platformunda yürütüldüğü dijital uygulamalara bırakmıştır. Bilgisayarlı ortam muhasebe işlemlerini kolaylaştırmış ve hız kazandırmıştır. Ancak pek çok güvenlik sorununu da beraberinde getirmiştir. Bu nedenle işletmeler için hayati öneme haiz muhasebe bilgilerinin bilgisayarlı ortamdaki güvenliğinin sağlanması için gerekli önlemleri alması zorunluluk haline gelmiştir (Alagöz ve Allahverdi, 2011, ss. 58-59).

4. BİLGİ GÜVENLİĞİ İLE İLGİLİ ULUSLARARASI STANDARTLAR VE DÜZENLEMELER

İşletmelerin kullandıkları BT ortamları, benzer teknolojileri kullanıyor olsalar bile birbirinden oldukça farklıdır. İşletmeler, arzu ettikleri hedeflere ulaşmak adına onları destekleyen ve yönlendiren BT ortamları kullanmaktadır. Dolayısıyla her bir işletme farklı risk profiline sahiptir. Her bir denetim faaliyeti, gerek büyüklük ve kullanılan kaynaklar bakımından gerekse yürütülen denetim adımları bakımından farklılık gösterdiği için, bu faaliyetlerin yürütülmesinde tutarlı bir çerçeveye ihtiyaç duyulur (Weiss and Solomon, 2016, p.74). Bilginin gizliliği, bütünlüğü ve kullanılabilirliği ile onu destekleyen süreç ve sistemlerle ilgili riskleri yönetmek için gerekli denetim ortamının kurulması ve bakımının sağlanması şarttır. Bu amaçla bilgi güvenliği yönetimi için bir takım standartlar geliştirilmiştir (Takçı ve diğerleri, 2010, s. 170).

Genel olarak bir standart ister hesap verebilirlik standardı olsun, ister teknik bir standart ya da bilgi güvenliği standardı olsun, bir sistemin başarması gereken bir dizi gereksinimi temsil eder. Standartlar, ürün ya da

hizmetlerin kalite, güvenlik, güvenilirlik, verimlilik vb istenilen özelliklere sahip olmasını sağlar (Tofan, 2001, p. 128). Bilgi güvenliği ile ilgili standart ve düzenlemeler, bilginin bir organizasyon içinde yönetilme biçimlerini tanımlayan bir dizi belgelenmiş, üzerinde anlaşmaya varılmış politikalar, prosedürler ve süreçler olarak ifade edilebilir. Ana hedef, riskleri ve güvenlik açıklarını azaltarak organizasyonun genelinde güveni artırmaktır. Bu amaçla çeşitli sektörler için küresel olarak geliştirilen çok sayıda standart ve düzenleme vardır. Bu standart ve düzenlemelerden bilgi güvenliği ile ilgili olan ve en yaygın kullanım alanı bulanlar ISO/IEC 27000 Serisi, COBIT, ITIL ve NIST SP 800 Serisi standartlar ve düzenlemelerdir.

4.1. ISO/IEC 27000 Serisi (Information Technology- Security Techniques- Information Security Management Systems-Overview and Vocabulary)

Organizasyonların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamak için teknik önlemlerin yanında, teknik olmayan (insan faktörü, prosedürel faktörler, vb.) önlemlerin alınması, tüm bu süreçlerin devamlılığının sağlanması ve bilgi güvenliği standartlarına uygun olarak yönetilebilmesi amacıyla Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları gerekmektedir. Bilgi güvenliği standartları kurumların kendi iş süreçlerini bilgi güvenliğine yönelik risklerden korumaları ve önleyici tedbirleri sistematik biçimde işletebilmeleri ve standartların gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir (Şen ve Yerlikaya, 2013, s. 677).

Bilgi Güvenliği Yönetim Sistemi, ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Bu standart daha sonra Uluslararası Standartlar Örgütü (ISO) tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır (Marttin ve Pehlivan, 2010, s. 50).

Uluslararası Standartlar Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından geliştirilerek yayınlanan ISO/IEC 27000 Serisi, bilgi güvenliği yönetimi için küresel olarak tanınan bir çerçeve sağlamaktadır. Her ne kadar ISO/IEC 27000 standartlar serisi bilgi güvenliğine yönelik olsa da ön planda olan standart ISO/IEC 27001'dir.

ISO/IEC 27001 standardı, bir bilgi güvenliği yönetim sisteminin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli şartları ortaya koyar. Bu standartta ortaya konulan şartlar geneldir ve türleri, büyüklükleri ve doğalarından bağımsız olarak tüm kuruluşlara uygulanabilir olması hedeflenmiştir. Teknik ve teknoloji bağımlı bir standart değildir. Belli bir ürün veya bilgi teknolojisi ile ilgilenmez. Tek ilgi alanı vardır, o da "*bilgi güvenliği"*dir. Teknik detaylara inmeden kuruluşların bilgi güvenliği hususunda neler yapması gerektiğini açıklar (Gündoğan, 2016, s. 20).

BGYS yaşayan bir süreç olmak zorundadır. Bu nedenle standart, BGYS için, "*Planla- Uygula- Kontrol Et- Önlem Al (PUKÖ)"* döngüsünü benimsemiştir. PUKÖ modeli aşamaları şu şekilde özetlenebilir (Şen ve Yerlikaya, 2013, s. 679):

Planlama: Kurumun BGYS politikası, amaçları, hedefleri, prosesleri ve prosedürlerinin oluşturulur.

Uygulama: BGYS'nin gerçekleştirilmesi ve işletilmesini yani, BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesini ifade etmektedir.

Kontrol etme: BGYS'nin izlenmesi ve gözden geçirilmesi, BGYS politikası, amaçlar ve kullanım deneyimlerine göre süreç performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesini ifade etmektedir.

Önlem alma: BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilerek BGYS'nin sürekliliğinin ve iyileştirilmesinin sağlanmasını ifade etmektedir. Bu aşamalar sürekli bir biçimde birbirini izleyerek yaşayan bir sistem oluşturmaktadır.

Standardın 2005 yılına ait sürümünde sürekli vurgulanan Planla–Uygula–Kontrol Et–Önlem Al (PUKÖ) döngüsüne olan bağlılık 2013 yılında yayımlanan sürümünde yer almamaktadır. Ancak düzenli aralıklarla iyileştirme ve geliştirme yapılmasının önemi vurgulanmaktadır. Bu durum, PUKÖ döngüsünün istenilirse sürekli iyileşmeyi sağlamak adına güncel sürümde de kullanılabileceğini göstermektedir (Gündoğan, 2016, s. 21).

ISO/IEC 27000 Standart Ailesi içinde yer alan ve dikkat çeken bir diğer standart, bilgi güvenliği risk yönetimi için ilkeler ortaya koyan ISO/IEC 27005'dir. Bu standart ISO/IEC 27001'de belirtilen genel kavramları destekleyerek, bir risk yönetimine dayalı olarak bilgi güvenliğinin sağlanmasına yardımcı olmak için tasarlanmıştır. Bu standart bilgi güvenliği risk yönetiminin analiz süreci olarak yorumlanır. Riskin kabul edilebilir bir düzeye indirilebilmesi için "ne yapılmalı" ve "ne zaman yapılmalı" konusunda karar vermeden önce olası sonuçların ne olabileceği ile ilgili analiz yapılabilmesine olanak tanır (Firoiu, 2015, p. 93).

ISO/IEC 27000 serisi Bilgi Güvenliği standartları bir kısmı zorunlu bir kısmı kılavuz niteliğinde olan çok sayıda standarttan oluşmaktadır. Bu standartları Tablo.1.deki şekilde özetlemek mümkündür.

Tablo 1: ISO/IEC 27000 Bilgi Güvenliği Standartları Serisi

• ISO/IEC 27000:2012 – ISO 27000 serisi standartlar için sözlük, terimler ve kavramlar. • ISO/IEC 27001:2013 – Bilgi Güvenliği Yönetim Sistemi için gereklilikler.	• ISO/IEC 27017 – Bilgi teknolojisi – Güvenlik teknikleri – ISO/IEC 27002'ye dayalı Bulut bilişiminin bilgi güvenliği boyutları • ISO/IEC 27018:2014 – Bilgi teknolojisi – Güvenlik teknikleri – Bulut bilişiminin	• ISO/IEC 27034-2 – Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 2 : Organizasyon normatif çerçeve. • ISO/IEC 27034-3 -Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 3 :

• ISO/IEC 27002:2013 – Güvenlik Teknikleri-Bilgi güvenliği için uygulama kodu. • ISO/IEC 27003:2010 – Bilgi teknolojisi – Güvenlik teknikleri – ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Rehberi • ISO/IEC 27004:2009 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği yönetimi ölçüm teknikleri • ISO/IEC 27005:2011 – Bilgi Teknolojileri – Bilgi güvenliği risk yönetimi • ISO/IEC 27006:2011 – Bilgi teknolojisi – Güvenlik teknikleri – Akredite olarak BGYS bağımsız denetim ve belgelendirme hizmetleri veren kuruluşlar için rehberlik • ISO/IEC 27007:2011 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği yönetim sistemleri denetim kuralları • ISO/IEC 27008:2011 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği kontrollerine ilişkin denetçiler için yönergeler • ISO/IEC 27010:2012 – Bilgi teknolojisi – Güvenlik teknikleri – Sektörler arası ve kurumlar arası iletişim için bilgi güvenliği yönetimi • ISO/IEC 27011:2008 – Bilgi teknolojisi – Güvenlik teknikleri – ISO / IEC 27002 dayalı telekomünikasyon kuruluşlar için bilgi güvenliği yönetim kuralları • ISO/IEC 27013:2012 – Bilgi teknolojisi – Güvenlik teknikleri – ISO/IEC 27001 ve ISO/IEC 20000-1 entegre uygulanması konusunda rehberlik • ISO/IEC 27014:2013 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi Güvenliği Yönetişimi • ISO/IEC 27015:2012 – Bilgi teknolojisi – Güvenlik teknikleri – Finansal hizmetler için bilgi güvenliği yönetim kuralları	kişisel olarak tanımlanan bilgiler ile ilgili gizlilik boyutları • ISO/IEC 27019:2013 – Bilgi teknolojisi – Güvenlik teknikleri – Enerji sektöründe özel proses kontrol sistemleri için ISO/IEC 27002 dayalı güvenlik yönetimi kuralları • ISO/IEC 27031:2011 – Bilgi teknolojisi – Güvenlik teknikleri – İş sürekliliği için bilgi ve iletişim teknolojisi hazırlığı için yönergeler • ISO/IEC 27032:2012 – Bilgi teknolojisi – Güvenlik teknikleri – Siber güvenlik için kılavuzluk bilgileri • ISO/IEC 27033-1:2009 – Bilgi teknolojisi – Güvenlik teknikleri – Ağ Güvenliği – Bölüm 1 : Genel bakış ve kavramlar. • ISO/IEC 27033-2:2012 – Bilgi teknolojisi – Güvenlik teknikleri – Ağ Güvenliği Bölüm 2 : Ağ güvenliği tasarım ve uygulama ilkeleri. • ISO/IEC 27033-3:2010 – Bilgi teknolojisi – Güvenlik teknikleri – Ağ Güvenliği – Bölüm 3: Referans ağ senaryoları – Tehditler, tasarım teknikleri ve kontrol sorunları. • ISO/IEC 27033-4 Bilgi teknolojisi – Güvenlik teknikleri – Ağ Güvenliği – Bölüm 4 : Güvenlik ağ geçitleri kullanarak ağlar arasında güvenli iletişim. • ISO/IEC 27033-5 – Bilgi teknolojisi – Güvenlik teknikleri – Ağ Güvenliği – Bölüm 5: Sanal Özel Ağ kullanarak ağlar arasında güvenli iletişim (VPN) . • ISO/IEC 27033-6 – Bilgi teknolojisi – Güvenlik teknikleri – Ağ Güvenliği – Bölüm 6: Kablosuz IP ağ erişimi güvence altına alınması. • ISO/IEC 27034-1:2011 – Bilgi teknolojisi – Uygulama	Uygulama güvenliği yönetimi prosesi. • ISO/IEC 27034-4 – Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 4 : Uygulama güvenliği onaylama • ISO/IEC 27034-5 – Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 5 : Protokoller ve uygulama güvenliği veri yapısı kontrol. • ISO/IEC 27034-6 – Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 6 : Özel uygulamalar için güvenlik rehberi. • ISO/IEC 27035:2011 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi Güvenliği Olay Yönetimi. • ISO/IEC 27036-1:2014 – Bilgi teknolojisi – Güvenlik teknikleri – Tedarikçiler İlişkileri için Bilgi Güvenliği – Bölüm 1: Genel bakış ve kavramlar. • ISO/IEC 27036-2:2014 – Bilgi teknolojisi – Güvenlik teknikleri – Tedarikçiler İlişkileri için Bilgi Güvenliği – Bölüm 2: Gereklilikler. • ISO/IEC 27036-3:2013 – Bilgi teknolojisi – Güvenlik teknikleri – Tedarikçiler İlişkileri için Bilgi Güvenliği – Bölüm 3: Bilgi ve İletişim Teknolojileri tedarik zinciri güvenliği için ilkeler. • ISO/IEC 27037:2012 – Bilgi teknolojisi – Güvenlik teknikleri – Dijital delil belirlenmesi, toplanması, elde edilmesi ve korunması için ilkeler • ISO/IEC 27038 – Bilgi teknolojisi – Güvenlik teknikleri – Dijital redaksiyon için özellikleri içerir. • ISO/IEC 27040:2015 – Bilgi teknolojisi – Güvenlik teknikleri – Depolama güvenliği • ISO 27799:2008 – ISO/IEC 27002 Kullanılarak Sağlık Sektöründe Bilgi Güvenliğinin Sağlanması

• ISO/IEC 27016:2014 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği yönetimi – Örgütsel ekonomi	Güvenliği – Bölüm 1 : Genel bakış ve kavramlar.	

(Kaynak: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en)

4.2. Control Objectives for Information Related Technology – Bilgi Teknolojisi ve İlgili Teknolojilere İlişkin Kontrol Hedefleri (COBIT)

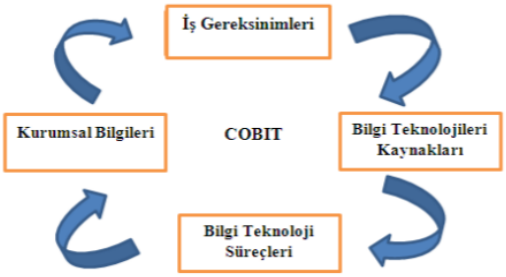
COBIT, bilişim sistemleri yönetimi ve denetimi konularında en geniş teorik çerçeveyi sunarak küresel çapta en fazla kabul gören ve kullanılan bilişim sistemleri standardıdır (Kayrak, 2007, s. 204).

COBIT, kar amacı gütmeyen, bağımsız bir organizasyon olarak 1969'da kurulan ISACA tarafından sunulmuştur. Bilgi güvenliği, güvence, risk yönetimi ve yönetişim konularında çalışan uzmanlara ve BT liderlerine, bilgi ve teknolojiden sağladıkları faydayı artırmaları ve bunlara ilişkin riskleri yönetmeleri konusunda destek sağlamaktadır. COBIT, kurumsal BT yönetişimini ve yönetimini destekleyen tek iş çerçevesidir. Yenilikçi ve etkin bilgi ve teknoloji kullanımını destekleyerek kurumların iş hedeflerine ulaşmasını sağlayan COBIT, tüm dünyada yaygın olarak kullanılmaktadır (https://m.isaca.org/About-ISACA/History/Documents/COBIT-5-translation_pre_Tur_0114.pdf).

COBIT, organizasyonların BT birimleri için yönetim denetim mekanizması olarak geliştirilmiştir. Zamanla BT yönetişim standardı olarak kullanılmaya başlanmıştır. Hedefi, kurum içerisinde değer yaratmak ve kurumun etkili BT süreçlerine sahip olması için gerekli kontrol hedeflerini tanımlamak, bu kontrol hedeflerine uygun rolleri önermek ve kurum yönetişim olgunluk seviyesini artırmaktır (Alıç ve Durdu, 2015, s. 351).

Organizasyonların iş hedeflerini ve gereksinimlerini karşılayacak bilgilerin üretimi ve aktarımının hızlı, sürekli ve güvenli olarak sağlanabilmesi için teknoloji kullanımından kaynaklanan risklerin belirlenmesi, yönetimi ve kontrolünün etkin ve verimli olarak yapılması gerekmektedir. Kısaca "Teknoloji risklerini nasıl yöneteceğiz ve bağlı oldukları yapıyı nasıl güvenli hale getireceğiz?" sorularının yanıtları, sadece bilgi işlem yöneticileri değil, teknoloji yoğun çalışan ve iş süreçlerine teknolojiyi entegre etmiş olan tüm kurumların yöneticileri için önem taşımaktadır. COBIT, bu sorulara sistematik bir yaklaşım sergileyerek ve yönetsel ihtiyaçlara da yanıt verecek şekilde oluşturulmuş bir yöntemdir. COBIT, iş hedeflerinin bilgi işlem hedeflerine dönüşümü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirmektedir (http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf).

COBIT, BT'nin maruz kaldıkları riskleri, bu risklerin değerlemesi ve ortadan kaldırılmasına yönelik kontrolleri ve bu kontrollerin denetlenme yöntemlerini ele alan bir bakış açısı ile oluşturulmuş bir mimariye sahiptir. COBIT, teknolojinin hızlı değişimi doğrultusunda güncel tutulmaktadır. 1996'da ilk kez yayınlanan COBIT, güncellenerek 1998'da 2., 2000 yılında 3. ve 2005 yılında 4., 2007 yılında 4.1 ve son ürünü olarak da COBIT 5 versiyonuna ulaşmış ve "Kurumsal BT Yönetişimi" kavramını ön plana çıkarmış bir standarttır. COBIT'in bir model olarak herhangi bir kurumda yer alabilecek tüm teknoloji süreçlerini kapsayan yapısı içerisinde, gruplanmış 4 süreç alanı ve 34 tane temel Bilgi Teknolojisi süreci yer almaktadır.



Şekil 1: COBIT'in Temel Prensipleri
(Kaynak: Moeller, Robert R. (2008).Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL. John Wiley&Sons, Inc., New Jersey. p.123.)

COBIT'in temel süreçleri, yukarıdaki şekilde görüldüğü şekilde dörde ayrılmaktadır. Bu süreçler; iş gereksinimleri, bilgi teknolojileri kaynakları, BT süreçleri ve kurumsal bilgilerden oluşmaktadır. İş gereksinimleri prensibinin oluşmasında etkinlik, verimlilik, gizlilik, bütünlük, erişilebilirlik, uyumluluk ve güvenilirlik ölçüleri önemli bir yer almaktadır. BT kaynaklarını uygulama, bilgi, altyapı (teknoloji) ve insan (olanaklar) oluşturmaktadır. Bilgi teknoloji süreçlerini ise etki alanları, süreçler ve faaliyetler oluşturmaktadır. Öncelikle bu süreçlerde bilgi teknolojileri kullanımı ile risk ve kaynak optimizasyonu sağlamaktadır (Gökoğlan, 2018, s. 70).

4.3. Information Technology Infrastructure Library- Bilişim Teknolojileri Altyapı Kütüphanesi (ITIL)

ITIL, 1980'li yılların sonlarında, İngiltere Ticaret Bakanlığının BT altyapı ve hizmet süreçlerinin standartlaştırılması çalışmaları ile ortaya çıkan bir kütüphanedir. 1990'lı yıllarda özellikle Avrupa ülkelerinde birçok büyük şirketin ve kamu kuruluşunun ITIL standartlarını benimsemesi ve uygulamaya koyması ile tüm dünyada kabul edilen bir endüstri standardı olmuştur (Dabade, 2010, p. 1).

ITIL, hizmet sunumu ve desteği süreçlerinden oluşan hizmet yönetiminin en etkin şekilde yapılmasına yönelik detaylı bir rehber niteliği taşır. Süreç odaklı olması, bilgi işlem süreçlerini birbirine entegre etmesi,

kullanıcı memnuniyeti öncelikli olması ve büyüklüğü ne olursa olsun tüm kurum ve sektörlerde uygulanabilir olması en belirgin avantajlarıdır (Gantz, 2014, pp. 182-183).

ITIL, güvenlik odaklı olarak BT geliştirme ve BT işlemleri için geliştirilmiştir (Susanto et. al, 2011, p. 25). İş süreç yaklaşımı sayesinde ITIL, müşteri, tedarikçi, IT departmanı ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını sağlar. 1987 yılında ilk hali ile BT yönetimine yönelik "en iyi uygulamalar"dan oluşan bir çerçeveyi anlatan el kitabı şeklinde iken günümüzde kütüphane olmaktan çıkmış ve BT yönetim metodolojisi haline gelmiştir (Gantz, 2014, p. 182).

ITIL'da BT servis yönetiminin asıl amacı, iş hedeflerinin karşılanmasına yönelik teknoloji tabanlı bilgi servislerinin sağlanması ve desteklenmesidir. ITIL ve COBIT birbirlerini tamamlar niteliktedir (Uysal, 2012, s. 254).

ITIL güvenlik politikası BT varlıklarının doğru/yanlış işlenmesi, erişim kontrolü, e-posta, internet, anti virüs, bilgi sınıflandırma, uzaktan erişim gibi konuları içerir (Jašek et. al, 2015, pp. 1-2).

4.4. National Institute of Standards and Technology (NIST) - Special Publications (SP) NIST-SP 800 Serisi

National Institute of Standards and Technology (NIST), 1901 yılında ABD Ticaret Bakanlığı bünyesinde kurulan bir standart kurumudur. Sahip olduğu elektrik-elektronik, fizik, kimya, bilişim teknolojileri gibi birçok alanda hizmet veren laboratuvarlarında bilim adamları, mühendisler, teknisyenler ve diğer destek personeli ile Amerikan endüstrileri için standartlar geliştirmektedir (https://www.nist.gov/director/pao/nist-general-information).

1990 yılında NIST tarafından SP 800 (Special Publications) grubu standartlar yayınlanmıştır. Bu standartlar en eski bilgi güvenliği standartlarıdır. Bilgi güvenliğinin neredeyse her yönünü kapsayan 100'den fazla belgeden oluşmaktadır. Bu dizideki yayınlar hükümetler, endüstriler ve akademik kuruluşlardaki güvenlik ve araştırma çabalarına ilişkin raporlar sunar (Kim and Solomon, 2018, pp. 397-398). Tüm bu belgeler arasında NIST yaklaşımını en iyi temsil eden, bilgisayar güvenlik el kitabı NIST SP 800-12'dir.

SP 800-12, bilgi güvenliği ile ilgili temel prensiplerin ayrıntıları ile ele alındığı çekirdek dokümandır. Bu belge dizinin geri kalan dokümanları ile birlikte güvenlik konularını temel ilkelere uygun olarak ele alınabileceği özel stratejileri, prosedürleri ve kontrolleri ayrıntılı şekilde açıklamaktadır. Örneğin NIST SP 800-45 Elektronik Posta Güvenliği Yönergeleri; NIST-SP 800-50 Bilgi Teknolojileri Güvenliği Bilinçlendirme ve Eğitim Programı Oluşturma; NIST-SP 800-63 Elektronik Kimlik Doğrulama Kuralları; NIST-SP 800-95 Güvenli Web Hizmetleri İçin Yönergeler sözü edilen bilgi

güvenliği ile ilgili bu ayrıntılı destek dokümanlarından sadece birkaçıdır (Tofan, 2011, pp. 131-132).

Bu standartlar arasında özellikle risk yönetimi konusunda dikkat çeken NIST-SP 800-30 Risk Değerlendirmesi Yürütme Kılavuzudur. Risk değerlendirmeleri etkin bilgi güvenliği programlarının geliştirilmesinde kritik bir rol oynamaktadır. Yöneticilerin örgütlerine ve BT altyapılarına ilişkin bilgi güvenliği risklerini değerlendirmelerine olanak tanır. NIST-SP 800-30 rehberi finans, sağlık, bilişim, üretim ve askeri organizasyonlar gibi pek çok organizasyon uyarlanabilir şekilde esnek olarak geliştirilmiştir (https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1)

Tüm NIST-SP 800 dokümanları, önemli temel kavramları, maliyet konularını, güvenlik kontrolleri arasındaki ilişkileri açıklayarak bilgisayar tabanlı kaynakların (donanım, yazılım ve bilgi dahil) güvenliğini sağlamada yardımcı olmaktadır. NIST'in kendisi bir sertifika programı sunmasa da farkındalık, gelişim ve eğitim alanlarında destek sağlamaktadır (Tofan, 2011, pp. 131-132).

5. TÜRKİYE'DE BT DENETİMİNDE BİLGİ GÜVENLİĞİ

BT denetiminde bilgi güvenliği konusunda Ülkemizdeki durum değerlendirildiğinde ISO/IEC 27000 ailesinden olan ISO/IEC 27001 standardı karşımıza çıkmaktadır. Orijinal ismi "Information Technology- Security Techniques- Information Security Management Systems- Requirements" olan bu standart, Türk Standartları Enstitüsü (TSE) tarafından Türkçeye çevrilmiş, "Bilgi Teknolojisi- Güvenlik Teknikleri- Bilgi Güvenliği Yönetim Sistemleri- Gereksinimler" adı altında TS EN ISO/IEC 27001 standardı hazırlanmıştır. Teknik bir standart olmayan ISO/IEC 27001 kurum, kuruluş ve işletmelerin güvenlik gereksinimlerini tanımlamış, ancak gerçekleştirme şekillerini işletmelere bırakmıştır. Başka bir ifade ile kurum içi ve dışı yanlış ve kötü amaçlı kullanıma karşı bilginin korunması için gerekli beklentileri tanımlamıştır. TSE tarafından hazırlanan standardın amacı Bilgi Güvenliği Yönetim Sistemini kurmak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak olarak ifade edilmiştir (Yılmaz, 2014, s. 51).

Ülkemizde özellikle bankalarda ve finans sektöründe bilgi güvenliği konusunda dikkat çeken bir diğer standart COBIT'tir. Türkiye'de COBIT'in kamuoyuna ilk yansıması Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)'nun bazı bankaları COBIT esaslı bir denetime tabi tutması ile gerçekleşmiştir. BDDK'nın 2006 yılından itibaren yayımladığı tebliğ ve yönetmeliklerde COBIT esaslı denetimi tüm bankalar için genişleterek zorunlu hale getirmesi ile tüm bankalar COBIT'le tanışmıştır (Güneş vd., 2013, s. 5). BDDK tarafından yayımlanan "*Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ*"de "*Genel Kontroller*" başlığı altında Madde 22 (2);

"Madde 22 (2): Banka, genel kontrollerin tesisi amacıyla uluslararası kabul görmüş bir standart, çerçeve veya metodolojiyi belirleyerek, buna göre kontrolleri tesis eder. Seçilecek standart, çerçeve veya metodoloji, bankanın faaliyet kapsamı ve faaliyetlerde yararlanılan bilgi teknolojileri ağırlığı ve karmaşıklığı göz önünde bulundurularak belirlenir. Bankanın bilgi sistemleri genel kontrollerini tesis etmek üzere kullanacağı standart, çerçeve veya metodolojinin COBIT'te ele alınan kontrol hedeflerini gerçekleyebilmesi, eğer bu konuda eksiklikleri varsa buna ilişkin kontrollerin ayrıca ele alınarak tesis edilmesi gerekir." ifadeleri ile BT denetiminin COBIT'i esaslarına uygun olarak yürütülmesi gerekliliğini belirtmiştir.

Ülkemizde sadece bankalarda değil, finans ve üretim sektörlerinde de COBIT süreç yönetimi kullanılmaktadır. Yasal mevzuat açısından incelendiğinde, Sermaye Piyasası Kurulu'nun yayımladığı "*Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri:X, No:22),* BT denetimi ile ilgili olarak bir *bilgi güvenliği standardına* vurgu yapmamakla birlikte, bilgi güvenliği konusuna işaret etmektedir. SPK'nın yayımladığı bir diğer tebliğ, doğrudan BT denetimini hedef alan "*Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2)*"dir. Söz konusu Tebliğ 2018 yılında 30292 sayılı Resmi Gazetede yayımlanmıştır. Tebliğin Üçüncü Bölümü'nde "Bilgi Sistemleri Bağımsız Denetim Faaliyetinde Bulunma Şartları" ile ilgili hükümler yer almaktadır. Bu bağlamda Madde 12-1 (a) ya göre;

"Madde 12 – (1) Bilgi sistemleri bağımsız denetimi yapmak üzere görevlendirilecek denetçi yardımcısı dışında kalan denetçilerin;

(a) *Bilgi Sistemleri Bağımsız Denetim Lisans Belgesi veya Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) tarafından verilen Bilgi Sistemleri Denetçisi Sertifikasına (CISA) sahip olmaları"* şartı getirilmiştir.

CISA sertifikası alabilmek için, denetçilerin CISA sınavında başarılı olmaları gerekmektedir. CISA sınavında ise COBIT, ISO 27001 ve ITIL dokümanlarının okunmasının faydalı olacağı belirtilmektedir (Erken ve Bozkurt, 2009, ss. 104-106). O halde SPK'nın BT denetiminde bilgi güvenliği konusunda COBIT, ISO 27001 ve ITIL standartlarını göz önünde bulundurduğunu söylemek mümkündür.

T.C. Hazine ve Maliye Bakanlığı İç Denetim Koordinasyon Kurulu (İDDK) tarafından 2014 yılında "Kamu BT Denetimi Rehberi" yayımlanmıştır. Rehberde uluslararası kabul görmüş risk tabanlı bir denetim yaklaşımı benimsenmiştir. Bu bağlamda BT denetimlerinin önemli bir alanını oluşturan BT yönetim süreçleri, uluslararası standartlar ve çerçeveler doğrultusunda belirlenmiştir. Rehber'de COBIT, ISO 27001 ve ITIL çerçevelerinden yararlanıldığı anlaşılmaktadır (Meral, 2016, ss. 92-93).

Ülkemizde BT denetimi açısından düzenlemeler gerçekleştiren bir diğer kurum olan Sayıştay, 6085 sayılı Sayıştay Kanunu'nun, "Sayıştay'ın Görevleri" başlıklı 5. Maddesi uyarınca, kamu idarelerinde mali denetim konusunda yetkilendirilmiştir.

Sayıştay denetimi kapsamına giren kamu kurumlarının BT'ne gün geçtikçe artan bağımlılığı, kurum bilgi sistemlerinin güvenli bir şekilde çalışıp çalışmadığı ve güvenilir veriler üretip üretmediği konusunda da denetlenmesini gerekli kılmaktadır. Bu amaçla Sayıştay Bilişim Sistemleri Denetim Rehberi yayımlanmıştır. Rehberin hazırlanmasında başta Bilgi Güvenliği Standartları (ISO 17799, ISO 27001, …) olmak üzere, Uluslararası Sayıştaylar Birliği (INTOSAI) rehber ve standartları, Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) rehberlerinden yararlanıldığı ifade edilmiştir (Bilişim Sistemleri Denetimi Rehberi, 2013, s. 1). Buna göre Sayıştay tarafından gerçekleştirilen BT denetimlerinin de ISO 27001 güvenliği standartlarına uygun olarak gerçekleştirildiği söylenebilir.

ITIL; doğru servislerin, doğru müşterilere, müşteri ihtiyaçları göz önüne alınarak tasarlanması, minimum risk ile hayata geçirilmesi ve mümkün olduğu kadar yüksek verimlilikle çalıştırılması esaslarına dayanan, tüm bu şartlar sağlandıktan sonra ise servislerin sürekli olarak iyileştirilmesini öngören endüstriyel bir "en iyi uygulamalar" kütüphanesidir. Kurumlara servisleri ile ilgili yapılması gerekenleri doğrudan göstermez; bunun nedeni her işletmenin farklı servislere, her servisin ise farklı süreçlere ihtiyaç duymasıdır. Ancak genel olarak servis mimarisini ve bu mimarinin oluşturulması veya iyileştirilmesi için takip edilmesi gereken yolları gösterir. Türkiye'de büyük ölçekli kurumlarda özellikle finans ve Telekom şirketlerinde ITIL uygulamalarıyla ilgili çalışmalar vardır. Örnek olarak 35 milyon abonesiyle Türkiye'de GSM operatörü Turkcell verilebilir.

Ülkemizde 24 Mart 2016 yılında TBMM'de kabul edilen ve 7 Nisan 2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu da gerek bireysel düzeyde gerekse kamu ve özel sektör kuruluşlarında bilgi güvenliği ile ilgili düzenlemeler getirmiştir. Anılan kanun ile şirketleri çalışanlarının, iş ortaklarının, danışmanlarının ve müşterilerinin kişisel verilerini korumakla yükümlü kılmaktadır. Bu amaçla kişisel verileri korumakla yükümlü şirketlere "uygun güvenlik düzeyini sağlamaya yönelik her türlü teknik ve idari tedbirleri alma" zorunluluğu getirilmiştir. Her ne kadar yasa ile sadece gerçek kişilere ait kişisel bilgilerin korunması hedeflenmişse de kişisel verileri işleyen şirketler veri sorumlusu olarak bilgi güvenliği ile ilgili her türlü tedbiri almakla yükümlü kılınmıştır. Bu tedbirler arasında kurum çalışanlarının eğitilmesi ve farkındalık çalışmalarını da içermek üzere, şirketlerin ağ ve sistem güvenliğini, verilerin güvenli şekilde depolanması ve iletilmesini, erişim kontrollerinin düzenlenerek sürekli gözden geçirilmesini, periyodik sistem zafiyet testlerinin yapılmasını güncel tehditlerin takip edilerek gerekli önlemlerin alınmasını veri yedekleme ve fiziksel güvenliğin sağlanması sayılmıştır.

6. SONUÇ

Yaşadığımız çağ bilgi çağı olarak isimlendirilmektedir. İşletmeler, bilgiye dayalı bir rekabet sistemi içinde varlığını sürdürmek zorunda kalmıştır. Günümüzde işletmeler rekabet avantajı kazandıracak bilgileri, başta bilgisayarlar ve internet olmak üzere çeşitli BT araçları ile elde etmekte, işlemekte, depolamakta ve gerektiğinde ilgililerle paylaşmaktadır. Muhasebe sistemleri de bu gelişmelerden etkilenmiş ve artık muhasebe bilgileri BT araçları ile üretilir ve üretilen bu bilgiler yine aynı araçlar ile denetlenir olmuştur.

Başta maliyet ve hız olmak üzere çeşitli avantajlar sağlayan BT araçları, aynı zamanda daha önce var olmayan bir takım riskleri de beraberinde getirmiştir. Bilgisayarlı ortama taşınan bilgilerin güvenliğinin sağlanması bu risklerden belki de üzerinde en yoğun çalışılan risk türü olmuştur. Bu amaçla pek çok uluslararası kurum ve kuruluş, gerek özel gerekse kamu kurumları için hayati öneme sahip bilgilerin korunabilmesi amacıyla bilgi güvenliği standartları ve düzenlemeleri geliştirmiştir.

Bilginin yetkisi olmayan kişilerin erişimine kapalı olması, değiştirilme veya yok edilme riskinin ortadan kaldırılması temeline dayalı olarak geliştirilen bu standartlardan en yaygın kullanım alanı bulanlar ISO/IEC 27000 serisi başta olmak üzere, COBIT, ITIL ve NIST SP 800 serisi standartlarıdır. Bu standartlar bilişim teknolojileri odaklı olarak bilgi güvenliğinin sağlanması için kurumlar nezdinde yapılması gereken işler, süreçler ve hizmetler hakkında çerçeve sunmuştur ve çağın gerekleri dikkate alınarak sürekli güncellenir olmuştur. Ayrıca söz konusu standartlara uyum derecesi arttıkça, şirketlere olan güven de artmıştır.

Muhasebe bilgilerinin üretildiği BT araç ve uygulamalarını da ilgilendiren bu standart ve düzenlemelere ülkemizde de uyumlaştırma çalışmaları göze çarpmaktadır. Örneğin BDDK yayımladığı yönetmeliklerde COBIT'e uyumu zorunlu kılmaktadır. Ayrıca birçok yasal düzenlemede bilgi güvenliğine vurgu yapılmakta ve gerekli tedbirleri alma konusunda kurum ve kuruluşlara sorumluluk getirmektedir.

KAYNAKÇA

Alagöz, A. ve Allahverdi, M. (2011). Kurumsal Bilgi Güvenliği ve Muhasebe Bilgi Sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi, 4* (3), ss.47-64.

Alıç, E. ve Onay Durdu, P. (2015). Bilgi Teknolojileri Proje Yönetişimi: Türkiye'deki Organizasyonların Durumu. *9. Ulusal Yazılım Mühendisliği Sempozyumu (UYMS),* 9-11 Eylül 2015, İzmir, ss.349-361.

Akolaş, A. (2004). Bilişim Sistemleri ve Bilişim Teknolojisinin Küreselleşme Olgusu ve Girişimcilik Üzerine Yansımaları. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı:12,* ss.29-43.

Biçer, A.A.ve Aydın, O. (2015). Denetimde Bilgisayar Destekli Denetim Tekniklerinin (BDDT) Kullanımı ve Bu Yöntem İle Bir Suistimal Vakasının Tespiti. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Özel Sayı:28*, ss.213-229.

Bankacılık Düzenleme ve Denetleme Kurulu (BDDK). (2007). Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ.

Dabade, T.D. (2010). Information Technology Infrastructure Library (ITIL). Proceedings. *Proceedings of the National Conference INDIACom-2007, Computing For Nation Development,* , February 25-26, New Delhi, pp.1-2.

Demir, B. (2005). Muhasebe Bilgi Sistemlerinde Bilgi Güvenliği. *Muhasebe ve Finansman Dergisi, Sayı:26*, ss.147-156.

Erken, H. Ve Bozkurt S.V. (2009). Bilgi Sistemleri Denetçiliği Sertifikası. *Denetişim*, Sayı:2, ss.104-107.

Firoiu, M. (2015). General Considerations on Risk Management and Information System Security Assessment According to ISO/IEC 27005:2011 and ISO 31000:2009 Standards. *Calitatea: Acces la Success, 16*(149), pp. 93-97.

Gökoğlan, K. (2018). COBIT ve COSO İç Kontrol Yaklaşımlarının Karşılaştırılması. *International Journal of Management and Administration, 2*(3), ss.66-80.

Gündoğan, B. (2016). Bilgi Sistemleri Denetiminde ISO/IEC 27001 Ve ISO/IEC 27002 Standartlarının Yeri. *Muhasebe ve Denetim Dünyası Dergisi, 1*(2), ss.15-28.

Güneş, F., Kızıldeniz, S., Selçuk, S., Suna, B. ve Coşkun, S. (2013). *Bilgi Teknolojileri Denetimi ve COBIT'in Sektörel Uygulanabilirliği"*. Akademik Bilişim Konferansı, 23-25 Ocak 2013, ss.1-8.

Henkoğlu, T. (2017). Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme. *Arşiv Dünyası Dergisi, Sayı:17-18*, ss.46-56.

İç Denetim Koordinasyon Kurulu (İDDK). (2014). Kamu BT Denetimi Rehberi.

Jašek, R., Králík, L. and Popelka, M. (2015). ITIL® and Information Security. *AIP Conference Proceedings, 1648* (1), pp.1-5.

Karkacıer, A. (2014). SPK'da Bilgi Teknolojileri Denetimi Faaliyetleri. *Journal of International Management, Educational and Economic Perspectives, 2* (1), ss.11-17.

Kayrak, M. (2007). Bilişim Sistemleri Stratejisinin Önemi ve Sayıştay Deneyimi, *Sayıştay Dergisi, Sayı:65*, ss.199-208.,

Kim, D. and Solomon, M.G. (2018). Fundamentals of Information Syatems Security. 3th. Ed., Jones&Bartlett Learning, USA.

Kişisel Verilerin Korunması Kanunu. (2016).

Marttin, V. ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları

Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi, 1*(1), ss.49-56.

Meral, E. (2016). Türkiye'de Bilgi Sistemleri Denetimi ve Kamu Gözetimi Kurumu'nun Bilgi Sistemleri Denetiminde Üstlendiği Misyon. *Muhasebe ve Denetim Dünyası, 1*(1), ss. 83-99.

Moeller, R.R. (2008). *Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL*. John Wiley&Sons, Inc., New Jersey.

Önder, Ş. (2018). ISO 27001 Standardı Kapsamında Kurumsal Bilgi Güvenliği ve İşletme Performansı Arasındaki İlişki: BİST 100 Endeksinde Yer Alan İşletmeler Üzerine Bir Uygulama. *Ekonomik ve Sosyal Araştırmalar Dergisi, 14*(14), ss.89-98.

Sayıştay. (2013), Bilişim Sistemleri Denetimi Rehberi, Ankara.

Sermaye Piyasası Kurulu. (2018). Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2).

Sermaye Piyasası Kurulu. (2006). Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No:22).

Susanto, H., Almunawar, M.N. and Tuan, Y.C. (2011). Infomation Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical&Computer Sciences, 11*(5), pp.23-29.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., ve Borandağ, E. (2009), Kurumlara Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri. *Akademik Bilişim'09 – XI. Akademik Bilişim Konfernası Bildiriler Kitabı,* 11-13 Şubat 2019, Harran Üniversitesi, Şanlıurfa, ss. 597-602.

Şen, Ş. ve Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. *Akademik Bilişim 2013- XV. Akademik Bilişim Konferansı Bildiriler Kitabı. 23-25 Ocak 2013*, ss. 677-681.

Takçı, H., Akyüz, T., Uğur, A., Karabağ, R. ve Soğukpınar, İ. (2010). Bilgi Güvenliği Yönetiminde Varlıkların Risk Değerlendirmesi İçin Bir Model. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 3*(1), ss.47-52.

Tofan, D.C. (2011). Informtion Security Standards. Journal of Mobile. *Embedded and Distributed Systems, 3* (3), pp. 128-135.

Uysal, M.P. (2012). Bilgi Teknolojileri Yönetim Süreçleriyle Bütünleşik Bir E-Öğrenme Tasarım Modeli. *E-Journal of New World Sciences Academy, 7*(1), ss.251-268.

Vural, Y. ve Sağıroğlu, Ş. (2007). Kurumsal Bilgi Güvenliği: Güncel Gelişmeler. *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 13-14 Aralık 2007*, Ankara, ss.191-199.

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık*

Weiss, M.M. and Solomon, M.G. (2016). *Auditing IT Infrastructures for Compliance*. Jones&Barlett Learning, USA.

Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Denetişim Dergisi, 15*, ss. 45-59.

http://www.denetimnet.net/UserFiles/Documents/Makaleler/BT%20Denetim/CobiT%20%C3%87er%C3%A7evesi.pdf Erişim Tarihi: 15/08/2018.

https://csrc.nist.gov/News/2012/NIST-Special-Publication-800-30-Revision-1 Erişim Tarihi: 25/08/2018

https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en Erişim Tarihi: 15/03/2019

https://m.isaca.org/About-ISACA/History/Documents/COBIT-5-translation_pre_Tur_0114.pdf Erişim Tarihi: 18/03/2019

https://www.nist.gov/director/pao/nist-general-information Erişim Tarihi: 17/03/2019