T.C.
KTO Karatay Üniversitesi
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı Yüksek Lisans Programı

# İŞLETMELERDE BİLGİ GÜVENLİĞİ UYGULAMA SORUNLARI VE ÇÖZÜM ÖNERİLERİ; KONYA ÖRNEĞİ

Mustafa YILMAZ

KONYA
*Ekim, 2018*

# İŞLETMELERDE BİLGİ GÜVENLİĞİ UYGULAMA SORUNLARI VE ÇÖZÜM ÖNERİLERİ; KONYA ÖRNEĞİ

Mustafa YILMAZ

KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü

İşletme Anabilim Dalı Yüksek Lisans Programı

Yüksek Lisans Tezi

KONYA

Ekim 2018

## KABUL VE ONAY

Mustafa YILMAZ tarafından hazırlanan "İŞLETMELERDE BİLGİ GÜVENLİĞİ UYGULAMA SORUNLARI VE ÇÖZÜM ÖNERİLERİ KONYA ÖRNEĞİ" başlıklı bu çalışma, 22/10/2018 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Dr. Öğr. Üyesi Fatma Didem TUNÇEZ (Danışman)

Dr. Öğr. Üyesi Ahmet ÇALIK

Dr. Öğr. Üyesi Humar KAHRAMANLI

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

Dr. Öğr. Üyesi Fatma Didem TUNÇEZ
Enstitü Müdürü V.

## ETİK BEYAN

KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü Tez/Proje Hazırlama ve Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

22/10/2018

Mustafa YILMAZ

## TEŞEKKÜR

Tez çalışmamda beni bilgisi, tecrübesi ve tavsiyeleriyle yönlendiren, bana yeni ufuklar açan ve tüm çalışmam boyunca yardımlarını esirgemeyen danışman hocam Dr. Öğr. Üyesi. Fatma Didem TUNÇEZ'e teşekkür ederim.

Tez çalışmasında mülakat yaptığım işletmelerin yöneticilerine bu konuda vakit ayıran değerli personellerine; yardımlarını esirgemeyen TSE ve TÜRKAK personellerine; tahsil hayatımda her zaman destek olan ve yol gösteren sayın M.Nevzat ÖRNEK'e teşekkür ederim.

Yaşamım boyunca destek ve sevgilerini eksik etmeyen, sevgili anne ve babama beni her zaman destekleyen değerli eşime, kızıma ve oğluma çok teşekkür ederim.

# ÖZET

İŞLETMELERDE BİLGİ GÜVENLİĞİ UYGULAMA SORUNLARI VE ÇÖZÜM ÖNERİLERİ; KONYA ÖRNEĞİ

YILMAZ, Mustafa
Yüksek Lisans, İşletme Ana Bilim Dalı
Tez Danışmanı: Dr. Öğr. Üyesi. Fatma Didem TUNÇEZ
Ekim, 2018

Bilgi, bir işletme için önemli olan ekonomik varlıklar gibi değerli olması, günlük hayatımızda vazgeçilmez bir yere sahip olması ve öneminin her geçen gün artması nedeniyle uygun olarak korunması gereken bir varlıktır. Günümüzde teknolojinin, iletişimin ve internetin gelişmesi ile birlikte sağlamış olduğu kolaylıkların yanında birçok tehdidi de beraberinde getirmektedir. Bilgi güvenliğinin öneminin artması, ortaya çıkan tehditlerin sonucunda işletmeler, kurumlar, devletler bilgilerinin korunması, yönetilmesi için en uygun bilgi güvenliği çalışmalarına ve çözüm arayışlarına yönelmişlerdir. Yapılan çalışmalar neticesinde ortaya bilgi güvenliğinin temel ilkeleri; gizlilik, erişilebilirlik ve bütünlük kavramları oluşmuştur. Bilgi güvenliği konusunda işletmeler, kurumlar kendi strateji ve süreçleri için en uygun çalışmaların, yaklaşımların sonucunda ortaya ITIL, COBIT, ISO/IEC 27001 gibi bazı standartlar ve yasal düzenlemeler ortaya çıkmıştır. Dünya'da ve Türkiye'de genel olarak kabul görmüş olan ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi standardının yapısı, kapsamı, faydaları, nasıl kurulması ve uygulanması gerektiği konusunda yazılı kaynak sayısı sınırlıdır. Bu kapsamda Konya ilinde bulunan ISO/IEC 27001 Bilgi güvenliği yönetim sistemleri sertifikasına sahip olan işletmeler tespit edilerek bu işletmelerle mülakatlar yapılmış, sistemin kurulması sırasında işletmelere uygulanabilecek çözüm önerileri sunulmuştur.

Anahtar Kelimeler: Bilgi Güvenliği Standardı, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 17799, COBIT, ITIL, BGYS

## ABSTRACT

INFORMATION SECURITY APPLICATION PROBLEMS AND SOLUTION PROPOSALS IN OPERATIONS; KONYA EXAMPLE

YILMAZ, Mustafa
MSc, Department of Business
Supervisor: Dr. Fatma Didem TUNÇEZ
October, 2018

Knowledge is an asset that is important for a business as well as an economic asset, an indispensable place in our daily lives, and an asset that needs to be appropriately protected due to the increase in the value of each day. Today, technology brings together many threats as well as the conveniences that it has provided with the development of communication and the internet. As a result of the increasing threat of information security, enterprises, institutions, governments have been directed to the most appropriate information security studies and solutions for the protection and management of information. The basic principles of information security emerged in the light of the work done; concepts of privacy, accessibility and integrity have been formed. In the field of information security, some standards and legal regulations have arisen as a result of the most appropriate work for enterprises and their own strategies and processes. ITIL who have seen this thesis generally accepted in the world and in Turkey, COBIT, ISO / IEC 27001 standard are given place. Information on the structure, scope, benefits, how to set up and implement the ISO / IEC 27001: 2013 Information Security Management System standard, an information security standard on information security, is presented. In this context, companies with ISO / IEC 27001 Information security management systems certificate in Konya province were identified and interviewed about these subjects. Drawing attention to the most common mistakes made in this regard, the solution proposals that can be applied to the short and long term settlements are presented for

these methods. In this thesis, the most current scientific world and from Turkey, the statistical data is accessed with the current situation is revealed.

Key words: Information Security, Information Security Standard, ISO / IEC 27001, ISO / IEC 27002, ISO / IEC 17799, COBIT, ITIL

## İÇİNDEKİLER

**4. BÖLÜM**
**BİLGİ GÜVENLİĞİ İSTATİSTİKLERİ ARAŞTIRMASI**



**5.BÖLÜM**
**ISO 27001 BGYS HAKKINDA YAPILAN MÜLAKAT SONUÇLARI**

## TABLOLAR LİSTESİ

## ŞEKİLLER LİSTESİ

## SİMGELER VE KISALTMA LİSTESİ

ASELSAN : Askerî Elektronik Sanayii

ABD : Amerika Birleşik Devletleri

BAE : Bileşik Arap Emirlikleri

BDDK : Bankacılık Düzenleme ve Denetleme Kurumu

BGG : Bilgi Güvenliği Grubu -

BGYS : Bilgi Güvenliği Yönetim Sistemi

BS : British Standards

BSI : İngiliz Standartlar Enstitüsü (British Standards Institute)

BTK : Bilgi Teknolojileri ve İletişim Kurumu

CCTA : Merkezi Bilgisayar ve Telekomünikasyon Ajansı (Central Computer and Telecommunications Agency)

CD : Kompakt Disk (Compact Disc)

CMMI : Capability Maturity Model Integration;

CMMI : Capability Maturity Model Integration

COBIT : Control Objectives For Information And Related Technology

COSO : Committee of Sponsoring Organizations of the Treadway Commission

EA : Avrupa Akreditasyon Birliği (European Co-operation For Accreditation)

EPDK : Enerji Piyasası Düzenleme Kurumu

GSYİH : Gayrisafi yurt içi hasıla

HAVELSAN : Hava Elektronik Sanayii

| | | |
|---|---|---|
| ICT | : | Bilgi ve iletişim teknolojisi (Information and Communications Technology) |
| IEC | : | Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission) |
| ISACA | : | Information Systems Audit and Control Association |
| ISO | : | Uluslararası Standartlar Örgütü (International Organization for Standardization) |
| IT | : | Bilgi Teknolojisi (Information Technology) |
| ITGI | : | IT Governance Institute |
| ITIL | : | Bilgi Teknolojileri Altyapı Kütüphanesi (Information Technology Infrastructure Library) |
| ITU | : | Uluslararası Telekomünikasyon Birliği (International Telecommunication Union) |
| ITU-T | : | International Telecommunications Union Telecommunication Standardization Sector |
| KVKK | : | Kişisel Verilerin Korunması Kanunu |
| MEBS | : | Muharebe Elektronik Bilgi Sistemler Okulu |
| NACE | : | Avrupa Topluluğunda Ekonomik Faaliyetlerin İstatistiki Sınıflaması |
| OGC | : | İngiltere Devlet Ticaret Ofisi (Office of Government Commerce) |
| OPM3 | : | Organizational Project Management Maturity Model |
| PCI DSS | : | The Payment Card Industry Data Security Standard |
| P-CMM | : | People Capability Maturity Model |
| PMMM | : | Project Management Maturity Model |

| | | |
|---|---|---|
| PRINCE2 | : | Projects In Controlled Environment |
| PUKÖ | : | Planla – Uygula – Kontrol Et – Önlem Al |
| SOA | : | Service Oriented Architecture Standards |
| TBDS | : | TÜRKAK Belge Doğrulama Sistemi |
| TOBB | : | Türkiye Odalar ve Borsalar Birliği |
| TSE | : | Türk Standardları Enstitüsü |
| TSK | : | Türk Silahlı Kuvvetleri |
| TUİK | : | Türkiye İstatistik Kurumu |
| TÜBİTAK | : | Türkiye Bilimsel ve Teknolojik Araştırma Kurumu |
| TÜRKAK | : | Türk Akreditasyon Kurumu |
| UPS | : | Kesintisiz Güç Kaynağı (Uninterruptible Power Supply) |
| YGG | : | Yönetimin Gözden Geçirmesi |

# GİRİŞ

İnsanların gündelik yaşamının daha rahat ve daha basit hale getirmek amacıyla öğrendikleri her şeye bilgi denilmektedir. Bugün bir bilgiye sahip olmak insanoğlunu daha üstün kılmaktadır. Bilgiyi elinde tutanlar gücün sahibi sayılmaktadır. Geçmişte ve günümüzde bilgi, yaşamın en önemli ekonomik gerçeğidir. Sahip olunan varlıklar arasında bilginin her dönem değerli olması bilginin etkili bir şekilde yönetilmesini gerektirmiştir. İşletme ve kurumlarda sunulan diğer ürün ve hizmetler kadar bilginin varlığı çok önemlidir. Bu sebeple eldeki bilginin uygun bir şekilde korunması ve denetlenmesi gerekmektedir.

Bilginin bir varlık ve değerli olması nedeniyle, sahip olunan bilgi ile ilişkin bazı konuların oluşturduğu şartların, özelliklerine göre düzenlenmesi gerekmektedir. Bilgi basit bir benzetme ile değerli bir meta ve paradır. Ülkeler, kurumlar ve bireyler için bilginin elde edilmesi kadar korunması da zor bir metadır. Değerli mülk olarak tanımlanan meta ve bilgi bir işletmenin, kurumun öz bilgi varlığı olarak kabul edilir (9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2016).

Gelişmekte olan ve değişen dünyada, bilginin önemi her geçen gün artmaktadır. İşletme ve kurum için önemli olan, bilgiye yönelik bir takım tehditler olmaktadır. Tehditlerin çoğu zaman göz ardı edilmesi ile birlikte meydana gelen tehditler insanları ve kurumların telafisi olmayan zor problemlere karşı savunmasız bırakabilmektedir. Bilgi hayatımızda sadece yazılı olarak değil bugün çok farklı ortam ve biçimlerde yer almaktadır. Bilginin farklı ortamlarda üretilmesi, saklanması ve iletilmesi, bilgi tehditlerini karmaşıklaştırmakta ve farklılaştırmaktadır. Bilginin iletilirken, saklanırken ve üretilirken farklı ortamlarda olması nedeniyle bilgiye yönelik tehditler her geçen gün çoğalmakta farklı ve karmaşık bir hale gelmektedir (Özbilgin & Özlü, 2010).

İletişim, bilişim ve internet teknolojileri birlikte hızla değişen işletme, kurumlarda birçok değişik olgu ve uygulamaların doğmasında sebep olmuştur. Bu nedenle, işletme ve kurumların yöneticileri hem bilgilerinin değerlerden ve ellerinde bulundurdukları bilgilerden en yüksek katma değer sağlamayı amaçlamışlardır. Bilginin nasıl yönetilmesi gerektiğinin önemi işletmeye sağladığı katma değerden ortaya çıkmaktadır. Bilginin boşa harcanmaması, kaybolmaması, doğru yerde ve doğru zamanda kullanılarak katma değer yaratması için bilgi yönetimi ortaya çıkmıştır (Demirtaş, 2013).

Bilgi güvenliği yönetim sistemi standardı (ISO ISO / IEC 27001 ) Bilgi Güvenlik Yönetim Sistemini işletmek, kurmak geliştirmek, gözden geçirmek, sürdürmek izlemek ve iyileştirmek amacıyla kılavuz olması için hazırlanmıştır. İşletme ve kurumlarda bilgiyi korumayı amaçlayan bir bilgi güvenliği standardıdır. İşin içinde sadece bilişim, bilgisayar ve internet güvenliği haricinde her türlü sürecin güvenliğinin yanı sıra doküman, kayıtların güvenliğini de kapsamaktadır (Gülmüş, 2010).

Bilgi yönetim alanı hızlı bir şekilde karmaşıklaşmakta, genişlemekte ve sürekli olarak değişime uğramaktadır. Bilginin yönetimi, işletmenin uygulamalarını, stratejisini, teknolojilerini, yönetim felsefesini, insan davranışları olarak birçok alanı kapsamaktadır. Bilgi yönetiminin temel amacı, işletmenin hedeflerini gerçekleştirmesinde yardımcı olmaktır. Bilgi yönetiminin kazanımı için, uzun dönemli şartlara uygun planlar ve kurum kültürü büyük önem taşımaktadır. Yeni ekonomide değere dönüştürülen bilgi ve sermaye işletmenin en önemli varlıklarından birisidir. Bilgiye dayalı ekonomide entelektüel sermaye bir kuruluş ve işletmenin en önemli rekabet kaynağı ve dayanağı olmuştur (Demirtaş, 2013).

Bu tez çalışmasında, Dünya'da ve Türkiye'de genel olarak kabul görmüş olan ITIL, COBIT, ISO/IEC 27001 standartlarına yer verilmiştir. Bilgi güvenliği konusunda kullanılan bir bilgi güvenliği standardı olan ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi standardının yapısı, kapsamı, faydaları, nasıl kurulması ve

uygulanması gerektiği konusunda bilgiler sunulmuştur. İşletmelerdeki bilgi güvenliği uygulama sorunları ile etkili bilgi güvenliği oluşturmak için ihtiyaç duyulan uygulamalar ve işletmeler için yararlı olacak bilgi güvenliği standartları incelenerek bu konudaki çözüm önerileri belirtilecektir. İşletmeler için bilgi güvenliği oluşturulması ve bilgi güvenliği yönetim sisteminin uygulama kapsamının belirlenmesi, bir sistem oluşturulması için yapılması gerekenleri belirlemek bu konuda önerilerde bulunulmuştur.

Araştırmanın Amacı:

Dünya ve Türkiye'deki işletmeler, devlet kurumları sürekliliklerini sağlamak için yoğun bir şekilde bilişim teknolojileri ile birlikte bilgi kullanımına yönelmişlerdir. Bilgi iş dünyasının en değerli kaynağı olarak, rekabet yapısını belirlemekte ve işletmelerin yaşamı süresince can damarı haline gelmiştir. Günümüzde, bilgi, iletişim, teknoloji ve internet alanındaki büyük, hızlı gelişmeler ve değişimler işletmeler arasında daha fazla rekabet olmasına neden olmuştur. Bilginin özünü oluşturduğu bu değişimin etkisiyle iş dünyasının tüm kuralları değişerek yeniden oluşmaktadır. Rekabet savaşında ayakta kalmak, rakiplerin bir adım önüne geçebilmek için bilginin rekabetteki yeri ve rekabetin işletmelerin, kurumların yaşamında önemi giderek artmaktadır. Gün geçtikçe değeri artan bilginin işletmeler için önemli olduğu görülmektedir. Bilgilerin kazanımının çok zor olduğu düşünüldüğünde elde edilen bilgilerin devamlılığın sağlanması ve korunması büyük önem arz etmektedir. Bilinçli yada bilinçsiz olarak yapılan en küçük bir bilgi sızıntısı sonucunda oluşacak hataların kurum ve işletmeler tarafından telafisi çok zor olmaktadır. Bu sebeple devletler, kurumlar, işletmeler var olan bilgi birikimlerini korumak için çeşitli alternatif ve yol yöntemlere başvurmuşlardır. Yapılan çalışmalar, birikimlerin neticesinde ortaya herkes tarafından benimsenen ve kabul gören standartlar ortaya çıkmıştır. İşletmeler PRINCE2, PMMM, BS7799, SOA, ITIL, COBIT, OPM3, CMMI, P-CMM, PCIDSS, COSO, OPM3, CMMI, P-CMM, PCIDSS, COSO gibi standartların içerisinden yapılarına ve sektörlerine göre kendileri için en uygun olan standartları kullanabilirler.

Bu çalışmada bilgi güvenlik yönetiminde dünyada en yaygın olarak kullanılmakta olan üç standart bu tez kapsamında incelenmiştir. Bu standartlardan ITIL

güvenlik yönetimi sürecine bakıldığı zaman, bilgi güvenliğin şeklen uygulanması konusunda tanımlama yapmaktadır. Bu süreç içerisinde basit seviyede bilgi güvenliği sağlamanın yanında ayrıca servis yönetimi kavramlarını tanımlamakta, sağlanan servis, hizmetlerin en iyi şekilde yürütülmesi, yönetilmesi ve süreçleri için rehberlik etmektedir. Diğer bir standart olan COBIT ise bilgi teknolojileri yönetiminde elde edilecek hedefleri ortaya koymakla beraber, hedeflere stratejik açıdan bakmaktadır. COBIT'in temelini yönetim kurulu kararları ile birlikte yönetebilirlik ve denetim üzerine kurulmuş geniş kapsamlı kontrol odaklı bir yapısı bulunmaktadır. ISO 27001 standardı bilgi güvenliği yönetim sisteminin ihtiyaçlarını tarif eden, uygulanabilen ve denetlenebilen bir standarttır. Bilgi teknolojileri güvenlik yönetimi için iyi sınıflanma yapılmış, yeterli derecede güvenlik denetimlerinin seçiminin yapılabilmesi için tasarlanmış kolay uygulanabilmektedir.

Tez kapsamında Konya ilinde bulunan ISO/IEC 27001 sertifikasına sahip olan işletmeler tespit edilmiştir. İşletmelerin bilgi güvenliği yönetim sistemlerini kurma gerekçeleri, mevcut kurulu yönetim sistemlerinin uygulama sorunlarının araştırma yapılarak çözüm önerileri sunulmaya çalışılmıştır. Konun bilgi güvenliği olması sebebiyle mülakat yapılan işletmeler bu konuda bilgi ve verilerini paylaşmak istememiştir. Ülkemizde, ilimizde yeni bir alan olması çalışmalarımızı oldukça zorlaştırmıştır. Bu çalışma ile ISO/IEC 27001, Bilgi Güvenliği Yönetim Sisteminin daha yaygın, bilinir olmasını sağlamak, model önerisi ve bilgi üretimi ile literatüre katkı sağlamayı hedeflemektedir.

Tez çalışması hazırlanırken öncelikli olarak literatür, tez, makale taraması yapılmış, yabancı kaynaklar araştırılmış ve Türkiye'de yapılan çalışmalar detaylı olarak incelenmiştir. Bu konuda araştırıcılar tarafından yapılmış çeşitli çalışmalar ve tezlerden yararlanılan kaynakların bazıları ise şunlardır.

Demirtaş (2013), "Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları: bir uygulama örneği" çalışmasında; kamu ve özel sektör kuruluşlarında uygulanan bilgi güvenliği sisteminin başarı dayanakları değerlendirilerek, bilgi güvenliği yönetiminin

performansını aşağı veya yukarı çeken faktörleri ortaya çıkarmak hedeflenmiş ve TS ISO/IEC 27001, Bilgi Güvenliği Yönetim Sistemini kurmak, uygulamak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model önerisinde bulunulmuştur.

Ganbat (2013); "Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması" çalışmasında BGYS standardı olarak tanımlanan ISO/IEC 27001 standardı ve bu standardın nasıl uygulanması gerektiği konusu işlenmektedir. Ayrıca, bilgi güvenliği yönetimine yardımcı olan Bilgi Güvenliği Risk Yönetimi (BGRY) standardı ISO/IEC 27005'in, ISO/IEC 27001 ana standardıyla nasıl bir bağlantıda bulunduğu ve BGYS'yi uygulama işlemlerinin her iki standart tarafından nasıl yönlendirilmesi gerektiği açıklanmaktadır.

Shojaie (2018); "Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in dierent cultures" çalışmasında ise; ISO 27001'in benimsenmesiyle ilgili ekonomik özellikler, ulusal kültürel, politik arasındaki potansiyel ilişkiler, 2006 - 2014 yılları arasında verilen sertifika oranlarının analizleri ve karşılaştırmaları yapılmaktadır.

Haklı (2012); "Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi" çalışmasında; Bilgi Güvenliğinin tanımı yapılmış, Bilgi Güvenliği Standartları incelenmiştir. Kamu kurumlarına, Bilgi Güvenliği Standartları uygulanması için bir model tasarlanmış ve tasarlanan model anlatılmıştır. Bu model önerisi için bir yazılım geliştirilmiştir. Bilgi Güvenliği Yönetim Sistemi'ni (ISO/IEC 27001 BGYS) kurup yönetirken yapılması gereken tüm adımlar sırasıyla yazılımda belirtilmiş ve açıklanmıştır. Kullanılan program doğrultusunda örnek çalışmalar yapılmıştır.

Çek (2017); "Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi" çalışmasında; ISO/IEC 27001 standardı açıklanarak, bilgi güvenliği yönetim sistemini detaylandırılmış. Bilgi güvenliğindeki risklerinin en aza indirilmesi ve bilgi güvenliği yönetişimi konusunda bilgileri, çalışanların bilgi güvenliği farkındalığına yer verilmektedir.

Kumaş (2009); “Bilgi güvenliğinin sağlanmasında risk yönetimi: e-Devlet kapısı uygulaması” çalışmasında tamamlanmış risk analizi verileri için e-Devlet Kapısı Projesi çerçevesinde, ISO 27000 bilgi güvenliği standart ailesi ve diğer bilgi güvenliği, risk yönetimi model ve metodolojilerinin uygulamasını ele almaktadır.

Bilgin (2016); “Bilgi teknolojileri denetimi ve bir uygulama” çalışmasında bilgi teknolojileri kavramına genel bir bakış açısıyla yaklaşılıp, bilgi teknolojileri denetimi ile ilgili kavramlar ve bilgi teknolojileri denetim süreci üzerinde durulmuştur. Çalışmanın son bölümünde bilgi teknolojileri sürecinin nasıl gerçekleştiği ile ilgili örnek bir uygulama yapılmıştır.

Bilgi güvenliği üzerine yapılan konferans, bildiriler taranmıştır. Bilgi güvenliği hakkında güncel sertifikasyon belgesi verilerine ulaşabilmek için Türk Akreditasyon Kurumu ve Türk Standartları Enstitüsü ile ilgili görüşmeler yapılmıştır. Uluslararası standartlar hakkında yapılan anket, araştırmalar ile çalışmamıza veri sağlamaya çalışılmış, en son, geniş kapsamlı BGYS standardı ISO 27001 konusunda ayrıntılara yer verilmeye çalışılmıştır.

# BİRİNCİ BÖLÜM
# BİLGİ, BİLGİ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

## 1.1. BİLGİ KAVRAMI

İnsanların günlük yaşamlarının daha kolay ve basit hale gelmesi amacı ile öğrendiklerine bilgi denilmektedir. Bilgi insanlığın yaşamını, düşüncesini, davranışını, iletişimini, gelişimini, üretmesini, tüketmesini belirleyen faktörlerin başında her zaman yerini korumuştur. Kişiler, kurumlar, işletmeler ve devletler için bilgi ye sahip olunması ve aynı zamanda elde tutulması zor olan bir varlıktır. Elinde bilgiyi tutanlar gücünde sahibi olmaktadırlar. Günümüzde ve geçmişte bilgi, ekonomik yaşamın en önemli gerçeğidir. Bilgi işletmelerin, kurumların her dönem sahip olunan varlıklar, arasında yer alması ve önemli olması nedeniyle bilginin yönetilmesini gerektirmiştir.

Bilgi işletmenin diğer önemli ekonomik varlıklarının korunduğu gibi, korunması gereken bir varlıktır. Bilgiyi elinde tutanlar güçlü olarak değerlendirilmekte, elindeki bilgiyi kullanarak yeni bilgiler üretenler ekonomik süreklilik sağlayarak rakiplerinin bir adım önünde bulunmaktadırlar (Atılgan, 2009). Yaşamakta olduğumuz zamana damgasını vuran bilgi, dünyanın oluşumundan itibaren sürekli büyüyerek önem kazanmış, tarım toplumundan bilgi toplumuna geçişle birlikte üretime ve işletmelerin gelişmesine etki eden en önemli olgu olmuştur (Demirtaş, 2013).

Bilginin gizliliği, güvenilirliği ve her an kullanılabilir durumda, hazır halde bulunması ve güncel olması; günümüzde tartışmasız olarak kabul edilen rekabet gücünün artmasında, kanuni yükümlülüklerini, verimliliğini, kurumsal ve ticari imajın etkin bir şekilde sürdürebilmesi ve koruması için gereklidir. Bilgi birçok biçimde ve ortamlarda bulunabilir. Örneğin; kâğıda basılmış olarak, disk, CD, disket, flash bellek v.b. ortamlarda depolanmış olarak, klasik posta yöntemi ile gönderilmiş biçimde, film, video formatında olabilir veya karşılıklı konuşma sırasında sözlü olarak dahi ifade edilebilir. Kişiler ve kurumlar için önem taşıyan bilgiler, hangi biçimde olursa olsun her zaman uygun bir şekilde korunmalıdır (Ersoy, 2012).

Bilgi ve teknolojinin kullanılmadığı, henüz gelişmediği dönemlerde bilginin korunması, güvenliği bugünkü şartlara göre daha basit ve kolay olmuştur. Günümüzde ise işlerin neredeyse tamamı bilgisayar ve mobil teknoloji ile yönetilmektedir. İletişim ve bilişim teknolojilerinin hızla gelişmesi ve yaşantımızın birer parçası olmasıyla birlikte birey olarak sahip olduğumuz bilginin yönetilmesi, korunması daha kolay iken; bir topluluk, bir kurum, bir işletme olduğu zaman bunun korunması daha zor karmaşık bir hal almaktadır.

## 1.2. BİLGİ YÖNETİMİ

Bilgi yönetimi, çeşitli araştırma ve kaynaklarda değişik uzmanlar tarafından ufak ayrıntılar dışında hemen hemen aynı biçimde tanımlanmıştır. Konuyla ilgili uzmanların çoğu, bilgi yönetiminin; bilginin üretimi, elde edilmesi, paylaşılması, kullanılması ve yönetilmesiyle ilgili çalışmaları kapsadığını ortaya çıkarmıştır (Özgener, 2002). Bilgi yönetimi açısından önemli olan bilginin sistematik, bilinçli ve sürekli bir şekilde üretilmesidir. Bilgi yönetimi, şirketlerin kurumsal bilgilerini çoğaltmak ve geliştirmek amacıyla yaptıkları sistemli çalışmalarla ilgilenmektedir. Yöneticilerin bilgi elde etmesinde dikkat etmesi gereken iki önemli nokta vardır. Bilginin sağlam ve güvenilir olmasının, yanısıra bilginin işletmelere rekabet avantajı kazandırması ve ihtiyaçlarına cevap verebilmesi gerekmektedir (Uzun & Durna, 2008).

Bilginin paylaşılması genel olarak deneyim ve tecrübelerin aktarılması mevcut bilgilerin işletme içinde etkin bir biçimde paylaşılması son derece önemlidir. Bilgi paylaşımının doğru yerde ve doğru zamanda yapılması işletmelere prestij kazandırmanın yanında, yapılan paylaşım işletmeler ve tecrübeli bireylerin yetişmesi ve bunların kendilerini geliştirmesine olanak sağlayacaktır. Bu durumda hangi bilginin ne zaman ve nasıl paylaşım yapılacağı konusu çok önemlidir.

Bilginin üretimi, geliştirilmesi, sınıflandırılması, depolanması ve aktarılması gibi tüm faaliyetler önemli olmakla birlikte, bu bilgiler sadece kullanıldığı ve

değerlendirildiği ölçüde faydalıdır. Bilgi yönetimi üretilmiş olan, sınıflandırılan ve paylaşılan bilginin işletmeye değer katacak bir biçimde kullanıldığında anlamlı ve yararlı bir faaliyete dönüşür (Aktan & Vural, 2005). Bilgi yönetimi; "işletme ve organizasyondaki her türlü bilgilerin, değer üretmek ve rekabet avantajı sağlamak, başarısını artırmaya yönelik etkili biçimde yararlanılması ve idare edilmesi ile ilgili etkinliklerin tamamıdır" (Zaim , 2005).

Kurumsal organizasyonlarda ve işletmelerde bilgi teknolojilerinin kullanılmaya başlaması, bilginin güvenliği ve korunması işlemlerini ciddi bir oranda zorlaştırmıştır. Bunun sonucunda işletme ve kurumlar için bilgi yönetimi kavramı oluşmuştur. İşletmeler tarafından bilgi, diğer rakiplerine karşı ekonomik süreklilik sağlamak ve rekabet avantajı, üretim için önemli bir kaynak olarak kullanılmaktadır. Bilgi yönetiminin bu derece önemli olduğu günümüzde bilgilerin güvende olması ve güvenli şekillerde taşınması ve saklanması çok önemlidir. Bilgi güvenliğinin sağlanması her kurum ve işletme için oldukça önemlidir.

Bilginin kullanımının yaygınlaşması bir değer farkındalık katması nedeniyle bilginin öneminin artması, bilgi yönetimini önemli kılmaktadır. Bilgi yönetiminin asıl amacı işletmenin hedeflerinin gerçekleşmesi konusunda yardımcı olmaktır. Bilgi yönetimi, işletmelerin, kuruluşların sahip oldukları beceri, yetenekler ve deneyimlerle elde ettikleri ortak akılla bilgilerin tanımlanması ve çalışmasıdır. Bu nedenle, bilgi yönetiminin ana hedefleri, işletmelerin uygulanabilirliğini ve genel başarısını sağlamak için işletmelerin mümkün olduğunca akıllı davranmasını sağlamaktır (Aktan & Vural, 2005).

Bilgi yönetimi temel olarak şirket ortamında sürekli artan bilgi kapasitesini güncellemek, oluşan bilgilerin ulaşılabilir olması, gerekli olanların ve bunlara ulaşmak için gerekli olan işlemlerin tanımlanması ve analizini kapsayan ve bunların şirket çalışanlarıyla paylaşılmasını sağlayan bir disiplindir (Demirtaş, 2013).

Geçmişte daha nesnel kavramları yönetmek ve bunların güvenliği ile uğraşmak zorunda kalan yöneticiler, günümüzde artık üretimin ana elemanı durumuna gelen bilgiyi yönetmek durumundadırlar. Bilginin en önemli ekonomik değer haline geldiği bu çağda, en çok korunması gereken kaynak olarak ciddi bir bilgi yönetiminin uygulanması gerekliliği artmıştır. Kurum içi veya kurumlar arası etkinliğin, bilgi kaynaklarını ne kadar etkin kullanabildikleri, ne kadar yönetebildikleri ve bunlardan ne denli yararlanabildiklerine bağlı durumdadır (Akyol, 2013).

## 1.3. BİLGİ GÜVENLİĞİ

Bilgi güvenliği ihtiyacının ne derece önemli olduğunu, yaşamış olduğumuz kayıplardan sonra anlaşılmaktadır. Günlük hayatta basit ve değersiz olan bir bilgi, işletmelerde telafisi olmayan değerli bir varlık haline gelebilir. Buradan bilginin kişiler ve işletmeler üzerinde oluşturduğu riskler herkese göre farklı bir anlam içermektedir. Bir bakkal dükkanının bilgi kaybı ile bir süper marketin bilgi kaybı aynı değerde olmamaktadır. Bilgi kaybı bakkalda fazla bir risk oluşturmazken kaybın telafisi mümkün olabilmektedir. Fakat aynı durum süpermarket için geçerli değildir. Bu durum her türlü iş süreçlerinin yönetimi açısından ciddi sıkıntılar, maddi ve manevi kayıplar oluşturmaktadır. Bilgi güvenliği; işletmelerin ekonomik sürekliliğini sağlamak, ekonomik kayıplarını en aza indirmek, fırsatların ve yatırımların dönüşünü en üst seviyeye çıkabilmesi için bilginin denetlenmesi ve korunması sağlamaktadır.

Bilgi güvenliği; kuruluşların organizasyon yapısına ve faaliyet alanlarına göre uygun metotlar, politikalar, geliştirilerek, kurum içinde bir dizi denetimler ile iç güvenlik grupları gibi organizasyonların gerçekleştirilmesi ve uygulanması ile sağlanabilir. Bilgi güvenliği denetimlerinin sağlanabilme koşulları, yöntemleri ve uygulanabilirliği her kurum ve kuruluş için kendine has özellikler taşımaktadır. Genel güvenlik esasları belli standartlar tarafından tanımlanmış olmasına rağmen, kurum ve kuruluşların hangi bilgilerin korunması gerektiğine kendilerinin karar vermesi gerekmektedir. (Ersoy, 2012).

Teknolojik olarak alınan önlemler sosyal mühendislik ile insanların internet, günlük yaşamlarındaki zayıflıklarını kullanarak çeşitli ikna ve aldatma yöntemleriyle istenilen bilgiyi elde edilmesi kurumları savunmasız bırakabilmektedir. Bu saldırıların asıl amacı, ne güvenlik duvarı, ne veri tabanı ne de bir web sunucusudur. Sosyal mühendisliğin hedefi sadece çalışanlar yani insanlardır (Mitnick, 2003). "Sosyal mühendislik saldırıları" ciddiye alınması gereken önemli bir tehditlerden biridir.

Bir işletmedeki, kurumdaki güvenlik düzeyini belirlemek için en zayıf halka tespit edilir. Bilgi güvenliği ve sistemleri konusunda en önemli en zayıf faktör, insan faktörüdür. Bu konuda istediğiniz kadar en son teknolojiler kullanılsın, teknik olarak ne kadar önlemler alınsın, yeteri kadar eğitimler verilsin yine de bilinçsiz bir kullanıcının bulunduğu bir ortamda bilgi güvenliğini sağlamak kolay olmayacaktır. Bu noktada güvenliğin en zayıf halkası olan insanlar bilinçli veya bilinçsiz bir şekilde çok sayıda bilginin silinmesi, kaybedilmesi gibi durumlara sebep olabilmektedir. Bilgi güvenliği sürekli artan tehditlere karşı kendini yenileyen, her zaman yenilikler için devamlı açık süreçtir (Yılmaz H. , 2014).

Kurumların ve işletmelerin bilgi güvenliği sağlanmadığı sürece, kişisel bilgilerin güvenliği de sağlanmamaktadır. Bilgiye istenilen yerden ve istenildiği zaman hızlı bir şekilde erişimin sağlanabildiği bir ortamda, bilginin göndericiden alıcısına ulaşana kadar gizlilik içerisinde, içeriğinin değiştirilmeden, başkası tarafından ele geçirilmeden, bütünlüğünün bozulmaması ve güvenli bir şekilde iletilmesi, ulaştırılması süreci bilgi güvenliği şeklinde tanımlanabilir (Schmidt, 2004).

Başka bir deyişle; bilgi güvenliği, bilginin gizliliği, bilgilerin bütünlüğü ve erişilebilir olması anlamına gelmektedir. Gizlilik, bütünlük ve erişilebilirlik bilgi güvenliğinin kilit unsurları olarak düşünülebilir. (Fussell, 2005).

Bilgi güvenliğini sağlayabilmek için dünya genelinde geçerliliği kabul edilmiş, standartlaşmış olan aşağıdaki üç temel madde olan; Gizlilik (Confidentiality), Bütünlük (Integrity), Kullanılabilirlik/Erişilebilirlik (Availability) kurallarına uyulması gereklidir. Bu şartlar, aynı zamanda bilgi güvenliğinin tanımını da içinde barındırır.

**Gizlilik (Confidentiality):** Bilgiye sadece yetkili kişiler tarafından erişebilir olduğu, yani yetkisiz erişiminin engellenmesi olarak ifade edilebilir. Bilginin gizlilik derecesinin, kurumun bilgi güvenliği yönetim sistemi uygulama sürecinde yapılacak olan risk analizinin sonucuna ve yasa, kanun, sözleşme gibi resmi zorunluluklara dayandırılarak belirlenmesi gereklidir. Gizlilik niteliğinin sağlanması için kurum tarafından hazırlanan politikada, belirli bir bilgi varlığının gizlilik seviyesi ve karşılıklı yapılması gereken işlemlerin (örneğin; kriptolojik yöntem) tanımlanmasının yapılması gerekmektedir (Ganbat, 2013).

Temel olarak erişim kontrolünün ve gizliliğin sağlanabilmesi bilginin güvenliği için çok büyük önem taşımaktadır. Bilgiye erişimin birçok biçimi, gizliliğin korunması ile ilgilidir. Bilgi hangi formda ve formatta olursa olsun gizliliğinin sağlanması için gerekli olan şifreleme, fiziksel güvenlik, farkındalık vb. gibi kontroller ve önlemler örnek verilmektedir (Aslandağ, 2010).

Erişim sistemine girişlerin belirli yapılar çerçevesinde kontrolünün yapılması sistemin bütünün güvenliği açısından büyük önem taşımaktadır. Sisteme girişlerin yetkiler çerçevesinde oluşturulan kimlik doğrulamaları vasıtasıyla yapılması gerekmektedir. Bu sayede yetkisiz erişimler engellenerek elektronik belgelere erişim kontrol altına alınmaktadır.

**Bütünlük (Integrity):** Bilginin göndericiden çıktığı haliyle bozulmadan bir bütün ve tam olarak alıcısına teslim edildiğini garanti eden bir güvenlik unsurudur. Bilgi iletişim sırasında geçtiği yollarda değiştirilmemiş, eksiltip çoğaltılmamış şekilde alıcısına ulaştırılarak bütünlüğü sağlanır (Gülmüş, 2010). Bilginin bütünlüğünün yanlışlıkla veya kasıtlı olarak kaybedilmesinin önüne geçilmesi için kurumdaki bütün

bilgi varlıkların değerlendirmeye tabi tutularak bu bilgilerden sorumlu kişiler atanmalıdır (Ganbat, 2013).

**Kullanılabilirlik/Erişilebilirlik (Availability):** Bilgiye yetkisi, erişimi olan kişiler ve kuruluşlar tarafından gerekli olduğu zaman kullanılabilir veya ulaşılabilir olması anlamına gelmektedir. Bilgiye erişim hakkının gizliğinin sağlanmasından ve korunmasından erişim hakkı verilen kişiler sorumludurlar. Erişim yetkilendirmesi doğru ve güvenli bir şekilde düzenlenmelidir. Bilginin kullanabilirliğini sağlamak için düzenli olarak izlenilmesi, kontrol edilmesi ve yedekli bir şekilde bulunması gereklidir (Aslandağ, 2010).

## 1.4. BİLGİ GÜVENLİĞİ YÖNETİMİ

İnternet teknolojisiyle gelişen, hızla değişen iş dünyası ve ekonomi birçok farklı uygulamaların oluşumuna yol açmıştır. Yöneticiler hem bilginin ne kadar değerli olduğunu, hem de bu bilgiden en yüksek katma değer sağlamak için bilgiyi nasıl yönetmeleri gerektiğini ve yönetebileceklerini anlamışlardır. Bilgi yönetimi, bilginin kaybolmaması, boşa gitmemesi, doğru kullanılması ve katma değer yaratması için ortaya çıkmıştır (Demirtaş, 2013).

İnternet kullanımın giderek arttığı ve buna bağlı olarak bilgisayar, tablet ve mobil cihazların çoğaldığı ve bilginin hayati bir önem kazandığı günümüzde işletmeleri bilgi hırsızlığı, elektronik saldırılar, sabotaj, bilgi sızdırma, yangın, deprem, sel gibi tehlike ve risklere karşı karşıya kalmaktadır. Bilgi kaybının önlenmesi, meydana gelebilecek zayıflıkların önceden tespit edilebilmesi, önlem alınması, alınan önlemlerin titizlikle uygulanması gerekmektedir. Bilgi güvenliği konusunda bilgiye verilen önem sonucunda işletmelerde planlı, yönetilebilir sürdürülebilir bir sistem arayışına gidilmiş son yıllarda kurumsal organizasyonlar tarafından "Bilgi Güvenliği Yönetimi" kavramı geliştirilmiştir.

Geleneksel iş dünyasında bilişim sistemlerine bağımlılığın artması, bilişim teknolojisinin sunduğu olanakların getirdiği iş fırsatları ve riskler ister istemez "bilgi" kavramının stratejik seviyede ele alınmasına ve yönetimsel bir yaklaşımla kurumları bu alanda sistem kurmaya zorlamıştır (Kahraman, 2006).

Bilgi güvenliği yönetimi, teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sistemi kurmak ve yönetmekle mümkün olmaktadır. Etkili bir bilgi güvenliği yönetim sisteminin oluşturulması için bilgi güvenliği yönetim sistemine ve belirli standartlara ihtiyaç duyulmaktadır.

### 1.5. BGYS NEDİR VE NİÇİN GEREKLİDİR?

Bilginin bütünlüğünü ve gizliliğini, kesintisiz olmasını (erişebilirliğini) sağlamak için sistematik düzenlenmiş planlanmış, yönetilebilir, sürdürülebilir, belgelendirilmiş, yönetim tarafından kabul edilmiş ve uluslararası güvenlik standartlarının esas alındığı faaliyetlerin tümü Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak tanımlanmaktadır (Ersoy, 2012).

BGYS'nin kuruluşa faydalı olabilmesi için etkin bir biçimde uygulanıyor olması gerekmektedir. BGYS, kurulduktan sonra tamamlanacak bir sistem değildir. Sürekli iyileştirme için sürekli devam edecek bir faaliyet olarak görülmelidir. Bunun için de kuruluşun iş ve işletme kültürünün bir parçası olması gerekir. Bilgi Güvenliği için kontrolleri iyi seçilmiş, uygun olarak uygulanmış ve kullanılmış olan bir yönetim sistemi, günün sonunda bir masraf kalemi olmayacak, organizasyonun başarısına katkı sağlayacaktır (Kajava et al., 2006).

Bir işletmenin sadece teknik önlemlerle bilgi güvenliğini ve iş devamlılığı sağlamasının mümkün olmadığı, bu teknik önlemlerin yanı sıra BGYS kapsamında kavramsal ve prosedürel bir takım önlem ve denetimlerin sağlanması gerektiği konusu tüm dünyada kabul edilmiş bir yaklaşımdır. Bilgi Güvenliği Yönetim Sistemi

çerçevesinde oluşturulacak güvenlik, sistem politikasına üst yönetim ve tüm çalışanların destek vermesi tavizsiz bir şekilde uygulamasıdır. Ayrıca işbirliği içerisinde olunan tüm üçüncü kişi ve kuruluşların da bu politikalara uygun davranmakla yükümlü olmaları güvenliği artırıcı bir faktördür. Bu kapsamda BGYS'nin sadece bilgi işlem ve IT (Information Technology) bölümlerinin işi olmadığını, tüm kurum birimlerinin ve çalışanların ortak projesi olduğunu özellikle vurgulamak gerekmektedir (Ersoy, 2012).

BGYS Politikasında; organizasyonun ve süreçlerinin, güvenlik politika hedeflerinin, güvenlik altyapısının açıklanması; bilgi varlıklarının ve bunlara ait tehdit ve risklerin tanımlanması, mevcut durum ve güvenlik önlemleri, acil durum planlarının belirlenmesi gibi konuların örgüte/kuruma nasıl uygulanacağının genel bir şekilde ifade edilmesi gerekmektedir (Tvrdíková, 2008).

Bilgi güvenliği bilincini oluşturma ihtiyacı duyan tüm kurum, kuruluşlar ve işletmeler için BSI (İngiliz Standartlar Enstitüsü) tarafından yapılan çalışmalar sonucunda temelleri 1993 yılında atılan ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile alınacak yönetimsel ve teknik önlemler standart hale getirilmiştir. Bu standart daha sonra devletler bazında da kabul görmüş ve kanunlara eklenerek bazı piyasalarda etkinlik gösteren firma ve kuruluşlar için zorunluluk haline getirilmiştir.

Aşağıda Bilgi Güvenliği Yönetim Sisteminin işletmelere, kuruma sağlayacağı faydalar ana hatlarıyla belirtilmiştir.

- Kurumsal prestijin korunması ve yükseltilmesi (Ersoy, 2012).
- Sürekli denetimler uygunsuzlukların tespit edilerek gerekli iyileştirmelerle sistemin hayatta kalmasını.
- Güvenlik standartlarına ve sektöre uyumlu olmasını.
- Sektörel rekabette güvenlik açısından geride kalmamasını (Ersoy, 2012).
- Kurum bilgi varlıklarının ve önem derecelerinin tespit edilmesini (Demirok, 2016).
- Kurumsal yönetim biçimini.
- Üst yönetim ve müşteri gereksinimlerinin karşılanmasını (Demirtaş, 2013).

- Yasa ve yönetmeliklere uyumlu olmasını.
- İş sürekliliğinin devam etmesini.
- Risklere karşı sürekli uyanık kalmasını.
- Bilgi kaynaklarına erişimin denetlenmesini.
- Bilgi sistemlerinin ve varlıkların kapsamlı bir envanterine sahip olunmasını.
- Bilgi varlıklarının doğruluğunun ve bütünlüğünün olmasını.
- Bilgi varlıklarının gizliliğinin, bütünlüğünü ve sürekli kullana bilirliği.
- Personelin, müşterilerinin ve yüklenicilerin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanmalarının engellenmesini.
- Personelin, başkaları tarafından yapılabilecek olan saldırılar nedeniyle suçlanmasının önüne geçilmesi (yetkisiz erişim engellenmesi ve loglama) (Ersoy, 2012) sağlamaktadır.

## 1.6. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

Bilgi güvenliği kurumun faaliyetlerini desteklemede çok önemli bir rol oynamaktadır, bilgi güvenliği konusundaki yönetim sistemlerinde oluşan ihtiyaçları düzenlemek için bir ölçüye, kalite yönetimine ve standartlara ihtiyaç duyulmaktadır. Bilgi güvenliği için uluslararası bir standardın uygulanması özellikle kurumsal işletmelerin/kamu kuruluşların güvenirliğinin ve iş sürekliliğinin sağlanması açısında oldukça önemlidir. Birçok özel ve devlet kuruluşu, bilgi kaynaklarının gizlilik, bütünlük olarak doğru bir şekilde korunması, doğru bir şekilde kullanılması, erişebilir olmasını sağlamak, erişimlerin ölçümlenebilir olması için yeterli güvenlik düzeyinde korunmasını sağlamak amacıyla bazı standartlar ve yasal düzenlemeler yapmıştır. Bu konuda düzenlemeler yapan standart kuruluşları, bilgi güvenliği konusunda çeşitli standartlar geliştirmişlerdir. Bunlar arasında İngiltere'nin oluşturduğu PRINCE2, PMMM, ISO27001, BS7799, SOA, ITIL, COBIT, Amerika Birleşik Devletlerinin ise OPM3, CMMI, P-CMM, PCIDSS, COSO gibi oluşturduğu bilgi güvenliği standartları bulunmaktadır (Susanto, Almunawar, & Tuan, 2011).

Dünyada ve Türkiye'de yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasında önemli bir rol oynayan güvenlik standartları mevcuttur. Ancak, bu

standartların bazıları, çeşitli sebeplerle, kuruluşlar tarafından iyi bir şekilde kullanılmamaktadır. Bilgi güvenliği üzerinde çalışmaya başlamadan önce araştırılması gereken en önemli konulardan biri hangi standartların seçileceği ve bu uygulamaların hangi kapsamda ele alınacağıdır. Örneğin ülkemizde Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)'nın getirdiği yasal mevzuat nedeniyle COBIT, finans sektöründe kabul görmüş bir sistem haline gelmiştir. Son kullanıcı ve müşterilere servis hizmeti veren firmaların tercihi ise ITIL bilgi güvenlik standardı olmuştur. Bilgi güvenliği süreç yönetim sistemi olan ISO / EIC 27000 ailesi savunma, hizmet ve finans sektöründeki özel durumlar dışında haberleşme, tasarım, ar-ge, üretim, sağlık, bilgi teknolojileri gibi ana faaliyet alanlarındaki firmaların ihtiyaçlarını karşılamaktadır. Bu standart ailesi, bilgi güvenliği süreçlerini tam olarak karşılaması, destekleyici diğer standartlarla herhangi bir eksiklik bırakmaması nedeniyle bu süreç yönetiminin çok yaygın olarak kullanılmasını sağlamaktadır (Evrin & Demirer, 2011). Bu tezde, bilgi güvenliği için yaygın olarak kullanılmakta olan ITIL, COBIT ve ISO 27001 standartları incelenmiştir.

Tezin ilerleyen bölümünde ise ISO 27001 standardı detaylı olarak incelenecektir.

### 1.6.1. ITIL (Information Technology Infrastructure Library)

1980'li yılların sonlarında ilk kez Merkezi Bilgisayar ve Telekomünikasyon Ajansı (CCTA) tarafından başlanılmış daha sonrada İngiltere Ticaret Ofisi Bürosu tarafından geliştirilen ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi), bilişim teknolojileri hizmetleri için bir referans model, çerçeve olarak özel sektör ve kamu sektörlerinde yaygın bir şekilde benimsenmiştir (Spremic, Zmirak, & Kraljevic, 2008).

Önemli bilgi teknolojileri organizasyonları için kullanılabilecek en iyi uygulamaları ve tecrübeleri bir araya getirerek oluşturulan süreç odaklı yaklaşım benimseyen bir yordam kütüphanesidir. ITIL çerçevesinin süreçleri planlamak kuruluşların uygulamalarını etkinliklerini ilişkilendirmek bilginin temel alabileceği yaklaşımları, görevleri, süreçleri ve faaliyetleri tanımlar; ancak bu faaliyetlerin nasıl uygulanması gerektiğini açıklamamaktadır. ITIL dünyada gerçekte standart olarak benimsenmiş, teoriden çok pratiğe dayalı bir yapısı olduğu görülmektedir. ITIL her

büyüklükteki organizasyonda ve sektörde uygulanabilme özelliğine sahiptir. Belli bir sektöre yönelik olarak hazırlanmamıştır. İster üretim, hizmet, ister kamuda ve BT sektöründe olan organizasyonların bilgi işlem grupları tarafından uygulanabilmektedir (Hacısüleymanoğlu, 2010).

ITIL'in yıllara göre tarihsel gelişimi

1980'lerde Merkezi Bilgisayar ve Telekomünikasyon Kurumu bir dizi öneriler geliştirmiştir. ITIL, BT hizmetlerini en başarılı yöneten örnek uygulamaları esas alarak başlamıştır.

1989-1996'da, ITIL versiyon 1'de kaynak sayısı, otuz cilde kadar çıkmıştır.

1990'ların başında Avrupa'daki büyük şirketler ve devlet kurumları bu çerçeveyi benimsemektedir. Hem İngiltere'de hem de dünya genelinde kullanımı arttıkça, BT değişmiş ve evrimleşmiş ve ITIL de gelişim sağlamıştır.

CCTA, 2000 yılında OGC'ye (Office of Government Commerce) katılmış, OGC tarafından basılan kitaplar tüm dünyayla paylaşılmış bu sebeple herkese açık süreçler olmuştur. Microsoft, mülkiyeti kendisinde olan Microsoft Operations Framework programını geliştirmek için temel olarak ITIL'yi örnek almış ve kullanmıştır. Bu konuya ek olarak da, dünyanın ilk ITIL uyumlu standardı BS15000 yayınlanmıştır.

Hizmet Desteği ve Hizmet Sunumu kitapları yeniden geliştirilmesiyle ITIL versiyon 2 2001'de 8 kitap olarak çıkmıştır.

2002'de BS15000 hizmet yönetimi standardı revize edilerek düzenlenmiştir.

2007'de ITIL versiyon 3'de ana kaynak olarak kullanılan 5 kitap olarak yayınlanmıştır (Odabaşı, 2011).

ITIL'in bir kuruluş ve işletmeler için,

BT hizmetleri ile artan kullanıcı ve müşteri memnuniyeti

Geliştirilmiş hizmet kullanılabilirliği, doğrudan işletme kazançlarının ve gelirin artması,

Azalan yeniden işleme, kaybolan zaman, gelişmiş kaynak yönetimi ve kullanımı ile finansal tasarrufu,

Yeni ürün ve hizmetler için pazarlama süresinin geliştirilmesi,

Geliştirilmiş karar alma ve optimize edilmiş risk, kontrolü gibi faydaları vardır.

ITIL doğru servisin doğru müşteriye doğru zamanda müşteri ihtiyaçlarını göz önüne alarak tasarlaması, gerekli servislerin sağlanıp ve gerekli servislerin sürekli olarak iyileştirilmesini ön görmektedir. ITIL bilgi teknolojilerinin iş hedeflerini destekleyen bir hizmet olarak görülmektedir (Odabaşı, 2011).

ITIL'de tasarlanan ve yönetilen hizmetleri oluşturan aşamaların tanımlandığı hizmetlerin geliştirilmesi, sürekli iyileştirilmesi süreci olan Hizmet Yaşam Döngüsü bulunmakta ve beş aşamadan oluşmaktadır. Yaşam döngüsünün merkezinde Service Strategy (ITIL Hizmet Stratejisi) bulunmaktadır. Hizmet stratejisi işletme ve kuruluşlara piyasa odaklı bir yaklaşım ile kullanım faydalarını anlamalarına, BT hizmetlerini yönetmek için bir hizmet yönetimi uygulamasını geliştirerek müşterilerinin ihtiyaç duyduğu hizmet ve ürünleri sunmalarına ve desteklenmesine yardımcı olmakta ve rehberlik etmektedir.

Service Design (ITIL Hizmet Tasarımı); hizmet ve süreçlerin tasarımının temellerini kapsamaktadır. Bir organizasyonun daha iyi hizmet sunmasına yardımcı olmak için bütünsel bir tasarım yaklaşımı sağlamaktadır.

Service Transition (ITIL Hizmet Geçiş); Bir hizmetin yaşam döngüsündeki değişiklikleri planlamaya ve yönlendirmeye yardımcı olmaktadır. Yeni, değişen ve iş gücü yüksek hizmetler için risk yönetimi ile ürün ortamını korumaktadır. Böylelikle işletmenin müşterilerine ve kendisine değer sağlamasına yardımcı olmaktadır.

Service Operation (ITIL Hizmet İşletimi); uygulayıcılara günlük işlemlerin nasıl düzenleyecekleri ve hizmet operasyonların nasıl uygulama yapılacağı konusunda rehberlik etmektedir. Bütün olarak bölümlerin devamlılığını ise Continual Service Improvement (ITIL Sürekli İyileştirme) sağlamakta ve diğer aşamalarda olduğu gibi bu aşamada hizmetlerin iyileştirme fırsatlarını tanımlamak, sürekli hizmet edebilecek şekilde devam etmesini sağlamak, iyileştirme çabalarının etkisini ölçmek için kontrol odaklı bir yaklaşım kullanmaktadır (BMC Software, Inc., 2016).


**Şekil 1. ITIL sürekli iyileştirme yaşam döngüsü**

Kaynak: (BMC Software, Inc., 2016)

ITIL'ın gelişmesinin nedenlerine bakıldığı zaman; işletmelerin ticari performansı yakalama ve ortaya çıkan iş ihtiyaçlarını bilgi teknolojilerini kullanarak memnun etme sürecidir. Bilişim teknolojileri, işletmeler tarafından en güncel sürüm olan v3 kullanılmaktadır. ITIL v3 bilgi güvenliği yönetim sistemi için, ITIL ve ISO / IEC 27001 standart hizmetleri ile birlikte entegre yaklaşıma sahip ve önemli bir tamamlayıcıdır. Her iki standardın amacı en iyi verim alabilmek için pratik çözümler üretmektir. ITIL en elverişli hizmet yönetimine odaklanırken ISO 27001 ise bilgi

güvenliğine odaklanmaktadır (Sahibudin, Sharifi, & Ayat, 2008). Ülkemizde 2013 yılında Türkçe'ye çevrilirmiş ve yayınlanmıştır.

### 1.6.2. COBIT (Control Objectives for Information and Related Technology)

Bilgi güvenliği, küresel olarak kabul görmüş standartlara veya modellere bağlı yönetilmesi ve uyulması gereken bir süreçtir. Dünyada, bilgi güvenliği yönetimi üzerinde yapılan çalışmalardan biri de iç kontrol standardı şeklinde oluşan COBIT'tir.

ISACA ve ITGI tarafından 1992 yılında geliştirilen, COBIT, Bilgi Teknolojileri yönetiminde elde edilecek hedefleri ortaya koymaktadır. "Control Objectives for Information and Related Technology" nin kısaltılmış hali olan COBIT'in Türkçe karşılığı ise "Bilgi ve ilgili teknoloji için kontrol hedefleri" anlamına gelmektedir. Bu tanım, COBIT"in amacını ifade etme açısından çok önemlidir (Akyol, 2013). Aynı zamanda tanımlama ve betimleme yapılacak olursa Bilişim Teknolojilerinin her alanını bir şemsiye gibi kaplamasıdır.

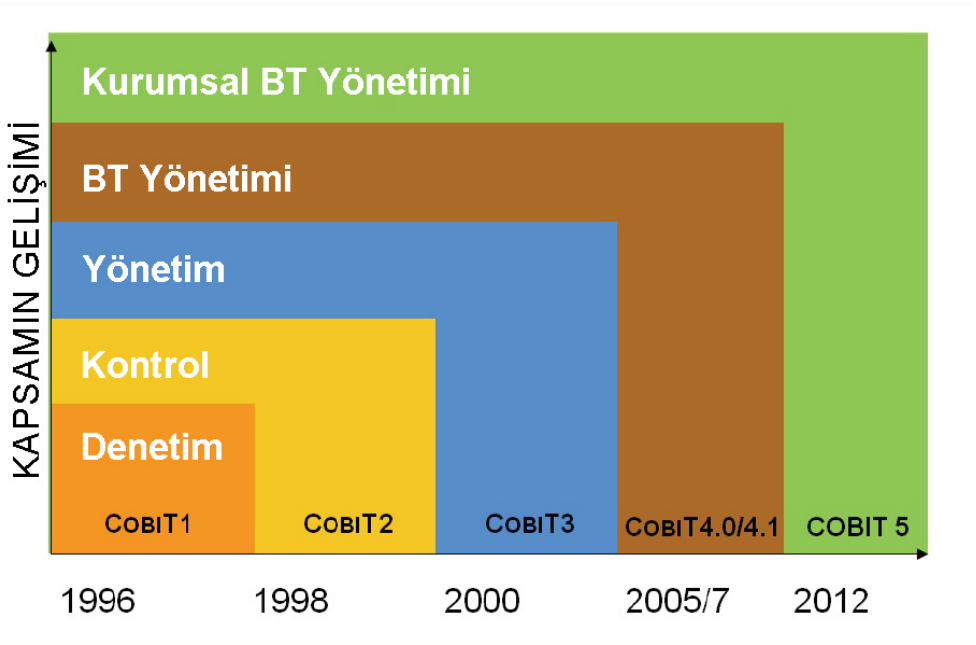
COBIT, bir sürece bağlı değildir, yapısı itibariyle kontrol odaklıdır. COBIT işletmelerdeki, kurumlardaki organizasyonların işlerini nasıl yürütmesiyle değil, bu konuda neler yapılması gerektiği konusunda tavsiyelerde bulunur. Kullanım bakımından yalnızca kullanıcılara ve denetçilere değil, aynı zamanda bu iş sürecine katılan her kesime hitap etmekte ve kapsamaktadır. COBIT'in çerçevesi bilgi sistemleri teknolojisine sağladığı kaynaklar için önemli bir kılavuz olmakla beraber bu alan için gerekli olan bilgileri sağlayan gruplandırılmış süreçler olarak da bilinir (Yılmaz O. , 2014).

COBIT, bilgisayar teknolojilerine dayanan kritik iş süreçlerini desteklemeyi amaçlamaktadır. Teknolojinin etkin ve yaygın kullanımı sonucunda ortaya çıkan kritik iş süreçlerinin bilinçli ve sistematik yöntemlerle desteklenmesinden doğan risklerin

yönetilmesinin yanı sıra, yasal düzenlemeler de bilgi üzerinde sağlanacak kontroller ile ilgili yenilik ve zorunlulukları getirmektedir. Tüm bu noktalar dikkate alındığında, Bilgi işlem teknolojisi ve risklerin yönetimi ve riskleri, organizasyon yönetiminin ayrılmaz bir parçası haline gelmektedir. Yönetim karmaşık ortamlarda risk ve kontrol hakkında daha hızlı ve doğru kararlar vermek için sürekli, yeterli, doğru ve zamanında elde edebileceği bir bilgi arayışındadır (Artinyan, 2009).

COBIT'in yıllara göre tarihsel gelişimi;

COBIT ‟in ilk sürümü 1996 yılında yayımlanmıştır. COBIT IT yönetim modelinin amacı bilgi teknolojilerinin yönetiminde ulaşılması gereken hedefleri ortaya koymaktır. Denetlenecek süreçlerin denetimi açısından bir denetim kontrol listesi şeklindedir. İlk sürüme temel olarak bakıldığında ise denetim ile sınırlı kalmıştır (Yılmaz O. , 2014). 1998, yılında kontrol kavramının ortaya çıkmasıyla birlikte COBIT 2'ye yönetim rehberleri eklenmiştir. Bu sürüm Bilişim Teknoloji sürecinin denetim ve kontrol, performans değerlendirilmesinin nasıl geliştirileceği ve nasıl uygulanacağına dair rehberlik etmek için geliştirilmiştir. 2000 yılında denetim, kontrol ve yönetim çerçevesi yönünde bir yaklaşım sonucunda COBIT 3 ortaya çıkmıştır. Bu sürüme bakıldığında ise yönetim özeti, uygulama rehberi, ölçüm kriterleri, yönetim rehberi, vb. yönetişim araçları yer almaktadır (Bilgin, 2016). 2003 yılında gelindiğinde daha önce yayınlanan bu sürüm online olarak internette hizmete sunulmuştur. COBIT büyümeye ve daha yaygın olarak devam etmesi nedeniyle 2005 Aralık'ta COBIT 4.0 sürümü yayınlanmıştır. 2007 yılında COBIT 4.1 ile hedeflerin açıklığa kavuşturulması kolaylaştırılmış işletmenin, bilgi teknolojisi yönetişim kavramı, hedef ve süreçleri arasındaki ilişkiler yeniden tanımlanmıştır. 2012 yılında piyasaya sürülen COBIT 5.0 sürümünde, en temel yenilik; yönetim, yönetişim kavramları birbirinden ayrılmış ve farklı süreçlerde ele alınmıştır. Bu sürüm beş prensip ve yedi sağlayıcı ile daha kapsamlı ve daha uzun yönetişimin zorluklarını kolaylaştıracak şekilde tasarlanmıştır. 2014 yılında COBIT 5'in Türkçe versiyonu ISACA tarafından kullanıma sunulmuştur. önceki versiyonlarından farklı olmasının nedeni ise kurumsal BT yönetişimine detaylı olarak yer verilmesidir (COBIT Framework, 2000).

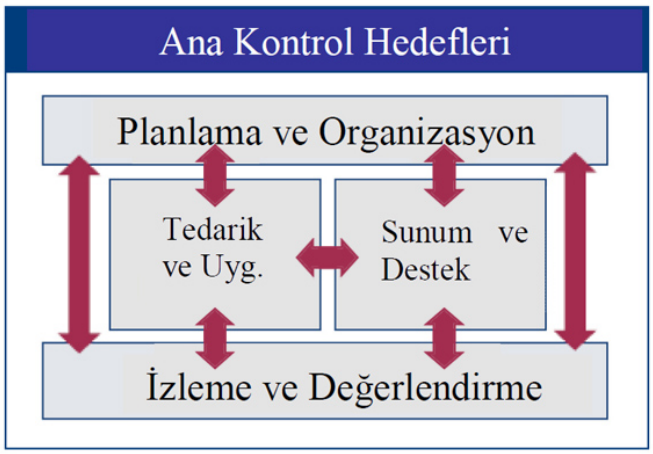



**Şekil 2. COBIT sürümlerinin zaman içindeki yapısal değişimi**
Kaynak: (ISACA,2013)

COBIT ana kontrol hedefleri Şekil 3' de gösterildiği gibi dört etki alanını kapsar:

- Planlama ve Organizasyon
- Tedarik ve Uygulama
- Hizmet Sunumu ve Destek
- İzleme ve Değerlendirme

COBIT'te dört ana kontrol hedeflerinin altında 34 adet bilişim teknolojileri kontrol hedeflerine ilave olarak 318 adet detaylı kontrol hedefleri ile, bilgi işlem güvenliğine kapsamlı ve en iyi uygulama yaklaşımı sunmaktadır. COBIT'in hazırlanması ve oluşturulmasında tüm en iyi uygulamalar ve standartlar (COSO, ISO 9000, CMM, ITIL, BSI7799 vb.) örnek olarak ele alınmış, dünya genelinde danışman, uzman, analistler ve akademisyenler ile ortak bir çalışma yürütülmüştür (Artinyan, 2009).



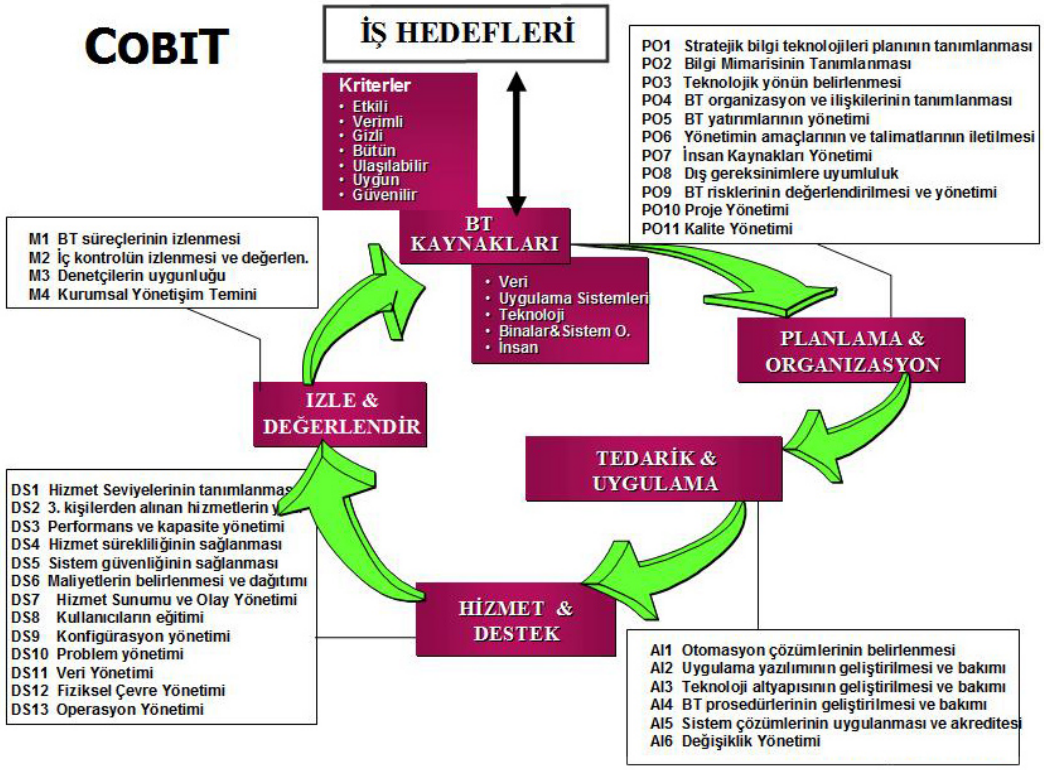

**Şekil 3. COBIT Ana Kontrol Hedefleri**

Kaynak:(ISACA,2007)

COBIT çerçevesinin oluşmasına neden olan içeriklerden biri olan bilgi için işletmenin amaçlarını gerçekleştirebilmesi için bilginin COBIT'in kullandığı denetim kıstaslarına uyumlu olmalıdır. COBIT'in çerçevesi, işletme, kurum ve iş yöntemleri için detaylı kılavuzluk yapmaktadır. Bu konudaki kontrol hedefleri COBIT'de belirtilmiştir. Kontrol prensipleri; denetim değerlendirmesi, uygunluk değerlendirmesi, anlamayı sağlama ve destek riski unsurlarından oluşmaktadır. COBIT tarafından saptanmış bilgi kriterleri şunlardır. Erişilebilirlik, gizlilik, bütünlülük, verimlilik, etkinlik, bilgi teknoloji kaynaklarını, veri, uygulama sistemleri, fiziksel ortam ve insanları kapsamaktadır (Bilgin, 2016).

COBIT'i IT yönetişim çerçevesi

- İş hedeflerine iyi bir bağlantı sağlaması
- Yönetim tarafından IT'nin, bilgi işlem işlevlerinin net olarak anlaşılması
- Süreçlerin, sorumlulukların açık bir şekilde tanımlanması ve netleştirilmesi
- Genel olarak kabul görmüş uygulamaları içermesi
- İş ortakları ve diğer taraflarla anlaşılan ortak bir dil olması
- Uygun bir iç denetim mekanizması olması denetim mekanizmasına değer katmasını sağlamaktadır.




**Şekil 4. COBIT İş Hedefleri**

Kaynak: (Artinyan, 2009)

Türkiye'de COBIT'in tanınması Bankacılık Düzenleme ve Denetleme Kurumu'nun, bazı bankaların COBIT standartları ile özel bir denetim gerçekleştirmesiyle ile ortaya çıkmıştır. BDDK 2006 yılında yayınlamış olduğu; Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi tebliği ile, bankacılık süreçleri denetimi her yıl, bilgi sistemleri denetimi ise iki yılda bir kez denetlenme zorunlu hale getirilmiştir. Hazine Müsteşarlığı tarafından 2016 yılında Sigorta ve emeklilik şirketleri için İç Sistemler Denetim Rehberi hazırlanmıştır. Şirketlerin bilgi sistemlerinden uygulanan standartlar içinde COBIT'te yer almıştır (Başbakanlık Hazine Müsteşarlığı Sigorta Denetleme Kurulu, 2016).

Yıllar boyunca, COBIT açık bir standart olarak geliştirilmiştir ve günümüzde küresel olarak gittikçe artan ve etkili bir şekilde uygulanmakta ve gösterilmekte olan

kontrol modeli olarak benimsenmektedir (IT Governance Institute, The Office of Government Commerce, 2008).

COBIT'in misyonu; denetçiler ve işletme yönetimleri tarafından günlük olarak kullanılmış, geçerli, verimli, çağdaş, milletlerarası kabul gören bilişim teknolojisi kontrol hedeflerini incelemek, tanıtmak, ilerletmek ve ar-ge çalışması yapmaktır. COBIT'in amacı, rekabet avantajı sağlamak, en az maliyetle en yüksek verim almayı, durum optimizasyonu, için iş riski, kontrol gereksinimleri ve teorik konular arasındaki boşlukları saptamak ve doldurmak amacıyla çatı oluşturmaktır (Uzunay, 2007).

Bilişim teknolojileri nerdeyse tüm alanlarda yer almakta ve her geçen gün işletmelerin bilgi teknolojilerine bağımlılıkları artmaktadır. İşletmeler yatırımlarını daha çok Bilgi Teknolojileri odaklı hale getirerek daha çok fayda sağlamayı amaçlamaktadır. Bu nedenle Bilişim Teknolojilerine olan ihtiyaç her zamankinden daha önemli bir noktaya gelmiş durumdadır. Bunun sonucunda Bilgi Teknolojileri yönetişimini, kurumsal yönetişiminden ayırt etmek nerdeyse imkânsız bir hal alamaya başlamıştır. Böyle bir çevrede yeni gereksinimlere cevap vermek amacıyla ortaya çıkmış olan COBIT Bilgi Teknolojileri yönetişimine yeni ve farklı bir yaklaşım getirmektedir (Cantürk, 2013).

COBIT, iş dünyasında, teknolojik çevrelerde, bütün iş modellerinde ve kurumsal kültürlerde kullanılabilir. COBIT, finans, finansal işlemler, analiz ve raporlama, güvence faaliyetleri, risk yönetimi, yasal düzenlemelere uyum, bilgi güvenliği, kurumsal bilgi teknolojilerinin yönetişimini ve yönetimi konularını içermektedir. ISACA tarafından COBIT güncellenmekte ve hazırlanmaktadır. COBIT kaynak ve içeriklerine ISACA‘nın internet sayfası üzerinden ücretsiz olarak erişilebilmektedir. COBIT’in işletmelerde ve kurumlarda uygulanmasının sonucunda her hangi bir şekilde sertifika verilmemektedir.

COBIT büyümeye ve daha yaygın olmaya devam ettikçe, bilişim teknolojileri ile iş dünyası dünyasını birbirine yakınlaştırmaya çalışan, özellikle "Stratejik uyum, katma değer yaratma, kaynakların etkin ve verimli yönetimi, risklerin yönetimi ve performans ölçülebilmesi" alanlarında kullanım için uygun bir yöntem haline gelmiştir.

## 1.7. ISO/IEC 27001 BİLGİ GÜVENLİĞİ STANDARDI

1993 yılında, BSI (British Standards Institution) rehberliğinde ortaya çıkan ilk bilgi güvenliği standardı çalışmasında, işletmelerden endüstriden ve devletten gelen talepler doğrultusunda ortak bir güvenlik yapılanmasında ciddi bir görev almıştır. Bu talebin asıl sebebi, işletme ve kurumların birlikte yaptıkları işlerin sürdürülmesi sırasında ortak olarak en düşük güvenlik seviyede yaptıklarını birbirlerine ispatlama ihtiyaçlarını hissetmelerinden kaynaklanmaktadır (Ersoy, 2012).

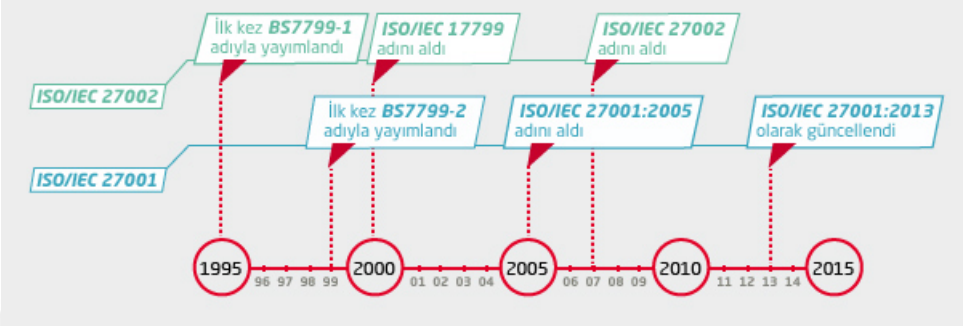
Bilgi Güvenliği Yönetim Sistemi (BGYS) biçimlendirmek için BS 7799 standardı 1993 yılında ilk bölüm olarak BS 7799-1, devamında ise 1999 yılında aynı standardın ikinci bölümü olarak tanımlanan BS 7799-2, İngiliz Standardı olarak yayımlanmıştır. 2000 yılında bazı düzenlemeler ve uygunluk çalışmalarından sonra ISO tarafından ISO/IEC-17799 adıyla kabul edilmiş ve uluslararası bir standart haline gelmiştir. 2002 yılında BSI'ın yapmış olduğu çalışma sonunda BS 7799-2 yeniden düzenlenerek İngiliz Standardı olarak bir kez daha yayımlanmıştır. ISO tarafından 2005 Yılında ISO/IEC-17799 kabul edilen standart üstünde değişiklikler yapılarak ISO/IEC–17799:2005 olarak yeniden yayımlanmıştır. 2005 Yılının sonunda yapılan son bir çalışma neticesinde BSI tarafından yeniden hazırlanan BS 7799-2 incelenip üzerine eklentiler yapılıp düzenlendikten sonra ISO/IEC:27001 adıyla uluslararası standart olarak yayımlanmıştır (Bingöl, 2010). Bilgi Güvenliği Yönetim Sistemi Standardı ISO / IEC 27001, ilk yayından 8 yıl sonra son versiyonu ISO/IEC 27001:2013 olarak 1 Ekim 2013 tarihinde yayınlanmıştır.

ISO/IEC 17799 ve ISO/IEC 27001 iki standardın arasındaki farklılıklar; ISO/IEC 17799'un ana maddeleri muhafaza etmek şartıyla, standardın bazı başlıklarının altında yer alan maddeler yeniden gruplandırılarak başka başlıklar altına alınmış, bazı maddeler ise ilgili diğer başlıklar ile yer değiştirilmiş ve bazı maddelere ilaveler yapılmıştır. Örneğin, daha önceki standartta yer alan Kurumsal Güvenlik Organizasyonu, Varlık Yönetimi, Personel Güvenliği gibi birbirine bağlı maddeler alt başlıklar seviyesinde detaylandırılmış, özellikle elektronik ticaret ile ilgili bölüm ayrı bir grup haline getirilmiştir. Ayrıca, bilgi işlem hizmetlerini izleme işlemleri gözetim adı altında yeniden sınıflandırılmıştır. Standartların faaliyet alanında ve önceki versiyonlara göre bir değişiklik bulunmamakta, bu konuda sadece yeni eklemeler yapılmıştır (Ganbat, 2013).

Dünyada ve ülkemizde bilgi güvenliği standardı ISO / IEC 27001'in tarihsel gelişimi şöyledir:

- 1993 yılında Bir endüstri çalışma grubunun kurulması
- 1993 yılında BS 7799-1 standardının kurallarını içeren rehberin yayınlanması
- 1995 yılında ise genel olarak İngiliz standardı olarak kabul görmesi
- 1998 yılında BS 7799-2 standardının oluşturulması
- 1999 yılı Mayıs ayında BS 7799-1 ve BS 7799-2 standart bölümlerinin uygunluğu yeniden gözden geçirilmiştir.
- 2000 yılı Ocak- Ağustos aylarında BS ISO/IEC 17999 (BS7799 - 1:2000) geçici versiyon olarak yayınlanmıştır.
- 2000 yılında Aralık ayında ISO tarafından standart olarak yayınlanmıştır.
- İngiltere' de 2000 yılında British Standards Institute tarafından BS ISO/IEC 17799:2000 / BS 7799-1:2000 olarak adlandırılması
- 5 Eylül 2002 tarihinde BS 7799 - 2:2002 yayınlanmıştır.
- 11 Kasım 2002 tarihinde TS ISO/ IEC 17799' un TSE tarafından kabul edilmiştir.
- 17 Şubat 2005'de TSE tarafından Bilgi güvenliği yönetim sistemleri kullanım kılavuzu olarak kabul edilmiştir.

- 2006 yılında TS 17799 – 2 iptal edilerek yerini TS ISO/IEC 27001 almıştır.
- 2 Mart 2006 tarihinde TSE tarafından TS ISO/IEC 27001:2005 kabul edilmiştir.
- 01 Ekim 2013 tarihinde ISO/IEC 27001'in son versiyonu yayınlanmıştır.




**Şekil 5. ISO/IEC 27001 Standardın Tarihsel Gelişimi**

Kaynak: İnnova Bilişim

Ülkemizde de Türk Standartları Enstitüsü Teknik Kurulu'nun 11 Kasım 2002 gününde alınan karar sonucunda tercüme edilerek TS ISO\IEC 17799 (Kısım-1) olarak resmen kabul edilmiştir. İkinci kısım olarak bilinen BS-7799-2.2002 Standardı ise yine Türk Standartları Enstitüsü Teknik Kurulu'nun 17 Şubat 2005 tarihinde aldığı karar sonucunda tercüme edilerek TS 17799-2 (Kısım-2) olarak kabul edilmiştir. (Ersoy, 2012)

# İKİNCİ BÖLÜM
# ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN TANITIMI, ÖZELLİKLERİ VE FAYDALARI

## 2.1. ISO/IEC 27000 BGYS STANDARTLARI AİLESİ

Standartlar, iş hayatında denetim ve kontrol işleyişinin herkes tarafından kabul edilmesini sağlamak için bir kurul tarafından geliştirilen, onaylanan bir dizi kuraldır. Standartlar kendi önem derecelerine göre değişir ve farklı olabilmektedir. Bir standardın kapsamına, ileride ortaya çıkacak ihtiyaçlara bağlı olarak gelecekte oluşturulacak alt bölümlerin hangi alanlarda olması gerektiği önemli bir hale gelmektedir.

Bilgi güvenliği ihtiyacı, iletişimin farklı yollarla genişletilmesi ile zaman zaman artırılmaktadır. Güvenlik duvarları veya anti virüs yazılımları gibi teknik önlemleri kullanarak bilgi güvenliğini sağlamak mümkün değildir. Bilgi güvenliği standartları, iş süreçlerini bilgi güvenliği risklerinden korumak, sistematik olarak uygulanan karşı önlemleri almak ve bu değerlendirmelere uygun şirketleri belgelendirmek için geliştirilmiştir. (Vural & Sağıroğlu, Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, 2007).

Uluslararası standardizasyon organizasyonu (International Organisation for Standardisation – ISO) 1947 yılında kurulmuş ve uluslararası geçerlikte olan standartlar konusunda çalışmalar yapan bir kuruluştur. Bundan başka bilgi güvenliği ve yöntemleri hakkında Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission - IEC) ve ve Uluslararası Telekomünikasyon Birliği (International Telecommunication Union - ITU) Bilgi ve İletişim Teknolojileri (Information and Communications Technology -ICT) kuruluşları ile beraber işbirliği yapan devletlere bağlı olmayan bir uluslararası organizasyon kuruluşudur (Evrin & Demirer, 2011).

Bilgi güvenliği yönetim sistemi uygulanırken ve kurulma aşamasında bilinmesi ve dikkate alınması gereken birçok standart maddesi vardır. Bu maddelerin bir bölümü zorunlu, bir diğer bölümü ise kılavuz niteliğindedir. 2005 yılında ISO düzenlemeye giderek bilgi güvenliği için 27000 standart serisini kullanmaya karar vermiştir. Aşağıda kullanılmakta olan güvenlik standartlarının başlık tanımlamaları ve maddeleri bulunmaktadır (Vural & Sağıroğlu, 2008).

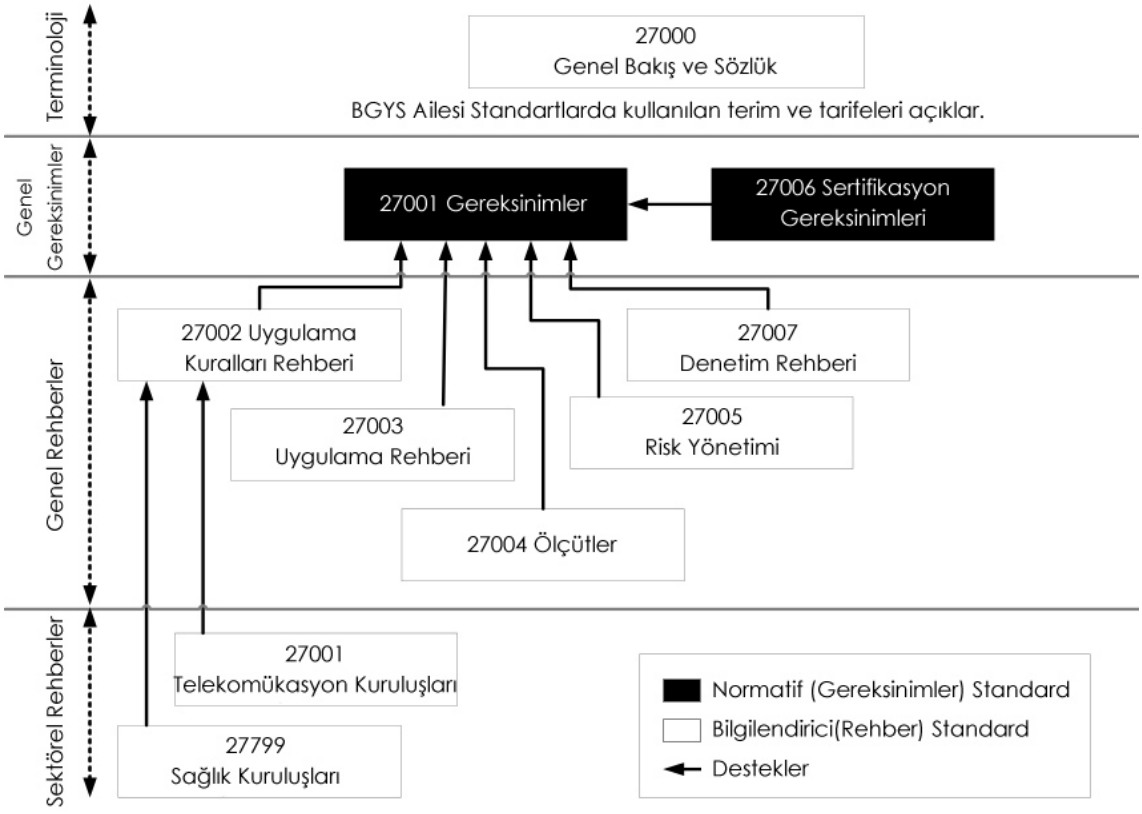
- ISO/IEC 27000:2012 – ISO 27000 serisi standartlar için sözlük, terimler ve kavramlar.
- ISO/IEC 27001:2013 – Bilgi Güvenliği Yönetim Sistemi için gereklilikler.
- ISO/IEC 27002:2013 – Güvenlik Teknikleri-Bilgi güvenliği için uygulama kodu.
- ISO/IEC 27003:2010 – Bilgi teknolojisi – Güvenlik teknikleri – 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 27009:2016 – Bilgi teknolojisi – Güvenlik teknikleri – ISO / IEC 27001'in sektöre özel uygulaması.
- 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.
- ISO/IEC 27016:2014 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği yönetimi – Örgütsel ekonomi.
- 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 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 Güvenliği – Bölüm 1 : Genel bakış ve kavramlar.
- ISO/IEC 27034-2 – Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 2 : Organizasyon normatif çerçeve.
- ISO/IEC 27034-3 -Bilgi teknolojisi – Uygulama Güvenliği – Bölüm 3 : 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 27035:2016-1 – Bilgi teknolojisi – Güvenlik teknikleri – Bilgi Güvenliği Olay Yönetimi.
- ISO/IEC 27035:2016-2 – 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 9000 standart serisinde olduğu gibi, ISO27000 serisi standartlarının sonunda bulunan 000 sayıları ile bize standardın hangi bölümde olduğunu ve önemini göstermektedir. Bu şekilde gösterilmesinin nedeni ise diğer standartlarla kendi içinde bir aile standardı olduğunun belirtilmesidir. Standart olarak 27000 – 27999 arası bilgi güvenliği standartları olarak ayrılmıştır. ISO 27001 standardı 2005 yılından sonra gelişen teknolojiler ile ortaya çıkan ihtiyaç ve tehditler doğrultusunda yeni standartlar oluşturulmuştur. Sektörlerin farklı olması nedeniyle bilgi güvenliğine duyulacak ihtiyaçlar için önceden planlama yapılmış ve buna göre yer ayrılmıştır (International Organization for Standardization, 2009).




**Şekil 6. BGYS Ailesi Standardları ve arasındaki ilişkiler**

Kaynak: ISO/IEC 27000 BGYS Genel Bakış ve Sözlük

Bu maddeler gün geçtikçe yavaş yavaş yeni standart maddeleri yerini almaktadır. Zaman içerisinde tanımlanan standartların güncel ihtiyaçlara karşılık vermemesi nedeniyle aynı standart numarası ile yeniden gözden geçilerek tekrar hazırlanmıştır. Bu nedenle standardın sonunda numarasından gelen yıllı belirtilen sayılarla değişikliğe gidildiği gösterilmektedir. Bilgi güvenliği gelişen yeni tehdit, teknoloji, açıklık ve yeni oluşan ihtiyaçlar için değişiklik yapılmaktadır. Standartlar dinamik yapılarını güncel olarak korudukları sürece zamana ve güncel tehditlere karşı koyabilmektedirler.

Bu standart; yönetim standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirildiğinden yönetim standartlarının gereklerini de yerine getirmektedir. Gereksinimleri belirtilen standartlara bakıldığı zaman ISO/IEC 27001, ISO/IEC 27006 ve ISO/IEC 27009 maddelerini kapsamaktadır. Genel kuralları açıklayan ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC TR 27008, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27016 ve ISO/IEC 27021 standart maddeleri yer almaktadır. Sektörlere göre özgü standartlara bakıldığında ise ISO/IEC 27011, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27019, ISO/IEC 27032 ISO/IEC 27035 ve ISO/IEC 27799 standartlarının yer aldığı görülmektedir. Aşağıda kurum, işletmelerin ihtiyaçlarına göre uyarlanmış, tüm kuruluşlar tarafından kullanılabilir olan bilgi güvenliği kontrollerinin uygulanmasına yönelik bazı standart maddelerinin açıklamaları bulunmaktadır (International Organization for Standardization, 2018).

## 2.2. BGYS GEREKSİNİMLERİ BELİRTEN STANDARTLAR

### 2.2.1. ISO/IEC 27001 Standardının Özellikleri

ISO/IEC 17799'un getirmiş olduğu ölçülebilirlik, tekrarlanabilirlik ve ölçeklenebilirlik gibi kavramların devamı ISO/IEC 27001 Bilgi Güvenliği Standardı bünyesinde devam etmektedir. Bu özellik sayesinde standart risklerin daha iyi bir şekilde değerlendirme, ölçülebilmesi çalışmaların istenildiği zaman tekrarlanabilmesi uygun büyüklükteki kuruluşlara veya bölüm, birimlerine uygulanması mümkün olmaktadır (Ersoy, 2012).

**Ölçülebilirlik**

Üçüncü taraflar ve denetim uzmanları tarafından değerlendirilebilen (ölçülebilen), geçerli, anlaşılır bir standart olma özelliğine sahiptir. Risklerin ölçülebilmesi ve varlıkların değerlendirilmesine imkân verebilmektedir. Tehditlerin değerleri, zayıflıkları, etkilenme durumları, risklere karşı alınacak toleransların ve tehditlerin gerçekleşme ihtimallerine karşı somut değerler oluşturulmaktadır.

**Tekrarlanabilirlik**

Yönetim sistemi bir çok kontroller kapsadığından, istenilen bölümler için istenildiği kadar tekrarlanabilmekte devamında ise planla, uygula, kontrol et ve önlem al (PUKÖ) proses yaklaşımını sunmaktadır. Bilgi güvenliği yönetim sisteminde üst yönetimin desteği ile tüm personelin belirli zamanlarda eğitim alması sonucunda risklerin gerçekleşme oranları düşmektedir.

**Ölçeklenebilme**

Yönetim sistemi öncelikle kurum içindeki belirli bölümler, birimler için geliştirilebilir ve istenildiği zaman diğer bölümler, birimlerle birlikte genişletilebilir. Uygulama sisteminden zaman içinde kaldırılan bölümler kapsam dışı bırakılabilir ve BGYS'nin kapsama alanı daraltılabilmektedir. Bu durumda kurulacak sistemin kapsamı esnek olmakla beraber tamamen işletme ve kuruluşların kararlarına bırakılmıştır. İstenildiği zaman ek denetimler eklenebilir veya azaltma imkânına sahiptirler (Ersoy, 2012)

#### 2.2.1.1. Standardın PUKÖ Yaklaşımı

Bilgi güvenliği yönetim sistemi teknik bir süreçten ziyade bir yönetim sürecidir. PUKÖ kavramı ile işletme ve kurumların bilgi güvenliğini daha faal bir şekilde uygulamak ve yönetmeyi amaçlamaktadır (Yılmaz H. , 2014). PUKÖ yaklaşımıyla, işletmeler ve kurumların, gerek duydukları takdirde standart maddelerine ilave olarak yeni denetimler uygulayabilmektedirler. BT risklerini mümkün olan en kısa sürede kaldırmayı hedeflemekte, sürekli olarak iyileştirme yöntemi olarak Planla, Uygula, Kontrol et, Önlem al (PUKÖ) döngüsünü temel almaktadır. ISO/IEC 27001 Bilgi Güvenliği Standardında bu modele göre belirlenecek olan döngünün düzenli, sürekli

aralıklarla işletmelerde, kuruluş ve kurumlarda gözden geçirilmesi gerekmektedir (Ersoy, 2012). Aşağıda bu modelin bileşenleri ve içerikleri açıklanmıştır.

**a) Planla (BGYS'nin kurulması):**

Bilgi güvenliği politikasının oluşturulması, süreçlerin, amaçların, hedeflerin ve prosedürlerin belirlenmesi gerekmektedir. Belirlenecek olan hedefler işletme, kurumun tüm hedef ve politikalarına uygun olmalıdır. Döngünün periyodik uygulanması sırasında bundan sonraki evrelerde oluşabilecek risk oranlarının düşük olması için önlemlerin önceden planlanmasını da içermektedir.

**b) Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi):**

Bilgi güvenlik politikasının, süreçler, prosedürler ve denetimlerin ayrıntılarının oluşturularak işletilmesidir. Bu işletim sürecinde ortaya çıkabilecek eksikliklerin tespit edilerek doküman, belge haline getirilmekte ve iyileştirme aşamalarına çözüm sunmaktadır.

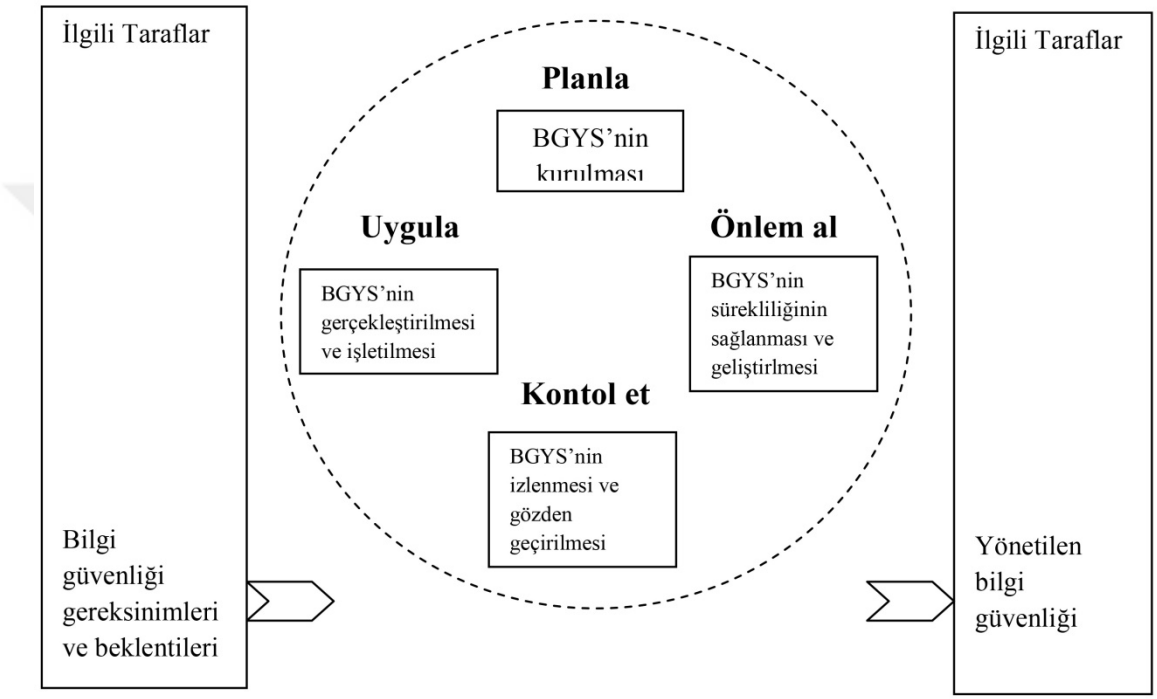
**c) Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi):**

Bilgi güvenlik politikasında alınan önlemlerin ne kadar iyi olduğunun ölçülmesi, performansın değerlendirilmesi, amaçların ve hedeflerin gözden geçirilmesi bu konuda raporların oluşturulması, ilgili sonuçların rapor edilmesidir.

**d) Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi):**

Bilgi güvenliği yönetim sisteminin, gözden geçirme sonuçlarında dayalı olarak düzeltilmesini, geliştirilmesini, önleyici faaliyetlerde bulunmak ve sürekliliğini sağlamak için gerekli tedbirlerin alınmasıdır. İşletmelerde bu aşamada fark edilen eksiklikler, güvenlik risk ve zayıflıkları bu aşamada düzeltilmektedir (Ersoy, 2012).

Bilgi güvenliği yönetim sistemleri sürekli bir gelişim, sürekli olarak devam eden bir süreç olarak düşünülmelidir. PUKÖ modelinde de olduğu gibi durmadan sürekli olarak bir döngü içinde devam etmektedir. PUKÖ modeli ne yapılması gerektiğine, nasıl karar verilmesi, verilen kararın gerçekleştirilmesi, çalıştığının kontrol edilmesi, hedefe uygun çalışmayan kontroller için önlem alınmasını sağlamaktadır (Yılmaz H. , 2014).




**Şekil 7. BGYS Proseslerine Uygulanan PUKÖ Modeli**

Kaynak: TSE, TS ISO/IEC 27001 2006:2

### 2.2.2. ISO/IEC 27006 Akredite Olarak BGYS Belgelendirme Hizmeti Verenler İçin Rehberlik.

Bilgi güvenliği yönetim sistemi sertifikasyonu, belgelendirme veren kuruluşlara rehberlik etmesi için hazırlanmış olan bu standart maddesi ISO / IEC 17021'de yer alan gerekliliklere ek olarak ISO / IEC 27001'e uygun olarak düzenlenmiştir. Standardın amacı; BGYS'ne göre belgelendirme, denetim yapan kuruluşların uyumlu olduklarını tecil etmek ve akreditasyon konusunda destek vermektir (International Organization for

Standardization, 2018). Standartta belirtilen akreditasyon süreçlerini, akredite kuruluşlar tarafından verilmiş olan ISO / IEC 27001 sertifika ve belgelendirmelerin geçerli olduğunu garanti etmektedir. Bu standart ilk olarak 2007 yılında yayınlanmış, akredite sertifikasyon süreçleri ile ilgili olarak EA 7/03 kılavuzun yerini almıştır. ISO/IEC 17021 maddesinin revize edilmesinden sonra 2011 yılında tekrar hızlı bir şekilde güncellemeye gidilmiştir. 2013 yılında ise ISO 19001 ve ISO/IEC 17021-1 maddelerinin revizyonuna paralel olarak gözden geçirilmiştir. ISO/IEC 27001'in 2013 versiyonun 2013 yılında piyasaya sürülmesinden sonra mevcut üçüncü baskı 2015 yılında yayınlanmıştır (ISO27k Infosec Management Standards, 2017). TSE tarafından ilk olarak 29.04.2010'da kabul edilmiş, 2014 ve 2015 yılında tekrar yenilenerek 05.04.2018 tarihinde tercüme edilerek yayınlanmıştır (Türk Standartları Enstitüsü, 2018).

### 2.2.3. ISO/IEC 27009 ISO/IEC 27001'in Sektöre Özel Uygulaması

ISO /IEC 27009 standart maddesine bakıldığında belirli bir sektörde (saha uygulama alanı veya pazar sektörü) olmak üzere ISO/IEC 27001'in kullanım şartlarını tanımlamaktadır. 27001 standart maddesine belirtilenlere ek olarak gerekliliklerin nasıl iyileştirmesini ISO/IEC 27001:2013 ek A'a maddesine ilave olarak kontrollerin veya kontrol setlerinin nasıl ekleneceğini açıklamaktadır. 2016 Haziran ayından yayınlanan standart için sürekliliği ve geliştirilmesi için çalışma süreci devam etmektedir (International Organization for Standardization, 2018).

## 2.3. BGYS GENEL KURALLARI AÇIKLAYAN STANDARTLAR

İşletme, kurumların genel iş riskleri durumunda bilgi güvenliği yönetim sistemlerinin oluşturulması, işletilmesi, gözden geçirilmesi, uygulanması, sürdürülmesi ve iyileştirmesi için gerekli olan standart ailesindeki bazı standartlar bir biriyle yakın ilişki içerisinde bulunmaktadır. Bu maddelerin bazıları yayınlanmış, geliştirme aşamasında olanlar ve tavsiye niteliği taşıyan standartlardır (ISO27k Infosec Management Standards, 2017).

### 2.3.1. ISO/IEC 27002 Bilgi Güvenliği İçin Uygulama Kodu

Bilgi güvenliği için uluslararası kabul görmüş olan iyi bir uygulama standartlarından biri olarak kabul edilmektedir. ISO/IEC 27002'nin geçmişine bakıldığı zaman bu konuda standartların öncüsü ve atası olan BS 7799'a dayandığı görülmektedir. Standart ilk olarak 2007 yılında kullanılmaya başlanılmış zaman içerisinde ISO yönetim sistemleri standartlarına daha uygun hale getirmek için 2013 yılında büyük ölçüde revize edilmiştir (ISO27k Infosec Management Standards, 2017). Türk Standartları Enstitüsü tarafından ilk olarak 18.12.2013 tarihinde kabul edilmiş, ilk olarak 2015 yılında tercüme edilerek yayınlanmıştır. 2015 ve 2017 yıllarında bilgi güvenliğinin devam eden gelişimi nedeniyle standart ile ilgili iptaller ve revizyonlar yapmış en son 14.03.2018 tarihinde TSE tarafından tekrar tercüme edilmiştir. Bu standart, kuruluşun bilgi güvenliği risk ortamını göz önünde bulundurarak, kontrollerin seçimi, uygulanması, yönetimi de dahil olmak üzere, kurumsal bilgi güvenliği standartları ve bilgi güvenliği yönetimi uygulamaları için rehberliği kapsamakla beraber 14 bölümde güvenlik maddelerinin toplandığı, 35 alt kontrol hedefleri ve 114 kontrol maddelerini içermektedir (Türk Standartları Enstitüsü, 2018).

### 2.3.2. ISO/IEC 27003 Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu

2010 yılında yayınlanmış olan bu standart maddesi tavsiye niteliğinde olan, özellikle yönetim sistemi konularını, kurum analizi, risk değerlendirme ve işleme planlarını yönetilmesi konularını içermektedir. ISO 27000 standartlarını uygulayanlar için rehberlik sağlamakta, başarılı tasarım ve uygulaması için kritik hususları kapsamaktadır (International Organization for Standardization, 2018). ISO / IEC 27003 standart maddesi en son 2017 yılında revizyon edilmiştir. TSE tarafından 18.02.2015 günü kabul edilmiş ve 20.03.2015 tarihinde tercüme edilerek yayınlanmıştır (Türk Standartları Enstitüsü, 2018).

### 2.3.3. ISO/IEC 27004 Bilgi Güvenliği Yönetimi Ölçme

ISO / IEC 27004 maddesine bakıldığı zaman kuruluşların, ISO / IEC 27001: 2013, 9.1'in gereksinimlerini yerine getirmek için bilgi güvenliği performansının ve bir bilgi güvenliği yönetim sisteminin etkinliğinin değerlendirilmesinde yardımcı olmayı amaçlamaktadır. Standart ilk olarak 2009 yılında yayınlanmış diğer standart maddelerinde olduğu gibi 2016 yılında revizyon edilerek tekrar yayınlanmıştır. Bu maddenin kapsamına bakıldığında ise; bilgi güvenliği performansının izlenmesi, ölçülmesi, süreçlerin, kontrolleri dahil olmak üzere bir bilgi güvenliği yönetim sistemi etkinliğinin izlenmesi, ölçülmesi, ölçüm sonuçlarının analizini ve değerlendirmesini kapsamaktadır (International Organization for Standardization, 2018).

### 2.3.4. ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi

Standart, bilgi güvenliği risk yönetimi için kılavuzlar sağlamaktadır. Ayrıca ISO / IEC 27001'de belirtilen genel kavramları desteklemekte, risk yönetimi yaklaşımına dayanan bilgi güvenliğinin uygun bir şekilde uygulanmasına yardımcı olmak üzere 2008 yılında tasarlanmış ve yayınlanmıştır (ISO27k Infosec Management Standards, 2017). Bu madde güncel gelişmeler sonucunda 2011 yılında revize edilmiştir. TSE tarafından 18.06.2014 tarihinde kabul edilmiş henüz Türkçeye çevirisi yapılmamıştır (Türk Standartları Enstitüsü, 2018).

### 2.3.5. ISO/IEC 27007 Bilgi Güvenliği Yönetim Sistemleri Denetim Kuralları

Bilgi güvenliği yönetim sisteminin iç veya dış denetimlerini yürütmek için 2011 yılında hazırlanan bu standart ISO 19001'de yer alan kılavuza ek olarak denetimlerin yürütülmesi ve denetçilerin yetkinliği hakkında rehberlik sağlamaktadır. TSE tarafından 18.12.2013 tarihinde kabul edilmiş ve İngilizce metin olarak yayınlanmıştır (International Organization for Standardization, 2018).

### 2.3.6. ISO/IEC 27008 Bilgi Güvenliği Kontrollerine İlişkin Denetçiler İçin Yönergeler

Standart kuruluşun oluşturmuş olduğu bir bilgi güvenliği uygulama standardına karşı, oluşturulmuş bir teknik rapor, teknik denetim standardıdır. Teknik uygunluğun kontrolü dahil olmak üzere bilgi güvenliği kontrollerinin gözden geçirilmesine odaklanmaktadır. Genel olarak bakıldığında ISO/IEC 27007'yi tamamlamak amacıyla 2011 yılında "Tip 2 Teknik Rapor" olarak yayınlanmıştır. Standardın bu maddesi ISO/IEC 27001 ve 27002'nin 2013 versiyonlarını yansıtmak ve geliştirmek üzere revize edilmektedir (ISO27k Infosec Management Standards, 2017). TSE tarafından ise 02.04.2015 günü kabul edilmiş ve 30.04.2015 tarihinde Türkçe 'ye çevrilerek yürürlüğe girmiştir (Türk Standartları Enstitüsü, 2018).

## 2.4. SEKTÖRLERE GÖRE HAZIRLANMIŞ STANDARTLAR

### 2.4.1. ISO/IEC 27010 Bilgi Güvenliği Sektörler Arası ve Kurumlar Arası İletişim İçin Bilgi Güvenliği Yönetimi

Bu standart kurumlar, sektörler arası iletişimde bilgi güvenliğini başlatmak, uygulamak, sürdürmek, iyileştirmek için özellikle kritik altyapıyı korumak yasal düzenleme ile etkilenen alanlar hakkında özel olarak kontrol ve rehberlik sağlamaktadır. ISO/IEC 27010 hem kamu sektörü, hem de özel sektör ile uluslararası alanda aynı sektör veya sektörler arasında her türlü bilgi paylaşımı ve güvenilir çalışma ilişkilerini sağlamak, uygun bilgi güvenliği üzerinde çalışılması için geçerlidir (International Organization for Standardization, 2018). Özellikle bir kuruluşun veya devletin kritik altyapısının güvenliğinin sağlanması, meydana gelebilecek siber saldırıların, tehditlerin önlenmesi, sistemdeki açıklar ile bakımı, korunması ile ilgili bilgi alışverişi ve paylaşımları için geçerli olmaktadır. Standart ilk kez Nisan 2012 de yayınlanmış daha sonra ISO/IEC 27001 ve 27002'nin 2013 sürümüyle uyumlu hale gelmesi için küçük değişiklikler ile yayınlanmış ve son düzenlemesi Aralık 2015'de yapılmıştır (ISO27k Infosec Management Standards, 2017).

### 2.4.2. ISO/IEC 27011 Telekomünikasyon Kuruluşları İçin ISO/IEC 27002 Standardına Göre Bilgi Güvenliği Yönetimi Sitemi Kılavuzu

ISO / IEC 27002'ye göre telekomünikasyon kuruluşlarında bilgi güvenliği kontrollerini başlatmak, uygulamak, sürdürmek ve iyileştirmek için yol gösterici bir kılavuzdur. ITU-T (International Telecommunications Union Telecommunication Standardization Sector) ve ISO / IEC JTC1 / SC 27 (ISO Uluslararası Elektroteknik Komisyonu) tarafından ortaklaşa geliştirilen standart telekomünikasyon kuruluşlarının gizlilik, bütünlük, kullanılabilirlik, erişim kontrolleri, fiziksel, çevresel güvenlik, iletişim güvenliği ve uyum konusunda Telekom kuruluşları için ek tavsiyede bir genişletilmiş kontrol setini içermektedir (International Organization for Standardization, 2018). Ağ güvenliği hakkında siber saldırıları ve ağ trafiğini kapsayan daha fazla rehberlik içermektedir. ITU-T'nin bu madde için; Küçük ve Orta Ölçekli telekomünasyon kuruluşları için güvenlik yöntemi yönergeleri ile telekom kuruluşları için iyi varlık yönetimi uygulamaları için bir rehber önerileri bulunmaktadır (International Organization for Standardization, 2018). ISO/IEC 27001 standart maddesi ilk olarak 2008'de yayınlanmış, ISO/IEC 27001 ve 27002'nin 2013 versiyonlarının daha iyi bir şekilde yansıtması için Aralık 2016'da revize edilerek yayınlanmıştır (ISO27k Infosec Management Standards, 2017). TSE teknik kurul tarafından ilk olarak 22.03.2011 tarihinde kabul edilmiş, 2016 yılında ISO tarafından revizyona uğraması nedeniyle 20.03.2017'de güncellenerek tekrar yayınlanmıştır.

### 2.4.3. ISO/IEC 27019 Enerji Endüstrisi Sektörü İçin Bilgi Güvenliği Yönetimi Sistem Kılavuzu

Bu standart maddesi, elektrik enerjisi, gaz, petrol, ısı üretimi, iletimi ve dağıtımı için enerji şirketleri endüstrisinde kullanılan elektronik, otomasyon, altyapı proses kontrol sistemlerini güvence altına almak için ISO/IEC 27002:2013'e göre belirtilen güvenlik amaçlarına, önlemlerine ek olarak enerji hizmetleri, enerji tedarikçileri tarafından kullanılan bilgi güvenliği hakkında daha fazla ve özel gereksinimleri ele alan sistemlere rehberlik sağlamaktadır. İlgili standardın kapsamına Nükleer Enerji Santralleri ve kontrol sistemleri girmemektedir (International Organization for

Standardization, 2018). ISO/IEC 27009 standardı 2013 yılında Alman standardı olan DIN SPEC 27009:2012-04'de yola çıkılarak teknik bir rapor olarak hazırlanmış ve ISO/IEC 27002'nin yapısını yakından takip etmektedir (ISO27k Infosec Management Standards, 2017). Ekim 2017 yılında ISO/IEC 27001,27002 maddelerine ve IEC TC57 standartlarının ön gördüğü şekilde revize edilmiştir. Enerji Piyasası Düzenleme Kurumu (EPDK) tarafından "Elektrik Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik" uyarınca kurulu gücü 100 MW ve üzerinde olan tesisler için 26.12.2014 tarihli ve 29217 sayılı Resmi Gazete' de yayımlanan yönetmelik değişikliği ile birlikte Elektrik, Doğalgaz, Petrol Piyasası'ndaki firmalar için ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesinin sahip olmalarının yanında ISO/IEC 27019 rehber dokümanını da referans olarak kullanılması zorunlu hale getirmiştir (CTR Uluslararası Belgelendirme ve Denetim Ltd. Şti., 2018). TSE tarafından ise 31.07.2017 tarihinde kabul edilmiş ve İngilizce olarak yürürlüğe sokulmuştur.

### 2.4.4. ISO/IEC 27032 Siber Güvenlik İçin Kılavuz

Ağ güvenliği, internet güvenliği, kritik bilgi altyapısını korumak ve siber güvenlik sorunlarını ele almak, iyileştirmek, rehberlik ve çözüm konusunda iş birliği yapılmasını sağlayan bir çerçevedir. Siber güvenliğin diğer bilgi güvenlik alanları ile ilişkilerini ve diğer standartlarla olan bağlantılarını bilgi alışverişlerini açıklamaktadır. Standardın odak noktası siber uzay ve internet güvenliği sorunlarını ele almak, yaygın güvenlik riskleri, uygulama güvenliği ve ağ güvenliği için teknik rehberlik sağlamaktadır. ISO/IEC 27001'de belirtilen kavramlar, çerçeve üzerine inşa edilmiş olan madde 2012 yılında kabul edilmiş ve yayınlanmıştır (International Organization for Standardization, 2018). Siber tehditlere karşı birey, kurum ve devletlerin tedbirlerini artırmaya ihtiyaçları vardır. Özellikle bu konuda ülkeler yasal düzenlemeler, önlemler ve siber olaylara müdahale birimleri kurulmaya başlanmıştır. Türkiye de kamu kuruluşları tarafından siber güvenlik konusu ele alınarak, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Siber Güvenlik Eylem Planları, Siber Güvenlik Müdahale Ekipleri ve Birimlerinin yanı sıra 2012 yılı içerisinde TSK bünyesinde MEBS ve Siber Savunma Komutanlığı olarak birim oluşturulmuştur (Güngör & Güney, 2017). Bu konuda ülkemizde önde gelen kuruluşlar TUBİTAK, BTK, HAVELSAN, ASELSAN, TSE gibi

kurumlar tarafından Siber Güvenlik Eğitimleri, Siber Güvenlik Tatbikatları, üniversiteler tarafından ise konferans, seminerler ve yarışmalar düzenlenmektedir.

### 2.4.5. ISO/IEC 27035 Bilgi Güvenliği İhlal Olayı Yönetimi

Bilgi güvenliği olaylarını ve zayıflıkların zamanında düzeltici önlemlerin alınabilmesi ve güvenlik açıklarının yönetim süreçlerini kapsamaktadır. Bilgi güvenliği olaylarını, ihlallerini sınıflandırarak daha önceden tanınmamış bilgi güvenliği olaylarını ihlallerini tespit etmeyi, güvenlik açıklarının kullanılmasından dolayı olumsuz etkilerini en aza indirmek, bu durumu raporlamak, analizini yapmak, ortaya çıkan bilgi ihlal olaylarından ders çıkarmak ve düzeltici kontrolleri amaçlamaktadır. Tehditlere karşı harekete geçmek için hangi sırayla olaya müdahale edilmesi gerektiği, ilk olarak tehdidi durdurmaya, kontrol altına almaya ve tehdidi yok etmeyi gerçekleştirilecek adımlar konusunda rehberlik sunmaktadır. ISO TR 18044'ün yerini alan standart maddesi ilk olarak 2011 yılında yayınlanmış, 2016 yılında ise 1. ve 2. bölüm olarak revizyona uğramıştır. 1. Bölümde bilgi güvenliği olay yönetimi destekleyen kavramları, ilkeleri özetlemekte 2. bölümde ise kuruluşun meydana gelebilecek bilgi güvenliği olaylarına uygun şekilde yanıt vermeye hazır olduğunun güvencesi ile ilgili güncellemeler yapılmıştır (ISO27k Infosec Management Standards, 2017). TSE tarafından 10.04.2013 tarihinde kabul edilmiştir. İlgili standart maddesinin henüz revizyonu yapılmış ve İngilizce metin olarak yayınlanmıştır (Türk Standartları Enstitüsü, 2018).

### 2.4.6. ISO/IEC 27799 Sağlık Sektöründe ISO/IEC 27002 Kullanımı İle Bilgi Güvenliği Yönetimi

Bu standart, sağlık hizmetleri hastaneler, laboratuvarlar, çeşitli tıbbi kuruluşlar dahil olmak üzere bilgi güvenliği yönetimi, kontrolleri ve tehdidi hakkında rehberlik sunmaktadır. Kişisel bilgilerin korunması, güvenliği kadar tüm bireyler, şirketler, kurumlar hükümetler için önemli olan bilginin, sağlık sektöründe de olduğu gibi kişisel sağlık bilgilerinin gizliliğini, bütünlüğünü, izlenebilirliğini ve kullanılabilirliğini sağlamak için karşılanması gereken özel gereksinimler bulunmaktadır (International

Organization for Standardization, 2018). Bu konu ile ilgili olarak 2008 yılında yayınlanan ISO 27799 standardı oldukça önem taşımaktadır. ISO / IEC 27002'de açıklanan kontroller için uygulama rehberliği sağlar ve gerektiğinde bunları takviye eder, böylece sağlık bilgi güvenliğini yönetmek için etkin bir şekilde kullanılabilirler. Sağlık bilgileri birçok kişi tarafından her türlü kişisel bilgilerin içinde en özel ve en gizli olarak kabul edilmektedir. Bu bilgilerin bütünlüğü, hasta güvenliğini sağlamak için mutlaka korunmalıdır, bu güvenliğin en önemli bileşeni bilginin tüm yaşam döngüsünün tamamen denetlenebilir olması sağlanmalıdır. ISO / IEC 27001 ve 27002'nin 2013 sürümlerini yansıtacak şekilde güncellenen standardın ikinci baskısı 2016 yılında yayınlanmıştır. Bu madde sağlık sektörü için "sektöre özel ve özgü" olarak çalışmalar ve araştırmaları devam etmektedir. (ISO27k Infosec Management Standards, 2017). TSE tarafından ilk olarak 09.04.2009 tarihinde kabul edilen standart, ISO tarafından revizyon edilmesinin ardından 09.12.2016 tarihinde güncellenerek İngilizce metin olarak yayınlanmıştır (Türk Standartları Enstitüsü, 2018).

# ÜÇÜNCÜ BÖLÜM
# TS ISO/IEC 27001 STANDARDI KAPSAMINDA BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN KURULMASI

Günümüzde bilginin öneminin giderek artması nedeniyle bazı işletmeler prestij, imaj, iş sürekliliği ve rekabette öne geçmek için bilgi güvenliğine yönelmişlerdir. Bunların haricinde; tehdit, riskler, daha önce gerçekleşmiş olan bilgi kaybı, kurumsal yönetim, işletmenin ihtiyaçları ve yasal süreçler sebebiyle bilgi güvenlik yönetim sisteminin kurulmasına yönelmişlerdir. ISO/IEC 27001 Bilgi güvenliği yönetim sistemi sadece bilgisayar, bilişim sistemleri ve bilgi işlemi kapsamakla beraber, bilgi casusluğu, insan kaynakları güvenliği, fiziksel güvenlik gibi her türlü bilginin güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, denetlemek, geliştirmek ve sürdürmek için risk analizi içeren süreci kapsamaktadır.

## 3.1. İŞLETMELERDE BİLGİ GÜVENLİĞİ UYGULAMALARI

ISO /IEC 27001 standardı bilginin önemli olduğu ve korunması gereken özel sektör işletmeleri, tüm kamu kuruluşların ihtiyaçlarını karşılamaktadır. Bilgi güvenliği yönetim sisteminin uygulandığı uluslararası bir standart olup International Organization for Standardization (ISO) üyesi olan tüm ülkelerde benzer hedefler için kullanıldığı görülmektedir.

**Tablo 1. Standart Kullanımı**

| Şirket Tipi | Büyüklük | Birincil Öncelik | Standardın Kullanımı |
|---|---|---|---|
| Küçük İşletme ve Organizasyon | 200 çalışandan az | Yönetimin ilgisini bilgi güvenliğine çekmek | Güvenlik konularını kapsayan TS ISO EN 27001 yönetim temel olarak alınmalıdır. |
| Orta Boy İşletmeler | 5000 çalışandan az | Uygulanabilir Kolektif güvenlik kültürü oluşturmak | Bilgi güvenliği politikası oluşturmak için uygulama içeren bir standart kullanılmalıdır |
| Büyük İşletmeler | 5000 çalışandan çok | Süreç sonunda güvenlik sertifikası almak | Şirket içi güvenlik referans belgesi için TS ISO EN 27001 kullanılmalıdır. |

Kaynak: (Pehlivan & Marttin, 2010)

Bilgi güvenliği yönetim standardı işletme, kamu kurumlarının temel öncelik, büyüklüğüne, öncelik koşullarına göre standart ile ilgili hangi kısımlarının kullanılmasını gösteren Tablo 1.'de verilmiştir (Pehlivan & Marttin, 2010).

İşletme ve firmaların risk durumları bulunduğu sektörlere göre değişiklik göstermektedir. Gıda, inşaat, tarım gibi alanlarda faaliyet gösteren firmaların düşük ölçekli; enerji, kimya, otomotiv gibi alanlarda faaliyet gösteren firmalar orta ölçekli; elektronik, biyomedikal, kamu kurumu ve savunma sanayisinde faaliyet gösteren firmalar ise yüksek ölçekte olduğu aşağıdaki Tablo 2'de gösterilmektedir (Pehlivan & Marttin, 2010).

**Tablo 2. İşletmelerin Sektörel Risk Grupları**

| **Düşük** | **Orta** | **Yüksek** |
|---|---|---|
| Tarım<br>İnşaat ve Emlak<br>Gıda ve Tütün<br>Endüstriyel Ekipman<br>Maden | Otomotiv<br>Kimya<br>Enerji<br>Nakliyat<br>Toptan Satış | Kamu Kurumları<br>Uzay Havacılık ve Savunma Biyomedikal<br>Elektronik<br>Finans ve Banka<br>Sağlık<br>Bilgi<br>Perakende<br>İlaç |

Kaynak: (Pehlivan & Marttin, 2010)

## 3.2. BİLGİ GÜVENLİĞİ YÖNETİMİ PROJE EKİBİNİN KURULMASI

Bilgi güvenliği ile ilgili çalışmaların başlatılması, desteklenmesi, doğru bir şekilde yönlendirme yapılabilmesi için işletmeler ve kurumlardaki üst yönetimin önerisi, talimatları doğrultusunda çalışmalara başlanılmaktadır. Sistemin kurulmasında üst yönetimden gelen talep, isteklerin bu konuya önem verildiğinin ve işin doğrudan desteklendiğinin bir göstergesidir (Ersoy, 2012). Bilgi güvenliği yönetim sisteminin kurulması, yönetilmesi takip edilmesi bir proje şeklinde çalışma olması sebebiyle

projenin sağlıklı yürütülmesi için bir ekibin oluşturulması ve gerekli iş bölümün yapılması gerekmektedir. Tüm bilgi güvenliği süreçlerinin oluşturulmasının ilk başlangıcı olarak bilgi güvenliği konusunda eğitim almış veya iyi eğitimli bir ekibin oluşturulması ile başlanılmaktadır (Mete, 2010).

Sistemin oluşturulması için üst yönetimin onaylamasından hemen sonra BGYS'nin çalışmalarını işletme, kurum içinde yürütmesini sağlamak amacıyla bir ekibin (Bilgi Güvenliği Grubu - BGG) kurulması gerekmektedir. Standarda bakıldığı zaman, bilgi güvenliği ekibinin kurulması forum olarak adlandırılmış, "Bilgi Güvenliği Organizasyonu (Madde A.6)" gereğince grubun kurulması ise zorunlu tutulmaktadır. Oluşturulan grupta görev dağılımı yapılmalı, bir bilgi güvenliği sorumlusu/yöneticisi ve üyeleri bulunmalıdır. Grubun sorumlusunun belirlenmesinde genellikle bilgi işlem bölümün yöneticisi bilgi güvenliği gurubunun başkanı olmaktadır.

Bilgi işlem yöneticisi aynı zamanda grupta üst yönetimi veya yönetim kurulunu temsil edecek olan yönetim temsilcisi olarak tanımlanmakta ve üst yönetim namına BGYS dokümanlarını yayınlamakta, onaylamakta, mevcut risklerin kabul seviyelerini belirlemektedir. Üst yönetimin kararlılığının, desteğinin tüm işletme, kurumda hissettirilmesi için, BGYS politikalarına destek verdiğini açıkça beyan edilmesi ve yayınlaması gerekmektedir. İşletme, kurumların kendi içinde BGYS oluşturmanın ilk başlangıcı olarak iki konuya dikkat etmesi gerekmektedir. Bu konular bilgi güvenliği yönetim sisteminin kurulma nedeni, amacının belirlenmesi ve işletme, kurum içerisinde uygulanacak BGYS'nin hangi bölümlerinin ele alınacağına karar verilmesidir (Ersoy, 2012).

### 3.3. BİLGİ GÜVENLİĞİ YÖNETİMİ KAPSAMININ BELİRLENMESİ

Kapsamın oluşturulması proje ekibinin tavsiyesi, yönetim kurulu kararları ve ISO/IEC 27001 standardın yönergesi doğrultusunda bilgi güvenliği yönetim sisteminin uygulama kapsamının/alanının belirlenmesi, varlık envanteri, risk analizinin yapılması

gerekmektedir. İşletme, kurumlarda kapsamın belirlenmesinde tüm bölüm/alanların dâhil edileceği gibi, öncelikle sadece acil önem taşıyan kritik alanlarda uygulanmasının yanında sınırlarının genişletileceği veya daraltılmasını mümkün kılmaktadır. BGYS kurulumu kapsamı tanımlanırken en geniş şekilde hazırlandığı halde uygulama ve kontrollerde ortaya çıkabilecek problemler kapsamda değişikliklere sebep olacaktır (Ersoy, 2012).

BGYS çalışmasında kapsamın içinde yer alan süreçlerin ortaya konulması ve örneklendirilmesinden sonraki, adım varlık envanterinin oluşturulmasıdır. Süreçleri oluşturan yapıtaşların varlıklar olması nedeniyle süreçlerin belirlenmesi, yazılı halde olması varlıkların daha sağlam ve eksiksiz belirlenmesini sağlayacaktır (Yılmaz H. , 2014). İşletme, kurumların bilgi varlıkları birçok şekilde bulunmaktadır. Bu varlıklara bakıldığı zaman yazılımlar, veri tabanları, donanımlar, uygulama yazılım kodları, iş akış şemaları, ağ ekipmanları, kâğıt dokümanlar, kıymetli evraklar, çek, hisse senetleri, fiziksel varlıklar (fotokopi, telefon, faks cihazı vb.) çalışanlar vb. şekilde olabilmektedir. İşletmelerin varlıkları sayıları, kurumun faaliyet alanlarına, yapılarına ve önem derecesine göre değişiklik göstermektedir (Ersoy, 2012).

Oluşturulan kapsamın durumu sıkça değişmek zorunda olmadığı halde yaşayan bir dokümandır. Gerekirse kapsamın içeriği değiştirilebilmekte, fakat faaliyet alanı ilk aşamada tanımlanırken yönetilebilir boyutta olması önemlidir. Bu nedenle organizasyonun fiziksel yapısı ve yöntemleri göz önünde bulundurulmalıdır. Örnek olarak az olmasına karşın yönetmek adına çok büyük kuruluşlarda yazılım geliştirme ve finans bölümü için iki ayrı bilgi güvenliği yönetim sistemi oluşturulduğu örneklerde mevcut bulunmaktadır (Perendi, 2008).

Kapsam oluşturulmasında amaç ve kapsam net bir şekilde ilk madde olarak yazılmalıdır. Sonraki aşamada organizasyon yapısının görsel, çizimler şeklide anlatılması gerekmektedir. Kurum, işletmenin merkez, şube, depoların açık adresleri ile

belirtilmesinin yanında teknoloji ve kısaca varlıklar genel hatlarıyla belirtilmelidir (Mete, 2010). Örnek BGYS kapsam dokümanı EK1'de verilmiştir.

### 3.4. VARLIKLARIN BELİRLENMESİ, SINIFLANDIRILMASI VE ENVANTERİNİN OLUŞTURULMASI

Kurum, kuruluş, işletmelerin sahip olduğu, ticari etkinliğini sürdürebilmesi için gerekli, önemli olan varlık; donanım, yazılım, teknik altyapı, evrak ve personelden vb. oluşmaktadır. İşletmenin, kurumun çalışmasını sağlam devam etmesi için, faaliyetleri sırasında ürettiği, sektörel veya ticari ilişkiler sürdürdüğü kurum, işletmelerden elde ettiği bilgiler, varlıkların güvenliğinin sağlanması için elektronik ortamda bulunan, bulunmayan değerli bilgilerin bulunduğu sistemlerin, ortamların birer bilgi varlığı niteliğinde olması nedeniyle standardın getirmiş olduğu zorunluluktan dolayı envanterler oluşturulmalıdır (Ersoy, 2012).

Risk analizi çalışmasının sağlam bir biçimde yapılabilmesi, bilginin etkili bir şekilde korunmasını sağlamak için bilgi varlıklarının da olduğu tüm varlıkların envanterinin hazırlanması ve sınıflandırılması gereklidir. Varlık envanterinin doğru şekilde oluşturulması, varlıkların önemi ve değeri hakkında bir fikir verecektir. Envanter hazırlandıktan sonra BGYS kurmuş, bir organizasyonda varlık envanterinden sorumlu kişinin ve envanterin bulunduğu yerin belirtilmesi gerekmektedir (Koç, 2008).

Yönetim tarafından atanan proje ekibi, işletme, kurumun ana iş süreçlerini bilgi varlıklarını ve fiziki varlıkların korunması için ne kadar kritik olduğunun analizi yapılmalıdır. Analiz sonucunda fiziksel varlıkların envanteri tüm paydaşlar dâhil hangi bilgilerin korunması gerektiği açıklığa kavuşturulmalı ve belgelendirilmelidir. Varlık envanteri için atanacak olan sorumlu sadece BGYS kapsamındaki ürün, hizmet, süreç ve varlıkları dikkate almalıdır. Her işletmenin varlığına ilişkin mevcut güvenlik durumunu belirlemek için risk analizi gereklidir. Bu analizin BGYS kurulmadan önce başlangıçta yapılması, mevcut güvenlik durumu ile BGYS gereklilikleri, beklentileri

arasındaki boşlukları doldurmak amacıyla gerekli güvenlik önlemlerin alınması, belirlenmesi önerilir (Ceauşu, Ilie, & Ionescu, 2018).

İşletme, kuruluştaki varlık envanteri oluşturmada izlenecek olan varlıkların belirlenmesi, varlıklara değer atanması risk analizi yöntemi için temel bir başlangıçtır. Varlıkların değerlerinin belirlenebilmesi için bir envanter bilgisine ihtiyaç vardır. İşletme ve kuruluşlarda envanterden kasıt ilk akla gelen bir çeşit zimmet listesidir. BGYS kurulum aşamasında başlangıç noktası olarak zimmet listesinden başlanılması özellikle yazılımsal, donanımsal ve fiziksel varlıklar için faydalı olmaktadır. Fakat bazı durumlarda sistemin kurulması için yeterli, gerekli ayrıntıya sahip olmayabilir, BGYS için mühim olan bilgi varlıklarının belirlenmesinde yetersiz kalabilmektedir. Bu nedenle işletme, kuruluş içerisinde bir varlık yönetim kılavuzu veya varlık envanter yönetim kılavuzu hazırlanmasında yarar vardır. Hazırlanacak olan kılavuzda ayrıntılı olarak yeni bir varlığın eklenmesi, envanterden çıkarılması ve envanter ile ilgili sorumlu kişi net olarak belirtilmelidir. Varlık dökümü hazırlanırken öncelikle bütün varlıkların dâhil edildiğinden emin olunması için gruplandırma yapılması varlıkların tanımlanmasını kolaylaştıracaktır. Gruplandırma bilgi varlıkları, fiziksel varlıklar, yazılım varlıkları, personel bilgi varlıkları, servisler vb. şeklinde olmalıdır (Koç, 2008).

Örnek olarak kapsam dâhilinde bir bilgi işlem birimi incelendiğinde bu birimin kontrolü altında bulunan varlıkların oluşturulmasında; uygulama yazılımları, bilgi sistemleri varlıkları, donanımlar, hizmet yazılımları ve bilgi varlıkları olarak bölümlere ayrılabilmektedir. İşletmeler örnekte olduğu gibi bir ayrım yapma konusunda bir zorunlulukları bulunmamaktadır. Bu sınıflandırmalar işletmenin yapısına, büyüklüğüne göre istediği biçimde ve şekilde sınıflandırma yapabilmektedir (Ersoy, 2012).

Tablo 3'de donanım varlıklarının kritiklik ve gizlilik derecelendirmesi konusunda değerlendirme seviyelerinin puanlama çalışması örnek olarak verilmiştir. Donanım varlıkları için; bilgisayarlar, sunucular, yazıcılar, dizüstü bilgisayarlar ve güç kaynakları (UPS) vb. şeklinde örneklendirme yapılabilir.

**Tablo 3. Donanım Varlıklarının Gizlilik Dereceleri ve Kritiklik Referans Tablosu**

| DONANIMLAR | DEĞERLENDİRME SEVİYELERİ |
|---|---|
| **Kritiklik (Erişilebilirlik + Bütünlük)** | Donanımla ilgili kritik durumu üç seviyede belirlenir; Düşük, Orta, Yüksek<br><br>**Düşük:** Bu ekipmanın kapalı olması halinde sistem güvenliği etkilenmez. Sistem çoğu fonksiyonları ile çalışmaya devam eder. Düşük kritiğe sahip bir ekipmanın iki güne kadar kapalı kalması kabul edilebilir. **Kritik derecelendirilme puanı 1'dir.**<br><br>**Orta:** Bu ekipmanın kapalı olması halinde, sistem çalışmaya devam eder fakat sistemin bir kısmı hasar görmüş olabilir. Orta kritiklik derecesine sahip olan bir sistemin yirmi dört saate kadar kapalı kalması kabul edilebilir. **Kritik derecelendirme puanı 3'tür.**<br><br>**Yüksek:** Bu ekipmanın kapalı olması tüm sistemin devre dışı olmasıdır. İş devamlılığı ve sistem güvenliği tehlikeye girer. Yüksek kritiklik derecesine sahip olan bir sistemin bir saate kadar kapalı kalması kabul edilebilir. Sistem bütünlüğünü sağlamak çok önemlidir. **Kritik derecelendirme puanı 5'dir.** |
| **Gizlilik Derecesi** | Bu ekipman üzerindeki bilgilere yetkisiz erişim olduğunda gizliliğin derecesi sistem güvenliğinin tehlikeye girdiği duruma göre belirlenir. Gizlilik derecesi 3 seviyedir:<br><br>**Önemsiz Gizlilik:** Bu gizlilik seviyesindeki bir ekipmana ait erişim bilgilerinin ortaya çıkması iş sürekliliğini ve sistem güvenliğini etkilemez. **Gizlilik puanı 1'dir.**<br><br>**Gizli:** Bu gizlilik seviyesindeki bir ekipmana ait erişim bilgilerinin ortaya çıkması durumunda sistem güvenliği için tehlike oluşturmaz, fakat sadece bu ekipmana yetkisiz kişilerin erişimine açık hale gelir ve zafiyet yaratabilir. **Gizlilik puanı 3'dür.**<br><br>**Çok Gizli:** Bu gizlilik seviyesindeki bir ekipmana ait erişim bilgilerinin ortaya çıkması durumunda yetkisiz kişilerin sisteme erişmesi mümkün hale gelir. Bilgi güvenliği ve sistem tamamen tehlikeye girer. **Gizlilik puanı 5'dir.** |

Kaynak: (Ersoy, 2012)

Tablo 4'de ise kullanılan uygulama yazılım varlıklarının kritiklik ve gizlilik derecelendirmesi konusunda değerlendirme seviyelerinin puanlama çalışması örnek

olarak verilmiştir. Yazılım varlıkları için örnek ; genel olarak kullanılmakta olan bordro takip, muhasebe programları gösterilebilir.

**Tablo 4. Yazılım Varlıklarının Gizlilik Dereceleri ve Kritiklik Referans Tablosu**

| YAZILIMLAR | DEĞERLENDİRME SEVİYELERİ |
|---|---|
| **Kritiklik (Erişilebilirlik + Bütünlük)** | Yazılımla ilgili kritik durumu üç seviyede belirlenir; Düşük, Orta, Yüksek<br><br>**Düşük:** Bu yazılımın kapalı olması halinde sistem güvenliği etkilenmez. Sistem çoğu fonksiyonları ile çalışmaya devam eder. Düşük kritiğe sahip bir yazılımın iki güne kadar kapalı kalması kabul edilebilir. **Kritik derecelendirilme puanı 1'dir.**<br><br>**Orta:** Bu yazılımın kapalı olması halinde, sistem çalışmaya devam eder fakat uygulamaların bir kısmı hasar görmüş ve kısa süreli olarak devre dışı kalabilir. Orta kritiklik derecesine sahip olan bir sistemin kırk sekiz saate kadar kapalı kalması kabul edilebilir. **Kritik derecelendirme puanı 3'tür.**<br><br>**Yüksek:** Bu yazılımın kapalı olması tüm iş devamlılığını büyük ölçüde aksatır ve etkiler. Yüksek kritiklik derecesine sahip olan bir yazılım bir saate kadar kapalı kalması kabul edilebilir. Yazılım bütünlüğünü sağlamak çok önemlidir. **Kritik derecelendirme puanı 5'dir.** |
| **Gizlilik Derecesi** | Bu yazılımın kullanımı yetkisiz kişilerin erişiminde olduğu zaman gizliliğin derecesi sistem güvenliğinin tehlikeye girdiği duruma göre belirlenir. Gizlilik derecesi 3 seviyedir:<br><br>**Önemsiz Gizlilik:** Bu gizlilik seviyesindeki bir yazılıma yetkisiz erişimin olduğu zaman iş sürekliliğini ve sistem güvenliğini etkilemez. **Gizlilik puanı 1'dir.**<br><br>**Gizli:** Bu gizlilik seviyesindeki bir yazılıma yetkisiz erişimin olduğu zaman bilgi güvenliği için tehlike oluşturmaz, fakat sadece bu yazılım yetkisiz kişilerin erişimine açık hale gelir ve zafiyet yaratabilir. **Gizlilik puanı 3'dür.**<br><br>**Çok Gizli:** Bu gizlilik seviyesindeki bir yazılıma yetkisiz erişim olduğunda kontrolün yetkisiz kişiler tarafından kullanılması durumunda bilgi güvenliği tamamen tehlikeye girer. **Gizlilik puanı 5'dir.** |

Kaynak: (Ersoy, 2012)

Tablo 5'de ise bilgi varlıklarının kritiklik ve gizlilik derecelendirmesi konusunda değerlendirme ve puanlama çalışması örnek olarak verilmiştir. Bilgi varlıklarına bakıldığında veri tabanında bulunan bilgiler, kâğıt ortamındaki sözleşmeler, şartnamelerden oluşabilmektedir.

**Tablo 5. Bilgi Varlıklarının Gizlilik Dereceleri ve Kritiklik Referans Tablosu**

| BİLGİ VARLIKLARI | DEĞERLENDİRME SEVİYELERİ |
|---|---|
| **Kritiklik (Erişilebilirlik + Bütünlük)** | Bilgi varlıkları ile ilgili olarak kritik durumu üç seviyede belirlenir; Düşük, Orta, Yüksek<br><br>**Düşük:** Bu varlığın kullanım dışı olması halinde bilgi güvenliği ve sistem etkilenmez. Sistem bütün fonksiyonları ile çalışmaya devam eder. Düşük kritiğe sahip bir varlığın iki güne kadar kapalı kalması kabul edilebilir. **Kritik derecelendirilme puanı 1'dir.**<br><br>**Orta:** Bu varlığın kullanım dışı olması halinde, sistem çalışmaya devam eder fakat uygulamaların bir kısmı hasar görmüş ve kısa süreli olarak devre dışı kalabilir. Orta kritiklik derecesine sahip olan bir sistemin sekiz saate kadar kapalı kalması kabul edilebilir. **Kritik derecelendirme puanı 3'tür.**<br><br>**Yüksek:** Bu varlığın kullanım dışı kalması tüm iş devamlılığını büyük ölçüde etkiler ve durdurur. Sistem hiçbir şekilde kullanılamaz hale gelir. Bu nedenle bazı yasal yükümlüklerin yaptırımlarıyla karşılaşılır. Yüksek kritiklik derecesine sahip olan bir varlık (bilhassa veri tabanları) bir saate kadar kapalı kalması kabul edilebilir. **Kritik derecelendirme puanı 5'dir.** |
| **Gizlilik Derecesi** | Bu varlığın kullanımı yetkisiz kişilerin erişiminde olduğu zaman gizliliğin derecesi sistem güvenliğinin tehlikeye girdiği duruma göre belirlenir. Gizlilik derecesi 3 seviyedir:<br><br>**Önemsiz Gizlilik:** Bu gizlilik seviyesindeki bir varlığa yetkisiz erişimin olduğu zaman iş sürekliliğini ve sistem güvenliğini etkilemez. **Gizlilik puanı 1'dir.**<br><br>**Gizli:** Bu gizlilik seviyesindeki bir varlığın bilgilerinin ortaya çıkması durumunda yetkisiz erişimin olduğu zaman bilgi güvenliği için tehlike oluşturmaz, fakat sadece bu bilgi varlığına yetkisiz kişilerin erişimine açık hale gelir ve zafiyet yaratabilir. **Gizlilik puanı 3'dür.**<br><br>**Çok Gizli:** Bu gizlilik seviyesindeki bir varlık kesin olarak yetkisiz kişilerin eline geçmemesi gerekir. Bu durumda bilgi güvenliği ve sistem tamamen tehlikeye girer. **Gizlilik puanı 5'dir.** |

Kaynak: (Ersoy, 2012)

Oluşturulacak varlıklar ile ilgili olarak bu tip bir ayrım yapmak zorunlu değildir, işletme, kurumlar kendi yapılarına göre istenilen biçimde sınıflandırma yapabilmektedirler. Yapılan çalışmalar sonucunda elde edilen bilgiler sırasıyla donanımlar, uygulama yazılımları ve bilgi varlıklarına ait olmak üzere tablolar oluşmaktadır. Varlık oluşturma (envanter) çalışmaları kapsamındaki varlıklar; uygulamam yazılımları, hazır hizmet yazılımları, donanımlar ve bilgi varlıkların düzenlenmesi, tasnif edilmesi, standart varlıkları sınıflandırma ilkesine göre (Varlık Yönetimi – Madde A.7) maddesine göre sınıflandırma yapılarak gizlilik seviyeleri belirlenmektedir (Ersoy, 2012).

İşlemelerde varlıkların değerinin belirlenmesi risk analizinde bir temel başlangıçtır. Varlıkların tümü belirlendikten sonraki aşamada ise varlık için değer atama yapılabilmesi için kriterlerin belirlenmesi gereklidir. Birden çok varlık çeşitlilikleri olduğunda değer belirlenme kriterleri işletmeden işletmeye değişiklik gösterebilir. Bazı varlıkların değeri nicel şeklinde belirlenirken (rakamla derecelendirme yapılarak), bazıların değerini ise nitel tanımlamalar (düşük, çok yüksek vb.) kullanılmaktadır. Nitel değerlendirmede; ihmal edilebilir, çok düşük, düşük, orta, yüksek, çok yüksek, kritik şeklinde derecelendirme yapılabilmekte, bu durum işletmenin güvenlik ihtiyaçlarına göre değişebilmektedir. Nicel şeklinde değerlendirmeler işletmenin ihtiyacına ve büyüklüğüne göre 5-7 derecelendirme kullanılabilirken daha küçük işletmeler için 3-4 derecelendirme seviyesi kullanılabilmektedir (Koç, 2008).

Varlık çizelgeleri hazırlanırken her varlık için farklı farklı sütunlarda, standartta belirtilen gizlilik, bütünlük ve kullanılabilirlik (erişilebilirlik) nitelikleri dikkate alınarak, bu varlık için bir sayısal değeri bulmaya çalışılır. Varlık değerlendirmeleri için genel olarak 1'den 5'e kadar puanlama yapılmakta, işletme/kurum için varlık ne kadar önemli ise, verilen puanların derecesi büyük olmalıdır (Ersoy, 2012). Varlık Tablosu (Tablo 6) ile ilgili olarak "B" varlığının derecelendirmesi gizlilik=4, bütünlük=3, kullanabilirlik=5 olarak değerlendirme yapılırsa B varlığının değeri 5*3*4= 60 olacaktır.

**Tablo 6. Varlıklar Tablosu**

| Varlık | Konumu | Sorumlusu | Yetkili Personel | Gizlilik | Bütünlük | Kullanılabilirlik | Varlık Değeri |
|---|---|---|---|---|---|---|---|
| A | 3. Kat Oda 333 | Bilgi İşlem Şubesi Şb. Bşk. | Şube Başkanı | 5 | 5 | 5 | 125 |
| B | 1. Kat Oda 113 | Bilgi İşlem Müdürü | Sistem Sorumlusu | 4 | 3 | 5 | 60 |
| C | ….. | ….. | ….. | 5 | 2 | 4 | 40 |
| D | ….. | ….. | ….. | 1 | 2 | 3 | 6 |

Kaynak: (Ersoy, 2012)

Tablo 6'deki A varlığı için; gizlilik, bütünlük, kullanılabilirlik değerlerine bakıldığında varlıkla ilgili olarak bilgi güvenliğinden en küçük bir ödün bile verilmediği görülmekte ve bu nedenle işletme için çok büyük bir önem taşımaktadır. A varlığının erişime kapanması, gizliliğinin ihmal edilmesi ve bütünlüğünün kaybolması durumunda varlıkla ilişikli olan tüm işlemlerin durmasına sebep olacaktır. Çoğunlukla bu durumda en yüksek puan alan varlıklar, işletmelerin tüm bilgilerin bulunduğu veri tabanları ve sunucular olduğudur. Her işletme veya kurum tablodaki derecelendirmeyi istedikleri gibi (örnek olarak 1-10 arasında) puanlama yapabilirler. Yukardaki tablo işletme, kurum ve kuruluşlar için fikir vermesi için Tablo 6'de örnek verilmiştir.

Bilgi sistemleri varlıklarının değerinin belirlenebilmesi için örnek tabloda olduğu gibi;

Varlık Değeri = Gizlilik x Bütünlük x Kullanabilirlik

formülü ile hesaplanabilmektedir (Ersoy, 2012).

## 3.5. BİLGİ GÜVENLİĞİ POLİTİKASININ OLUŞTURULMASI

Bilgi güvenliği politikaları, bir kuruluşun, işletmenin değerli bilgilerinin yönetimini, muhafaza edilmesi, dağıtımını, önemli görevlerin korunmasını düzenleyen kural ve uygulamadır (Tuğlular, 2003). Bilgi güvenliği yönetim sistemi politikası yönetime yön veren, hedefleri ortaya koyan, harekete geçiren, meydana gelebilecek risklerin değerlendirileceği ve yönetileceğine ilişkin kapsam, kriterlerini belirten bir yapı olmalıdır. BGYS politikasının hedeflerine ulaşabilmesi için yönetim kurulu politika kapsamındaki maddelerin uygulamaya geçirileceğinin ve bu konudaki kararlılıklarını çalışanlara hissettirmelidir (Önel & Dinçkan, 2007). Bilgi güvenliği politikası işletmenin, kurumun bilgi güvenliği ihtiyaçlarını ve bilgi güvenliği kavramını işletmenin, kurumun bilgi kaynaklarını kullanan her kişiye anlatılmak için hazırlanmalıdır. İşletme, kurumun bilgi güvenliği gereksinimleri, işletmenin yaptığı işin sonucunda ortaya çıkmış veya ilgili kanunlar, yönetmelikler sonucunda belirlenmektedir. Bu nedenle iş gereksinimleri ve yasal yükümlülükler bu dokümanda net bir biçimde yer almalıdır (Öztürk, 2008). İşletme, kurumun tüm süreç, kademesini kapsayan, her konuda genel bir bilgi güvenliği politikaları oluşturulmalıdır. Ancak bu politikalar bir genel bilgi güvenliği politikası hazırlandıktan sonra biçimlendirilmelidir. Yan konular ve alt bölümler için hazırlanacak politikalar daha detaylı, teknik konuları içerecek özellikte olmalıdır. Bilgi güvenliği politikası ile ilgili olarak ISO/IEC 27001 standardının A.5.1. maddesinde olan BGYS Kontrolleri Gerçekleştirilmesi ve Denetlenmesi Kılavuzunda belirtildiğine göre; bilgi güvenliği politikalarında aşağıdaki hususların yer alması uygun olacaktır (Humphreys & Plate, 2005).

a) Bilgi güvenliğinin genel kapsamı, tanımı ve hedefi,
b) Bilgi güvenliğinin işletme, kurum için ne kadar değerli olduğu, bilgi güvenliğinin oluşturulmasının hedefi ve bilgi güvenliğinin hedef ve ilkeleri için yönetimin desteği,
c) Kontrollerin seçimi ile birlikte kontrollerin hedefleri için risk değerlendirme ve risk yönetimini de içeren taslağın ortaya konulması,
d) Güvenlik ilkeleri, standartları, politikaların ve uyum ihtiyaçlarının özet bir açıklaması,
e) Bilgi güvenliği ile ilgili olarak tüm sorumluluk ve görevlerin tanımı,

f) Diğer ayrıntılı politika ve özel bilgi sistemleri ve işlemlerle ilgili kullanıcının izlemesi gereken kurallar, bu kuralları, politikayı destekleyen dokümanlara atıflar.

Bilgi güvenliği politikası bilgi güvenliğini işletmede ve kurumda yön verici temel bir doküman olmasının yanında, işletmenin, kurumun, personeli, iletişimde olduğu tüm paydaşları tarafından ulaşılabilen ve tanınan bir doküman olmalıdır. Bu sebeple politika yazılırken dikkat edilmesi gereken ilk konu, politikanın mümkün olduğu kadar kısa ve kolay anlaşılır olması gereklidir. Yazılan politika çok uzun olduğu zaman kurum, işletme kullanıcıları tarafından okunmayacak, bu durumun göze alınarak, bilgi güvenliğine politikasına ilave olarak, tamamen işletme ve kurum kullanıcılarını hedefleyerek bilgi güvenliği politikasının özet bir sürümü hazırlanabilir. Bu nedenle kullanıcıların tüm politika dokümanını okumaları ve kendilerinden ne beklenildiğini daha iyi anlamları mümkün olmaktadır (Öztürk, 2008).

### 3.6. RİSK YÖNETİM SÜRECİ

Risk yönetimi bilgi güvenliği yönetimi kurulum aşamaları içerisinde önemli bir yere sahiptir. İşletme, kurum yapısal durumlarına göre ve yasal bağlılıkları dikkate alarak ISO 27001, COBIT, ITIL gibi kabul görmüş uluslararası standartlarca desteklenen, onaylan bilgi güvenliği yönetim sistemini benimsemeli, uygulamalıdır (Şahinaslan, Kandemir, & Kantürk, 2010). Bilgi güvenliği aslında bir risk yönetim süreci olmakla beraber, bu sürecin sürekli ve sürdürülebilen bir süreç olması gereklidir. İşletme, kurumun her geçen gün değişen teknoloji, değişken ortamların sonucunda riskler sürekli olarak değişmekte bunun sonucunda yeni riskler sürekli olarak ortaya çıkmaktadır. Bu nedenle bilgi kaynaklarının riskleri, tehditleri ve zayıf yönleri düzenli olarak gözden geçirilmelidir. Bu yapılan işlemler bilgi güvenliği yönetim sisteminin temelini oluşturmaktadır (Djapić & Lukić, 2007). Risk analizinin oluşturulmasındaki amaç; bilginin karşılaşabileceği tehditlerin, risklerin tespit edilerek, bu risklerin makul bir seviyeye düşürmek üzere karşı önlemlerin tespit edilmesidir. Gerekli tespitlerden sonra bir plan dâhilinde bu önlemlerin alınması ve uygulanması gereklidir. Yapılacak analizlerin sonucunda yeni yatırımlara ihtiyaç duyulacağı gibi, yalnızca basit bir takım

kuralların uygulanması sonucunda masrafsız bazı önlemler alınmış olacaktır (Ersoy, 2012). İşletmelerde, kurumlarda bilgi güvenliğinin oluşmasında ki ana şarttan biri de risk analizleridir. Yapılacak olan güvenlik risk analizi; işletmenin, kurumun karşılaşabileceği olası güvenlik risklerini ortaya çıkararak, işletmenin, kurumun önceliklerinin ortaya çıkarılması, tehditlerin tespit edilerek, risklerin ortadan kaldırılması, bilgi güvenliğini sağlamak oldukça çok önemlidir (Çek, 2017).

### 3.6.1. Risk Analizi

Risklerin belirlenmesi, değerlendirme çalışmalarında risk analizi geniş bir alanı kapsamaktadır. İşletme, kurumun sistemin esaslarını etkileyecek belirsiz olayların tanımlanması, denetlenmesi, ortadan kaldırılması veya en aza indirmeyi amaçlayan süreç olarak tanımlanmaktadır. Bu süreçte uygulama, test etme, fayda maliyet analizi, seçim, öncelik sıralaması, önlemlerin güvenlik değerlendirmesi gibi bütün güvenlik denetimlerini içerebilir (Kumaş, 2009). Risk analizi ISO/IEC 27001 standardında kaynakları tanımlamak, riskleri öngörmek için bilginin sistematik kullanımını tanımlanmıştır. Risk analizi kapsamın belirlenmesi ile birlikte süreç başlamaktadır. Tanımlanan kapsamda yer alan varlıklar belirlendikten sonra, güvenlik açıkları, tehditler ve mevcut kontroller belirlenmektedir. Daha sonraki aşamalarda olasılık değerlendirmesi ve analizleri yapılır. Son olarak tespit edilen riskler derecelendirilerek belgelendirilir (Eskiyörük, 2007). Varlığın önem seviyesini tespit etmek için; bu varlığın bütünlük, gizlilik ve kullanılabirliğinde oluşabilecek zararın işletme, kurumda oluşturacağı etkinin seviyesini baştan ortaya konulması gereklidir. Varlıkların bu üç temel güvenlik özelliklerine gelecek zararlar farklı etki seviyelerine sahip olabilir. Örnek olarak çok gizli seviyede olan bir bilginin ortaya çıkması işletmeye, kuruma büyük zarar verebilirken, aynı gizli bilginin kulanım dışı kalması o kadar büyük zararlar yaratmayabilir (Önel & Dinçkan, 2007). Başka bir ifadeyle, varlığın korunması için alınacak önlemlerin maliyeti ile tehdit nedeniyle etkilenecek olan varlığın devre dışı kalması sebebiyle işletmenin, kurumun maddi ve manevi açıdan uğrayacağı zararlar arasında önemli bir ilişki olmasıdır. Kayıpların hangilerinin olabileceği belirlenirken, sadece varlıkların maddi değerinin dikkat alınması yanıltıcı bir yol olacaktır. ISO/IEC 27001 standardında risk değerlendirilmesinde dikkat edilmesi gerekenler;

a) Varlıkların bütünlük, gizlilik ve sürekli kullanılabilme özelliğinin kaybedilmesi ile meydana gelebilecek işin aksamalarını ve iş kayıplarının belirlenmesi
b) Zayıflıklar ve tehditlerin yapılan kontroller sonucunda, varlıklar ve yöntemler üzerinde hangi olasılıkla daha etkili olabileceğinin gerçekçi bir tanımın yapılmasıdır (Ersoy, 2012).

### 3.6.2. Risk Analiz Kapsamın Belirlenmesi

Risklerin analizindeki ilk başlangıç kapsamın belirlenmesidir. İlk aşamada kapsamın işletmenin, kurumun hedeflerine uygun, doğru olarak belirlenmesi gereksiz emek harcanmasını önleyerek risk analizinin kalitesini artırmaktadır. Risk analizine dair her şey kapsamda net olarak belirlenmelidir (Eskiyörük, 2007). Kapsamın netleştirilmesi BGYS'nin sınırlarının açıkça tanımladığı anlamına gelmektedir. Bilişim teknolojileri alt yapı sınırlarını da içermelidir. İşletme, kurum fiziksel konumların yanı sıra kritik verilerin yerlerini de belirlemelidir. Dış tedarik işbirliği içinde olan kişi ve kuruluşlarında kapsam belirleme süreci içerisinde dikkate alınmalıdır (Ceauşu, Ilie, & Ionescu, 2018). Örnek olarak bir kapsam şu şekilde olabilir. "Risk analizi işletmenin, kurumun servis hizmetlerinde kullanılan tüm yazılım, donanım ve personeli kapsamaktadır." Bu nedenle servis hizmetlerinde kullanılan, yazılım, uygulamalar, bilgisayarlar, sunucular, işletim sistemleri ve tüm bunları kullanan, yöneten personelinde risk analizi içerisinde yer alması gereklidir (Eskiyörük, 2007).

### 3.6.3. Risk Varlıklarının Belirlenmesi

Varlık, işletmenin, kurumun sahip olduğu maddi değerler gibi, imaj, tecrübe, bilgi gibi maddi olmayan değerlerden oluşmaktadır. Tüm işletme ve kurum için ilk olarak mevcut varlıkların tespiti ile oluşturulan varlık tablosundan sonra ihtiyaçlar belirlenir. Mevcut varlıkların bilinmesi risk analizinin daha doğru ve kolay yapılmasını sağlayacaktır (Koç, 2008). İşletme, kurum için önem taşıyan her varlığın güvenliğinin sağlanması için gerekli olan çalışmanın amacı oluşturulmakta, bütün varlıkların korunması hedeflenmektedir. Bu nedenle ilk olarak varlıkların envanterini açık bir şekilde sıralamak ve sınıflandırılması gerekmektedir. Öncelikle varlık envanteri düzenlenirken bilgi ve süreç değerlendirilmesi yapıldıktan sonra varlıkların üzerinde barındırılan donanım, yazılımların güvenlik açısından değerlendirme ve sınıflandırma

işlemleri gerçekleştirilmelidir (Mete, 2010). Varlık, bilişim teknoloji yönetiminde bulunan yazılım, donanımların haricinde; ürün bilgileri, satış bilgilerini içeren dosyalar, kişisel bilgisayar, yazıcılar, sunucular, telefonlar, modemler, haberleşme cihazları, işletim sistemleri, ofis programları, sözleşmeler, üretilen mamuller, çekler, para, personel, kurumun imajının yanı sıra sisteminin bir parçasında yer alan ve işletme için değerli olan her şeydir (Eskiyörük, 2007).

### 3.6.4. Tehditlerin Belirlenmesi

Süreç ve sistemlerinin, diğer bilgi sistemlerinin işleyişini tamamen veya kısmen durmasına sebep olabilecek potansiyel tehlikeler tehdit olarak adlandırılır (Ersoy, 2012). Bilgi güvenliği tehditleri, bir işletme, bir kurumun ve kişilerin bilgi kaynaklarına zarar verebilme potansiyele sahip bir eylem olabilir. Bu tehditler bilinçli olabileceği gibi, bilinçsiz bir kaza sonucu olarak, hem işletme içinden veya dışından kişi ve gruplar tarafından oluşturulabilmektedir (Kahraman, 2006). Bu durumda ciddi olan her bir varlık için oluşabilecek bütün tehditlerin ayrıntılı bir şekilde incelenerek gözden kaçırılmaması gereklidir. Tehdit ile ilgili olarak daha önce yaşanmış tecrübeler, bilgi teknolojilerini, güncel güvenlik konularının yakından takibi ile mevcut tehdit tabloları kaynak olarak kullanılmalıdır (Mete, 2010).

Tehditlerle ilgili değerlendirme yapılırken herhangi bir tehdidinin küçümsenerek göz ardı edilmesi doğru olmayacaktır. Bu sebeple göz ardı edilen tehdit işletme ve kurum güvenliğinde zayıflık yaratabilmektedir. Tehditlere örnek olarak; sel, toprak kayması, fırtına, yıldırım düşmesi ve deprem; doğal tehditler, uzun süreli elektrik kesintileri, hava kirliliği; çevresel tehditler olarak adlandırılmaktadır. İnsan kaynaklı olanlar ise zararlı yazılım yüklemesi, yanlış veri girişi, ağ saldırıları, yetkisiz erişim vb. tehditlerden oluşmaktadır (Eskiyörük, 2007).

Bilişim teknoloji sistemlerinde sıkça karşılaşılan örnek tehditler ve kaynakları Tablo 7'de bulunmaktadır. Meydana gelebilecek tehditler konusunda oluşabilecek zararlar ve önlemler için işin uzmanlarından bu konu hakkında yardım alınarak tablolar oluşturulabilir.

Oluşan tehdit kaynağındaki kısaltmaların, anlamları ve açılımları şu şekildedir. **B:** İnsan Kaynaklı bilerek, **D:** Doğal, **Ç:** Çevresel, **K:** Kaza ve İnsan Kaynaklı

**Tablo 7. Bilişim Teknolojileri Sistemlerinde Karşılaşılan Tehdit Ve Kaynakları**

| Tehdit | Tehdidin kaynağı |
|---|---|
| Bakım hataları | K |
| Deprem | D |
| Fırtına | D |
| Güç Kesintisi | B, Ç, K |
| Hırsızlık | B |
| İletişim dinlenmesi | B |
| Personel yetersizliği | K |
| Sel | D |
| Tozlanma | Ç |
| Yangın | B, K |
| Yazılım hataları | B, K |
| Yetkisiz kişilerin ağa erişimi | B |
| Zararı yazılımlar | B, K |

Kaynak: (Eskiyörük, 2007)

### 3.6.5. Açıklıkların Belirlenmesi

Açıklıklar, sistemdeki yazılım, tasarım ve donanımdan kaynaklanan bir bilgi güvenlik ihlaline yol açabilecek işletim sistemlerindeki açık noktalar, hatalar ve zayıf kalmış yönlerdir. Bir güvenlik ihlalinin sonucu oluşan güvenlik açığı, sistemdeki bilgisayarlara ve ağ üzerindeki kaynaklara yetkisiz erişmesini sağlamaktadır (Kumaş, 2009). Açıklık sistemlerde kendi başlarına bir tehlike oluşturmaz, bunun gerçekleşmesi için bir tehdidin olması gereklidir. Örneğin web sunucusunun yazılım güncellemelerin yapılmaması nedeniyle veya düzgün port yapılandırılması olmadığında, kötü niyetli bir kişinin bu açıkları kullanarak sisteme sızması ve yetkisiz erişim sağlaması tehlikeli olacaktır. Güvenlik açıklığı değerlendirilmesi, tehditler tarafından uygulanabilecek açık, zafiyetlerin ne kadar kolay gerçekleştirilmesini ele almaktadır. Sistemdeki açıklık varlığını belirlenmesinde birebir görüşme, anket, dokümantasyon ve otomatik tarama yapan araçlar gibi yöntemler kullanılabilir (Eskiyörük, 2007). Kullanılan bilgi

sisteminin teknik açıklığı hakkında zamanında bilgi edinilmeli, kurumun bu açıklığa maruz kalması değerlendirilmeli ve ilgili riskleri ele almak için uygun önlemler alınmalı, yazılım ve donanım üreticilerinin yayınlamış oldukları güncel açıklıkları ve yama listelerini sürekli olarak takip etmelidir (Ganbat, 2013).

### 3.6.6. Olasılık Değerlenmesi

Olasılık beklenmedik bir olayın meydana gelme ihtimali olarak tanımlanmaktadır. Risk analizinde sistemde oluşan bir açıklığın gerçekleşme olasılığının belirlenmesi büyük önem taşımakta ve belirlenen bütün açıklıklar için bir olasılık değerlendirilmesi yapılmalıdır. Olasılığın ortaya çıkarılması için, tehdit kaynağını, açıklığın cinsi, var olan denetimlerin varlığı ve etkinliği göz önünde bulundurulmalıdır. Olasılığın değerlendirilmesinde ilk yapılacak olan işlem bilgi güvenliği yönetim sistemi ekibi tarafından kaç aşamalı değerlendirme olacağının ve bu aşamaların nasıl belirleneceği tanımlanmalıdır. Üç seviyeli olasılık değerlendirme yapılabilmesi için Tablo 8 örnek olarak kullanılabilir.

**Tablo 8. Bilişim Teknolojileri Sistemlerinde Karşılaşılan Tehdit Ve Kaynakları**

| **Olasılık seviyesi** | **Olasılık tanımı** |
|---|---|
| Düşük | Tehdit ve kaynağı az etkili, açıkların gerçekleşmesini engelleyecek ve zorlaştıracak kontroller mevcut |
| Orta | Tehdit ve kaynağı etkili, açıkların gerçekleşmesini engelleyecek kontroller mevcut |
| Yüksek | Tehdit ve kaynağı etkili, açıkların gerçekleşmesini engelleyecek kontroller yok veya yetersiz |

Kaynak: (Eskiyörük, 2007)

### 3.6.7. Risk Derecelenmesi ve Değerlendirmesi

Risk değerlendirmesi için kullanılan yöntemler, modeller gerçekleştirilecek olan değerlendirmenin kapsamına ve risk etkenleri ile ilgili verilerin biçimlerine göre farklılık göstermektedir. Bilgi güvenliği alanındaki varlıkların risklerini hesaplamak için

nitel ve nicel metotlar geliştirilmiştir. Nicel değerlendirmede riskin azaltılması için kullanılacak yöntemlerin maliyeti matematiksel ve istatistiksel yöntemlerle hesaplanmaktadır. Hesaplama olayın gerçekleşme ihtimali, olası kayıpların maliyeti ve alınacak önlemlerin maliyeti kullanılarak yapılmaktadır. Risklerin gerçekleşme olasılığı ve maliyeti hakkında güvenilir bir bilgi yoksa risk, yüksek, orta, düşük gibi öznel bir terimlere ifade edilebildiği gibi uzmanlık gerektiren durumlarda nitel yaklaşımlar kullanılabilir. (Takçı, Akyüz, Uğur, Karabağ, & Soğukpınar, 2010). Risk analizi bu iki temel model üzerinde geliştirilen çeşitli yöntemler kullanılır. Bazı durumlarda bu yöntemlerde iki yapı bir arada kullanılmaktadır. Karma yapılı yöntemlerde, nitel veya nicel özelliklerden birisi daha ağırlıklı olmakta, yöntem bu özellikle bir kat daha nicel ve daha nitel olarak sınıflandırılmaktadır. Kullanılan yöntem nicel veya nitel olursa olsun, genel olarak tüm risk analizlerin ana hedefi toplam risk değerini öngörmektir (Aktaş & Soğukpınar, 2010).

Nicel risk değerlendirme tekniklerinde, riskin meydana gelme olasılığı ve sonuç üzerindeki etkisi sayısal değerlere dönüşür ve sayısal bir değer olarak hesaplanır. Bu sürece risk analizi veya risk ölçümü denilmektedir. Riskin seviyeleri nitel tekniklerle belirlenir, bu işlemlere risk derecelendirme olarak ifade edilmektedir.

**Tablo 9. Risk Derecesi ve Açıklamaları**

| **Risk Derecesi** | **Açıklama** |
|---|---|
| Düşük (0-3) | Riske karsı önlem alınıp alınmayacağı sorumlusu tarafından karar verilebilir ve önlem alınmayacaksa risk kabul edilebilir. |
| Orta (4-6) | Riske karsı önlem alınması gerekmektedir. Alınacak önlemler uygun bir sürede planlanmalı ve uygulanmalıdır. |
| Yüksek (9) | Riske karsı en yakın zamanda önlem almak gerekmektedir. Sistemin güvenli bir şekilde çalışmasına devam etmesi alınacak önleme bağlıdır |

Kaynak: (Mete, 2010)

Nitel risk değerlendirme tekniklerinde ise istenilmeyen olayların oluşma olasılığına göre etkileri düşük, orta ve yüksek şeklinde sınıflandırılmaktadır. Sonuç üzerinde en fazla etkiye sahip olan risk senaryoların geliştirilmesinde kullanılmaktadır. Nitel değerlendirme teknikleri analiz sonucunda verilerin mevcut olmadığında riskin düşük olduğu durumlarda kullanışlı olmaktadır. Risk değerlendirmesinde, işletmenin, kuruluşun kompleks yapısına, hazır verilere ve yönetim yaklaşımlarına bağlı olarak farklı yöntemler kullanabilmektedir (Kahraman, 2006).

Risk değerlendirmesi;

Risk= Varlık Değeri x Tehdidin Gerçekleşme Olasılığı x Etki Değeri

formülü ile hesaplanmaktadır.

Risk analizi örneği Tablo 10'da verilmiştir.

**Tablo 10. Risk Analizi Örneği**

| Varlık | Tehdit | Açıklık | Varlık Değeri | Olasılık | Tehdit Etki Değeri | Risk | Risk Üstlenme | Açıklama |
|---|---|---|---|---|---|---|---|---|
| Sunucu | Elektrik kesintisi | UPS pil ömürleri | 5 | 3 | 4 | 60 | Risk yüksek kabul edilemez | UPS sistemi gözden geçirilmeli |
| Sistem Odası | Doğal afetler, yangın | Yangın söndürme sistemi yok | 5 | 4 | 4 | 80 | Risk yüksek kabul edilemez | Yangın söndürme sistemi kurulmalı |
| Bilgisayarlar | Virüs saldırısı | Teknik açıklık | 2 | 3 | 2 | 12 | Risk orta dereceli kabul edilebilir | Anti virüs programı bütün bilgisayarlarda bulunmaktadır. |

Kaynak: (Ersoy, 2012)

Risk değerlendirme Tablo 11'de verilmiştir. Oluşan risklerin tabloya göre puanlamasında 24-81 değerleri arasında kırmızı ise yüksek, 8-18 değeri arasında sarı ise orta, 1-6 değerinde bulunuyorsa düşük olarak değerlendirme yapılabilir. Bu sistem sayesinde, işletmelerde mevcut olabilecek bilgi güvenliği ihlallerinden kaçınılır ve tüm varlıklar tehditlerden korunmuş olur.

**Tablo 11. Risk Değeri Tablosu**

| | | Olasılık x İşe Etki | | | | | |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 6 | 9 |
| Açıklık x Tehdit | 1 | 1 | 2 | 3 | 4 | 6 | 9 |
| | 2 | 2 | 4 | 6 | 8 | 12 | 18 |
| | 3 | 3 | 6 | 9 | 12 | 18 | 27 |
| | 4 | 4 | 8 | 12 | 16 | 24 | 36 |
| | 6 | 6 | 12 | 18 | 24 | 36 | 54 |
| | 9 | 9 | 18 | 27 | 36 | 54 | 81 |

Kaynak: (Demirtaş, 2013)

### 3.6.8. Riskin Kabul Edilmesi

Riskin kabulü mevcut tedbirlerin yeterli olduğu, ek önlemlerin, kontrollerin uygulanmasına gerek olmadığını ifade etmektedir. Herhangi bir ek güvenlik denetimine gerek olmadan, riskin belirlenen düzeyde devam etmesi kararıdır. Güvenlik riski hazır olan fakat saldırı riski olmayan bilgi varlıkları için risk maliyetine girilmesi yerine riskin göz ardı edilmesi tercih edilmektedir (Gülmüş, 2010).

### 3.6.9. Riskin Transfer Edilmesi

İşletme, kurumların kontrolünde, yönetimi altında olmayan varlıkların durumlarına ilişkin ilgili kurum ve işletmelerin müdahale imkânı olmayan konuların oluşturduğu risklerin başka işletme, kurumlara transfer edilmesidir. Örnek olarak hırsızlık, doğal afet, yangın gibi tehditleri azaltmak için yapılan denetimlerden sonra

çıkan artık riskin, itfaiye, emniyet güçlerine ve sigorta şirketlerine aktarılmasıdır. Risk nedeniyle etkilenen bilgi varlıklarının zararını başka kurumlara veya sigorta kuruluşlarına devredilmesidir. Bu sebeple riskten kaçınılma maliyetleri azalmakta ve bu konudaki sorumluluk başka işletme ve kurumlara verilmektedir (Gülmüş, 2010).

## 3.7. ISO/IEC 27001 BGYS ANA MADDELER VE KONTROLLER

ISO /IEC 27001:2013 standart versiyonunda 14 ana madde, 114 kontrol maddelerinden oluşmaktadır. 2005 yılında yayınlanan versiyondan farklı olarak 3 adet ana madde sayısı ilave edilmiş, kontrol maddeleri ise 16 adet azalmıştır. Bu bölümde ISO/27001:2013 versiyonunda yer alan ana maddeler ve kontroller yer almaktadır.

### 3.7.1. Bilgi Güvenliği Politikaları (ISO /IEC 27001:2013 Madde A.5)

İşletme ve kurumun amacı BGYS kapsamında bilgi güvenliği politikaların oluşturulması bu konuda yönetimin desteklemesi amaçlanmaktadır. İşletmede bilgi güvenliği politikaları bütün personele iletilmeli, yönetimin de desteklediği açıkça belirtilmelidir. Bütün çalışanlar belirlenen bilgi güvenliği politikalarına uymalı ve farkında olmalıdır (Çek, 2017). Yönetim işletme genelinde bilgi güvenliği politikasının desteklendiğini, güvenlik ilkelerine bağlılığını gösterdiğini, işletmenin, kurumun bilgi güvenliği politikasının sürekliliğin sağlanmasının amaçladığını bütün çalışanlarına ve işbirliği içinde olunan işletmelere gösteren bir yaklaşım sergilemelidir (Ersoy, 2012).

### 3.7.2. Bilgi Güvenliği Organizasyonu (ISO /IEC 27001:2013 Madde A.6)

Bu maddenin temel amacı; işletmede kurulacak olan bilgi güvenliğini yönetecek, bilgi güvenliği grubu, komite ve komisyonun kurulmasıdır. Kurulan grup aracığıyla işletmenin bilgi güvenliği politikasını düzenlemek, güvenlik önlemlerini, rollerini belirlemek, oluşabilecek riskleri değerlendirmek, yeni güncel tehditleri izlemek, risklerin nasıl azaltılacağını planlamak, farkındalık eğitimleri vermek, bilgi güvenliği bütçesinin belirlemek, mobil cihazların kullanılması ile ilgili riskleri için politikalar düzenlemek, BGYS belgelerinin takibini yapmak, daha genel olarak bakıldığı zaman bilgi güvenliği yönetim sisteminin düzgün çalışması amaçlanmaktadır. Oluşturulan

grubun görevi PUKÖ proses yaklaşımı çerçevesinde, Yönetimin Gözden Geçirmesi (YGG) çalışmalarının belirli aralıklarla yapılması ve takibinin yapılması önemlidir (Ersoy, 2012). Yönetim işletme içinde uygulanacak olan güvenlik önlemlerine aktif olarak destek vermeli, bilgi güvenliği amaçları belirlenmeli ve sorumlu kişiler atanmalıdır. Kurumun, işletmenin güvenlik politikasının aynı olduğunu, güvenlik politikasının etkili uygulanabilir olmasını sağlamak için bağımsız kurum veya kuruluş tarafından düzenli olarak denetlenmelidir (Şen & Yerlikaya, 2013).

### 3.7.3. İnsan Kaynakları Güvenliği (ISO /IEC 27001:2013 Madde A.7)

Çalışanların, yüklenicilerin, üçüncü şahısların sorumluluklarını kavraması, görevi kötüye kullanma, hırsızlık, sahtekârlık ve çalışan hatalarından oluşabilecek güvenlik açıklıklarının engellemesi, işletmede belirlenen rollere uygun işe alımlarda oluşabilecek riski azaltma konusunda güvenlik taraması ile birlikte yapılacak iş sözleşmelerinde bilgi güvenliği yükümlüğü belirtilmelidir. Yapılacak anlaşma işletmenin bilgi güvenliği politikalarına, yasal mevzuatlara göre uygun olarak tanımlanmalıdır. Tüm çalışanlar, yükleniciler ve üçüncü şahıs kullanıcılar sorumlulukları hakkında bilgi sahibi olmaları, bilgi güvenliği tehditleri, işletmenin güvenlik politikaları, prosedürlerine uygun ve insan riskinin azaltılmasını sağlamak için farkındalık eğitimleri düzenlenmelidir. Bilgi güvenliği ihlali yapan çalışanlar için disiplin süreci belirlemek bu aşama kapsamındadır (Government of Mauritius, 2018).

### 3.7.4. Varlık Yönetimi (ISO /IEC 27001:2013 Madde A.8)

İşletmenin bilgi varlıklarını kapsayan bir varlık envanterinin çıkarılması gerekmektedir. Varlıkların envanteri hazırlanırken farklı türlerin dikkate alınması karmaşıklığı giderecektir. Bilgi varlıkları; sözleşme, anlaşmalar, sistem dokümantasyonu, evraklar ve veri tabanı vb. soyut varlıklar; işletmenin itibarı, markası ve imajı, fiziksel varlıklar; bilgisayarlar, sunucular, iletişim araçlarından oluşmaktadır. Varlık yönetiminde işletme ve kurumlar istedikleri şekilde sınıflandırma yapabilmekte, varlıkların kullanımı, bilgi sınıflandırılması ve ortak işleme kontrollerini içermektedir. Varlık envanteri herhangi bir afetten sonra normal çalışma şartlarına dönmek için gereken tüm bilgiler yer almalıdır (Şen & Yerlikaya, 2013).

### 3.7.5. Erişim Kontrolü (ISO /IEC 27001:2013 Madde A.9)

Bilgi güvenliği temellerinden biri olan erişim kontrolü işletmelerde bilgi güvenliği alanında yoğunlaşılan ve en çok çalışılan hassas olan bir bölümdür. Erişim konusunda gerekli kontrollerin yapılmaması sonucunda, yetkisiz erişim nedeniyle bilgilerin bütünlüğü, gizliliği ve erişebilirliği bozulabilmektedir. Bu nedenle erişim kontrolü bilgi güvenliğinin sağlanması için kritik bir öneme sahiptir (Mete, 2010). Bilgi işleme ve bilgiye erişimleri sınırlamak, kontrol edebilmek için işletmenin ve kurumun gereksinimlerine göre bir yöntem oluşturmalıdır. Oluşturulan yöntemlerle ağ, ağ hizmetlerine kontrollü erişim sağlanması, kullanıcı hesaplarının açılıp, kapatılması, sistemlere erişim haklarının yönetilmesi, periyodik olarak gözden geçirilmesi, uygulama erişim denetimleri için kurallar oluşturulması gereklidir (Demirok, 2016). Erişim kontrolün nasıl yapılacağı en yüksek ve en alt seviyedeki politikalara kadar talimatlarda açık bir alan bırakmadan dokümanlar hazırlanarak uygulanmalıdır. En yüksek ve en alt seviyede erişim kontrol politikası, gizlilik derecesi etiketleri, dosya izinleri, kullanıcı profillerine yetkilendirme yapıldıktan sonra uygun politikaya göre sistem erişim kontrolleri prosedürler halinde yayınlanmalı ve uygulanmalıdır (Mete, 2010).

### 3.7.6. Kriptografi (ISO /IEC 27001:2013 Madde A.10)

ISO 27001'in 2005 yılı versiyonunda ayrı bir ana madde olarak dahil edilmemiş, ancak 2013 yılında yayınlanan versiyon ile ayrı bir madde haline getirilmiştir. (Çek, 2017) Kriptografi kavramı, belli bir anahtar şifreleme yöntemiyle bilgi kodlanarak bilgi güvenliği kapsamında bilginin gizliliği, bütünlüğü ve kimlik doğrulamasını amaçlamaktadır. Kontroller kapsamında, kriptografik kullanımı için anahtarların kullanım süreleri için politikalar geliştirilmesine ve tüm sistemin yaşam döngüsü içindeki politikaların kullanılmasına yönelik kontrollerin yapılmasını sağlamaktadır. İşletme, kurum kriptografik kullanımı, kontrolleri için bir politika oluşturulurken dünyada yaygın olarak kullanılan kriptografi tekniklerinin kullanımıyla ilgili kanuni düzenlemelere uluslararası kısıtlamalara dikkat etmesi gereklidir (Gündoğan, 2016).

### 3.7.7. Fiziksel ve Çevresel Güvenlik (ISO /IEC 27001:2013 Madde A.11)

Fiziksel ve çevresel güvenlik kontrolleri, işletmenin, kurumun tesislerine, bilgi kaynaklarına yetkisiz erişimi, kaynaklara hasar verilmesini, müdahale edilmesini, faaliyetlerin durmasını engellemektir. Bu amaçla bilgi sistemlerini koruma amaçlarına yönelik güvenlik sınırlarının belirletilmesi, sadece yetkili personelin bu alanlara erişim izinlerinin verilmesi için uygun giriş çıkış kontrolü sağlanarak korunmalıdır. Doğal afetler, art niyetli saldırılar veya kazaların oluşmasına karşı fiziksel önlemlerin alınmasına, bilgi sistemleri ekipmanlarını etkiyecek tehditlerden kaynaklanan riskleri azaltmak için önlemler almak, sistem ekipmanlarının enerji, güç kaynağı, diğer kesintilerden korunmak, bilgi işlem için kullanılan enerji, telekomünikasyon (internet, telefon data vb.) kablolarını oluşabilecek hasarlara karşı korunmasını sağlamak, ilgili ekipmanların çevresel tehditlere göre bakımlarının düzenli yapılması riskleri azaltacak şekilde yerleşimlerin yapılması yetkisiz erişim, işletme dışına çıkarılmasına yönelik kontroller yapılmalıdır (Gündoğan, 2016).

### 3.7.8. İşletim (Operasyon Güvenliği) (ISO /IEC 27001:2013 Madde A.12)

Bilgi işlem tesislerinin işletim prosedürlerin oluşturulması, bilgi güvenliğini etkileyen tehlikelere karşı korumak, veri kaybını önlemek, sistemdeki değişiklikleri kontrol etmek, kaynakları etkin ve doğru kullanılması bu madde kapsamındadır. Ayrıca zararlı yazılımları tespit etmek, önlemek, imha etmek, işletim sistemlerinin, yazılımların kontrol edilmesini ve güvenlik açıklarının tespit edilip giderilmesini sağlamak işletim güvenliği kapsamındadır. Bilgilerin yedekleme işlemleri oldukça önemlidir, bilgi yazılım, sistem datalarının yedek kopyaları, kabul edilen bir yedekleme politikasında uygun düzenli olarak yedek alınmalı ve test edilmelidir. Sistem yöneticileri, sistem kullanıcı operatörlerinin işlemleri, kural dışı faaliyetleri, bilgi güvenliği olaylarını kayıt altına (log kaydı) alınmalı, alınan kayıtlar korunmalı düzenli olarak gözden geçirilmesi gerekmektedir (Daşdemir, 2016).

### 3.7.9. Haberleşme Güvenliği (ISO /IEC 27001:2013 Madde A.13)

Haberleşme güvenliğinin amacı, işletmenin, kurumun ağ güvenliğinin ve kuruluşun gerçekleştirdiği bilgilerin aktarımının güvenliğini, ağlarda bilginin ve

destekleyici alt yapının korunmasını sağlamaktır. Ağ güvenliği sağlanmasında, ağ hizmetleri güvenliği, ağlarda ayrım, bilgi transferi, ağ kontrolleri gerçekleştirilmektedir. Tüm ağlarla ilgili güvenlik mekanizmaları ve hizmet seviyelerini, bilgi transfer politikalarını, bilgi transfer sözleşmeleri, e-imza kullanımı, elektronik mesajlaşma, gizlilik ve ifşa etmeme ve yönetim gereksinimlerini tanımlamaktadır (Gündoğan, 2016).

### 3.7.10. Sistem Temini, Geliştirme ve Bakımı (ISO /IEC 27001:2013 Madde A.14)

Bilgi güvenliğinin yaşam döngüsü boyunca bilgi sistemlerinin ayrılmaz bir parçası olması sağlanmalıdır. Halka açık olan ağlar üzerinden servis sağlayan, uygulama hizmetleri, hileli eylemleri, sözleşme ihlallerini, gizli bilgileri açığa çıkarma, bilgi sistemlerini de içermekte ve korumaktadır. İşletme açısından işletim sistemleri Windows, Linux, veri tabanı vb. değişikliğinde güvenlik üzerinde olumsuz bir etki oluşturmaması için önemli ve hassas uygulamalar gözden geçirilmeli, bu konuda gerekli testler yapılmalıdır. Tüm sistem uygulamalarında, sistem yöneticisi atamak ve güvenli sistem mühendisliği prensiplerinin tanımlanması, yazılı hale getirilip uygulanmalıdır (Türk Standardları Enstitüsü, 2013).

### 3.7.11. Tedarikçi İlişkileri (ISO /IEC 27001:2013 Madde A.15)

Tedarikçinin işletmenin varlıklarına erişim sağladıklarında ortaya çıkabilecek risklerin azaltılması için, tedarikçi tarafından kabul edilen, sertifikalandırılmış ve bilgi güvenliği gereklilikleri ile tedarikçi hizmetlerinin gözden geçirilmesi, izlenmesi için usuller oluşturulmalıdır (Demirok, 2016).

### 3.7.12. Bilgi Güvenliği İhlal Olayı Yönetimi (ISO /IEC 27001:2013 Madde A.16)

Bir güvenlik ihlali, bilginin gizliliğini, kullanılabilmesini ve güvenirliliğini tehlikeye yol açan olaylar olarak adlandırılır. Bu maddenin amacı her türlü güvenlik ihlallerinin düzgün bir biçimde ele alınması ve değerlendirilmesini sağlamaktır (Kahraman, 2006). Bilgi güvenliği ihlali olay yönetimi bünyesinde yapılacak kontrollerin amacı; meydana gelen bilgi güvenliği olaylarının değerlendirme yapılarak,

bilgi güvenliği ihlali kapsamında sınıflandırma yapılıp yapılmayacağına karar vermek, ihlal olayı ekibinin kurularak sorumlusunu belirlemektir. Meydana gelen ihlal olaylarına hızlı ve etkili müdahale etmek, ihlal olaylarından sonra delillerin toplanması, delillerin korunması sağlamak, ihlal olaylarının tespiti için yazılı politika ve prosedürler kapsamında yetkili kişi veya makamlara raporlanmasını yapmaktır. Meydana gelen ihlal olaylarının incelenip, çözümlenmesinden elde edilen deneyimlerin, ileride oluşabilecek ihlal olaylarının meydana gelme olasılığını azaltmak için kullanılmasını sağlamaktır (Gündoğan, 2016).

### 3.7.13. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları (ISO /IEC 27001:2013 Madde A.17)

Bilgi güvenliği yönetim sistemin kurulması ve yönetilmesi açısından iş sürekliliği büyük bir öneme sahiptir. Bu nedenle sistemin kurulmasının esas hedeflerinden birini oluşturan iş sürekliliği işletmelerin hassas iş süreçlerinin devamlı olmasını sağlamak, planlanmamış kesintilerde, belirlenen süre içerisinde sistemin yeniden kullanılabilir hale getirilmesini sağlamaktır (Mete, 2010). İş sürekliliği süreci, en önemli güvenlik riskleri için yapılması gereken eylemler hakkında bazı senaryolar geliştirmeli ve oluşturmalıdır. Örneğin: siber saldırı sonrası sistemin tekrar devreye alınabilmesi için ayrıntılı bir eylem planı ve prosedürler oluşturulmalı, deprem durumunda sorumlu olan personelin bu konuda eğitimler verilmesidir. Yapılacak olan eylem planında öncelikle kritik süreçlerin hizmete alınması daha sonra ise diğer ilgili alanların devreye alınması gereklidir (Ceauşu, Ilie, & Ionescu, 2018). İş Sürekliliğini sağlamak için bilgi sistemlerinin (Felaket Kurtarma Merkezi) başka bina veya bölgede olmak şartıyla altyapı, ağ, yazılımların ve veri yedekleme planı oluşturulması, kritik personelin bir yedeğinin bulunması gerekmektedir. Felaket anında yapılacaklar, görevler, iş sürekliliği planlanmalı, iş tanımları belirlenmeli ve iş sürekliliği planları güncel durumda olmalıdır (Ersoy, 2012). Hazırlanan planların uygun olup olmadığının kontrol edilmesi süreçlerin, verilerin hızlı, eksiksiz bir şekilde kurtarılması için belirli zamanlarda bu konuda tatbikatlar yapılmalıdır. İş sürekliliğinin temel başarı faktörlerinden birisi personel için farkındalık eğitim programları düzenlenmelidir (Ceauşu, Ilie, & Ionescu, 2018).

### 3.7.14. Uyum (ISO /IEC 27001:2013 Madde A.18)

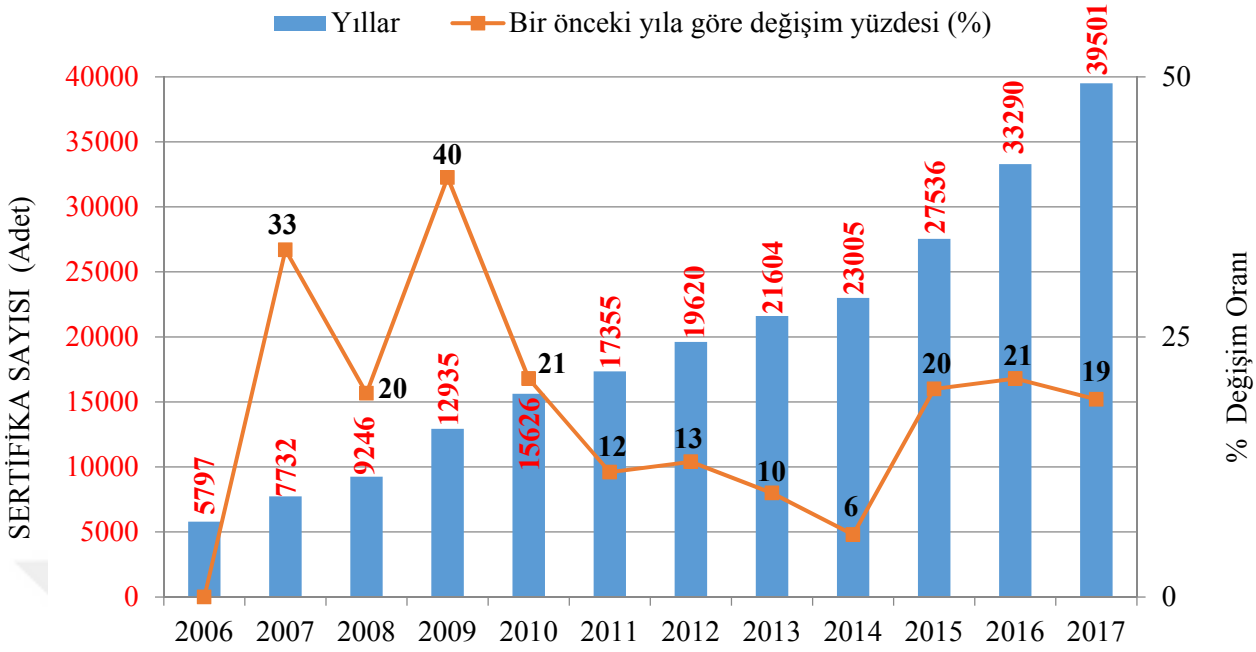
Uyum kapsamında yapılacak kontrollerin amacı; yasal sorumlulukların, yasal hükümlerin ve sözleşmelerden doğan yükümlülüklerin ihlalini önlemek amacıyla, kurumun bilgi sistemlerinin gereksinimlerinin açıkça tanımlanmasını ve yazılmasını sağlamaktır. İşletmeler diğer kurum ve kişilerin fikri mülkiyet haklarını ihmal etmemeli, ilgili yazılım ürünlerinin işletmenin bilişim ağlarında lisansız olarak kullanılmasını, fikri mülkiyet haklarının ihlal edilmesini yasaklamalı, engellemelidir. Bilgi sistemlerinde bulunan bilgi kaynaklarının kayıp, imha, sahtecilik, yetkisiz erişim ve yetkisiz yayınlamaya karşı korunması, kişinin kimlik bilgilerinin gizliliğini korumak ve kriptografik kontrollerin ilgili yükümlülüklere uygun olarak yapılmasını sağlamaktır (Gündoğan, 2016). Yasa, mevzuat ve yönetmeliklerin takibi için bir sorumlu belirlenmeli, aynı zaman da bu kişi lisanslı yazılım envanterinin takibinden de sorumlu olmalıdır. Yöneticiler, birim amirleri kendi sorumluluk alanında bilgi güvenlik politikaları ve standartları konusunda denetleme yapmalıdır (Türk Standardları Enstitüsü, 2013).

# DÖRDÜNCÜ BÖLÜM
# BİLGİ GÜVENLİĞİ İSTATİSTİKLERİ ARAŞTIRMASI

## 4.1. ISO/IEC 27001 BİLGİ GÜVENLİĞİ STANDARDININ DÜNYA'DAKİ YERİ

ISO 27001 standardı eski İngiliz Standardı olan 17799-2 versiyonun içeriğinin genişletilmesi ile oluşturulmuştur. BGYS bir işletmenin yönetilmesi, bütün görevleri, faaliyetleri için bilgilerin gizliliğinin sağlanması bu nedenle kullanılması gereken yöntemlerden oluşmaktadır. Uygun bilgi güvenliğini belirli bir sürede korunması veya meydana gelebilecek risklere karşı koruma sağlanması için teknoloji, organizasyon ve insanlara arasında kuvvetli bir etkileşim gereklidir. Bir işletmenin, kurumun hassas verilerini yönetebilmek için bir dizi prosedür ve politikalar gerekmektedir. Bu nedenle bir bilgi güvenliği politikasında organizasyonel yapıyı, prosedürleri içermelidir. ISO/IEC 27001 uluslararası standardı, dünyada kabul görmüş istikrarlı olan ortak terminoloji, çekirdek tanımları olan yüksek kaliteli bir yapıda BGYS'nin uygulanması ve işletilmesi için ortak bir yaklaşım sağlamak üzere geliştirilmiştir. ISO/IEC 27001'in yayınlanması ile birlikte standart dünya çapında büyük oranda kabul görmüştür. Bilgi güvenliğini dikkate alan işletmeler süreç gelişimi için ilke ve yöntemlerin giderek benimsenmesi sonucunda yaygınlaşmaktadır. Dünya genelinde birçok kuruluş ve ülke ISO 27001 gerekliliklerini karşılayan bilgi güvenliği yönetimine sahiptirler (Shojaie, 2018).

Dünya geneline bakıldığı zaman ISO/IEC 27001 BGYS standardını uygulayan ülke, işletme ve kurumların sayısı her geçen gün artmaktadır. ISO tarafından yayınlanan araştırma raporu istatistiklerine göre aşağıdaki grafikler oluşturulmuştur. Şekil 8.'de 2006 - 2017 yılları arasında verilen sertifika sayıları ve yüzde oranları verilmiştir. Grafikte görüldüğü gibi önümüzdeki yıllarda Bilgi Güvenliği Yönetim Sistemine başvuru sayısının artması beklenmektedir. 2017 yılında verilen sertifika sayısı 2016 yılına göre yaklaşık %19 oranında artış gösterildiği görülmektedir. 2017 yılında ise ISO/IEC 27001 sertifika sayısının dünyada toplam 39501 adet olduğu görülmektedir.



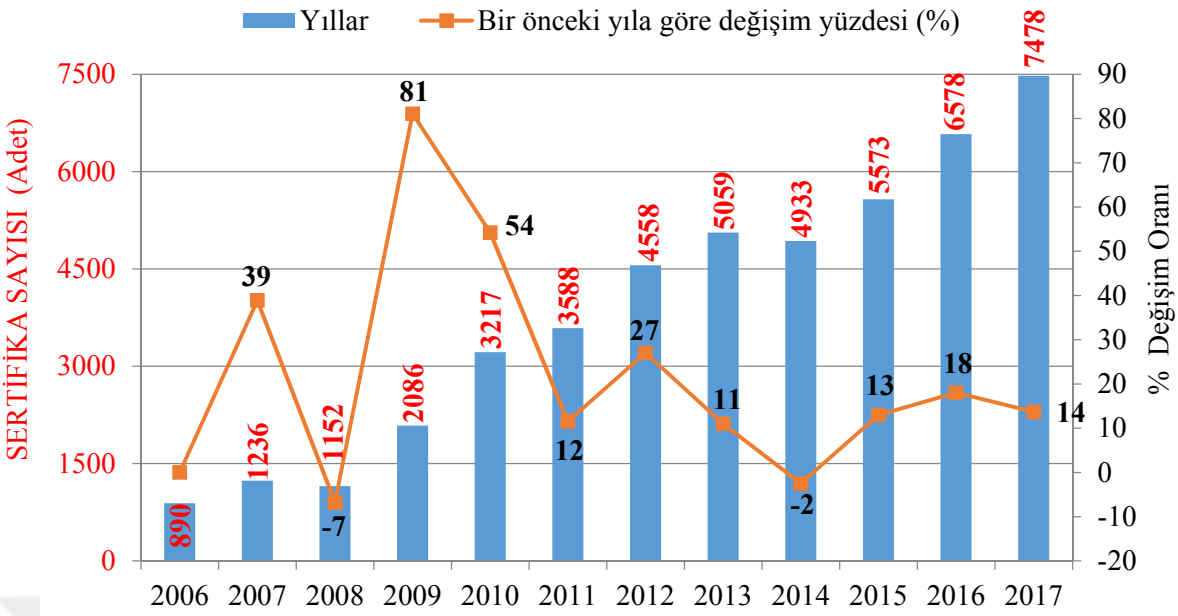

**Şekil 8. Dünya'da Sertifika Sayısı Ve Oranlarının Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

### 4.1.1. Dünya'da ISO 27001 Standardının Sektör % Oran Dağılımı

Dünya da BGYS nerdeyse her sektörde yaygın olarak kullanılmakta, ancak bazı sektörlerde daha ön plana çıktığı görülmektedir. ISO/IEC 27000 standart ailesine bakıldığında bilgi teknolojileri, sağlık, imalat, ar-ge, tasarım, iletişim, gibi kilit alanlardaki firmaların yanında savunma ve hizmet sektöründeki özel durumda olarak firmaların ihtiyaçlarını karşılamaktadır.

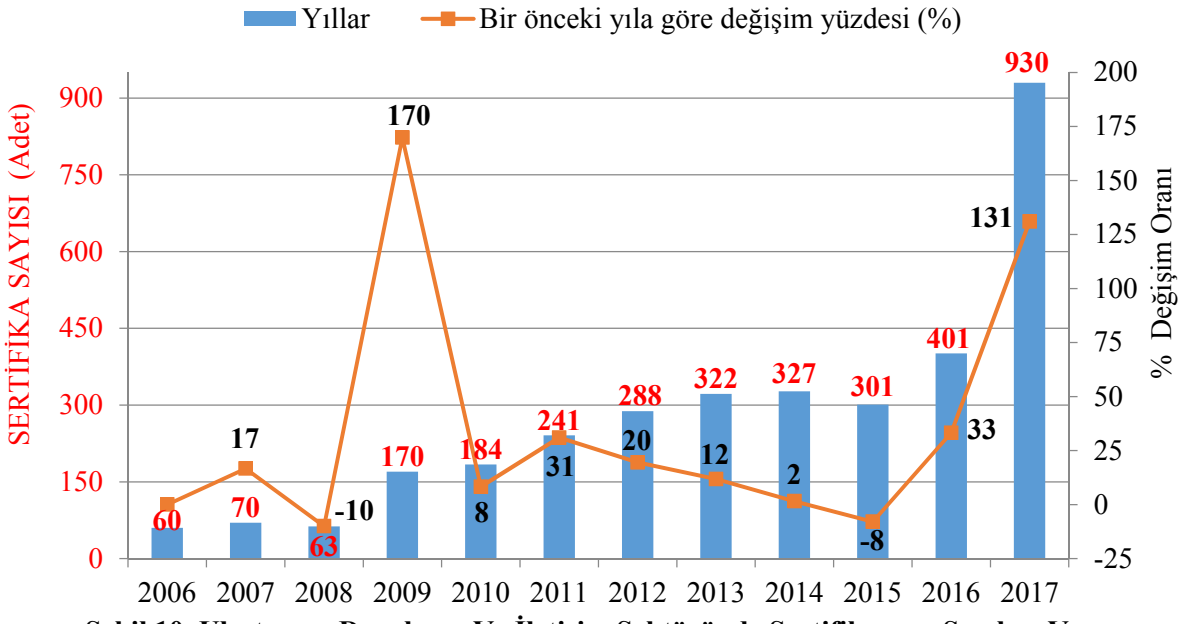
ISO'nun 2017 yılında yayınlamış olduğu araştırma raporuna göre Dünya genelindeki 2006 - 2016 yıllarına ait istatistik bilgilerine göre yoğun olarak kullanan ilk yedi sektörün yıllara göre almış olduğu sertifika sayıları ve % değişim oranları grafiklerde gösterilmiştir. Bu sektörlerin başında en yüksek sertifika sayısına sahip olan bilgi teknolojileri (Şekil 9) yer almaktadır. İşletmelerin iş süreçleri içerisinde yer alan bilgi teknolojileri internetin hızla gelişmesiyle birlikte günümüzde ihtiyaç haline gelmiştir. Dünya geneline bakıldığında bilgi teknoloji sektörünün yıllara göre artan sertifika sayısına göre sürdürülebilir bir büyüme içinde olduğu gözükmektedir.




**Şekil 9. Bilgi Teknolojileri Sertifikasyon Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

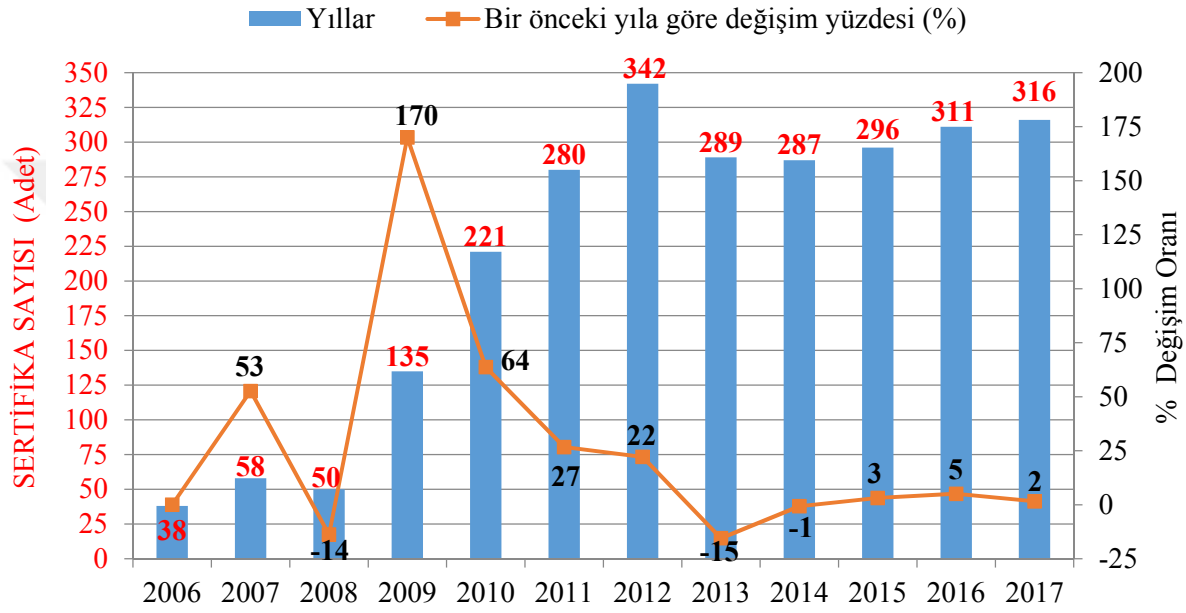
Dünya ekonomisinde, ticaretinde büyük bir yere sahip olan, ulaştırma, depolama ve iletişim sektörünün (Şekil 10) 2009 yılında % 170 değişim oranıyla en yüksek, 2017 yılında ise 930 adet sertifika ile en yüksek seviyeye ulaşmıştır.




**Şekil 10. Ulaştırma, Depolama Ve İletişim Sektöründe Sertifikasyon Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

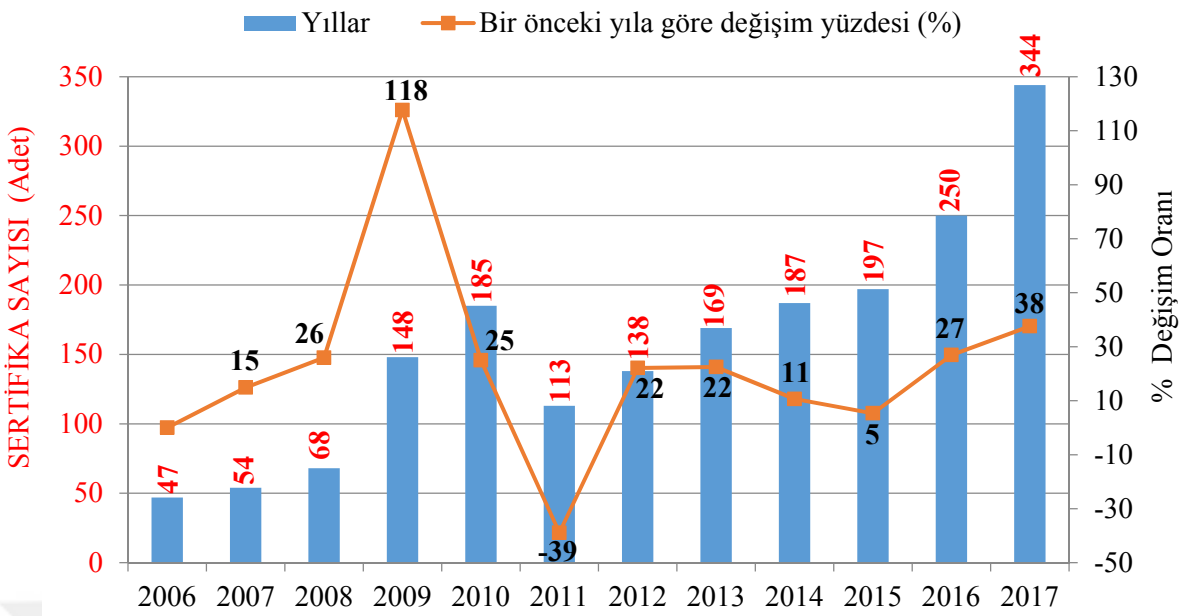
Şekil 11'de Elektrik ve optik ekipman sektöründe sertifika sayısının 2012 yılında sertifika sayısı ile; 2009 yılında ise bir önceki yıla göre % 170 değişim yüzdesi ile en yüksek seviyede olduğu görülmektedir. Yılların dağılımına göre sertifika değişim oranında 2008'den sonra 2013 yılında % -15 değeriyle en düşük seviyeye gerilemiştir.




**Şekil 11. Elektrik Ve Optik Ekipman Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

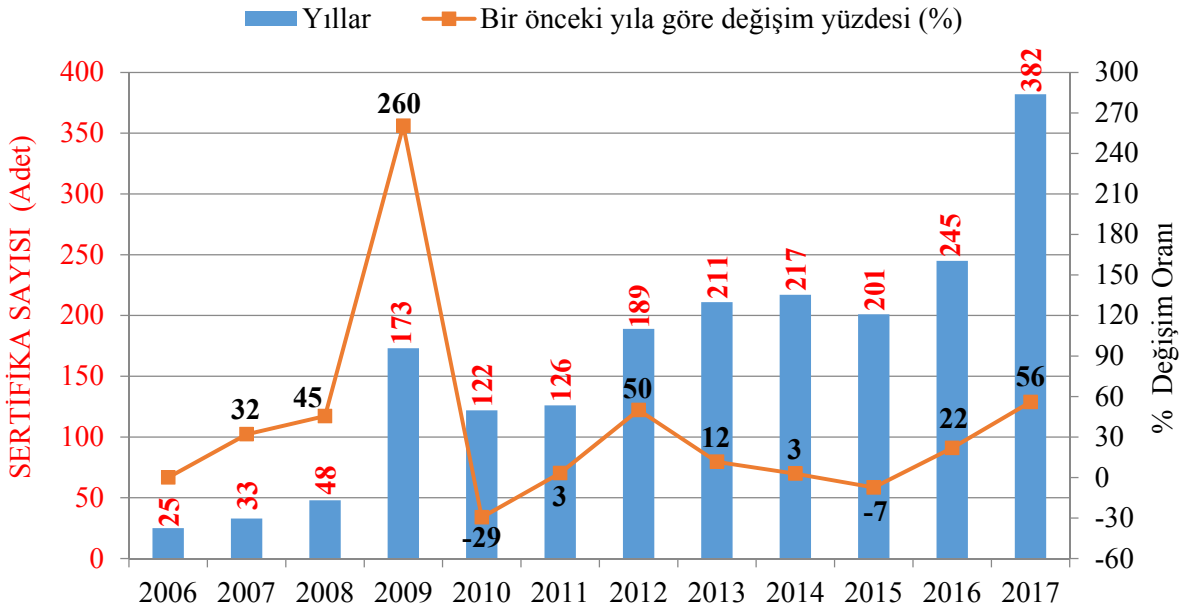
Finansal aracılık ve emlak sektöründeki sertifika sayıları ve değişim oranlarına bakıldığı zaman; 2006 - 2017 yılları arasında en düşük değişim oranının 2011 yılında yaşandığı % -39 gerilediği gözlemlenmiştir. 2011 yılında sertifika değişim oranında yaşanan bu düşüşün nedenine bakıldığı zaman sözü edilen küresel finans krizinden etkilendiği sonucu ortaya çıkmaktadır. ISO/IEC 27015 Finansal hizmetler için bilgi güvenliği yönetim kuralları standart maddesinin 2012 yılında yayınlanmasından sonra yıllarda bu sektörde bilgi güvenliğine olan ilginin arttığı görülmektedir (Şekil 12).




**Şekil 12. Finansal Aracılık Ve Emlak Sertifika Sayıları Ve Değişim Oranları**

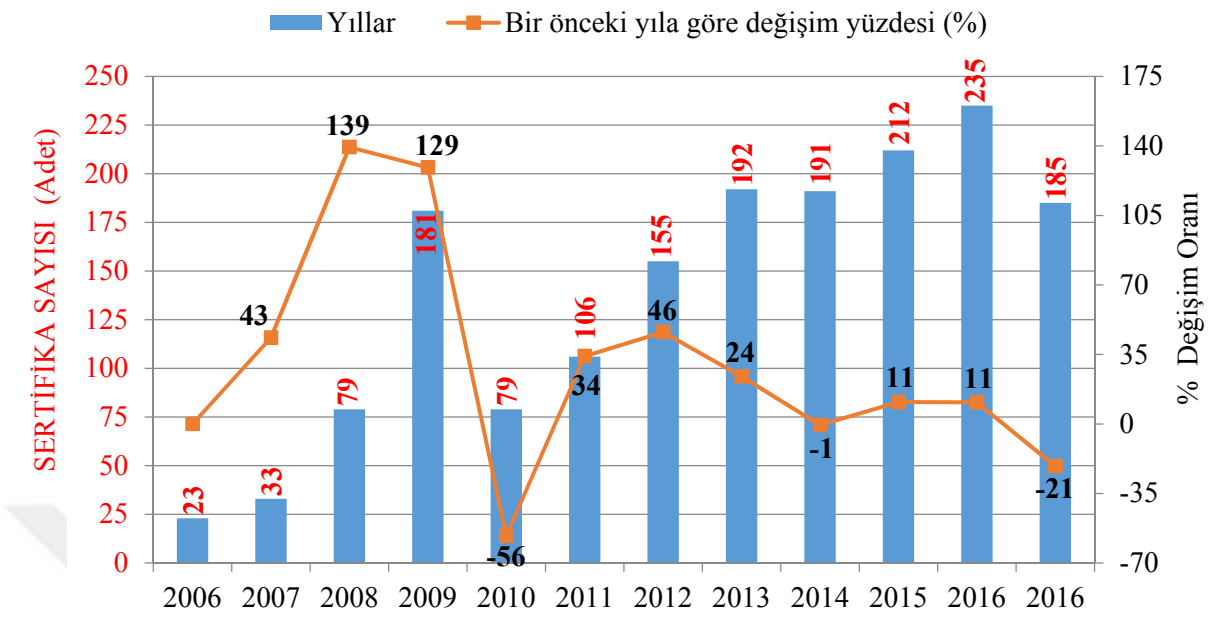
Kaynak: (International Organization for Standardization, 2018)

Mühendislik hizmetlerinde yıllara göre dağılım grafiğinde 2009'da % 260 değişim ile en yüksek seviyede iken 2010'da ise % -29 en düşük değişim oranındadır (Şekil 13).



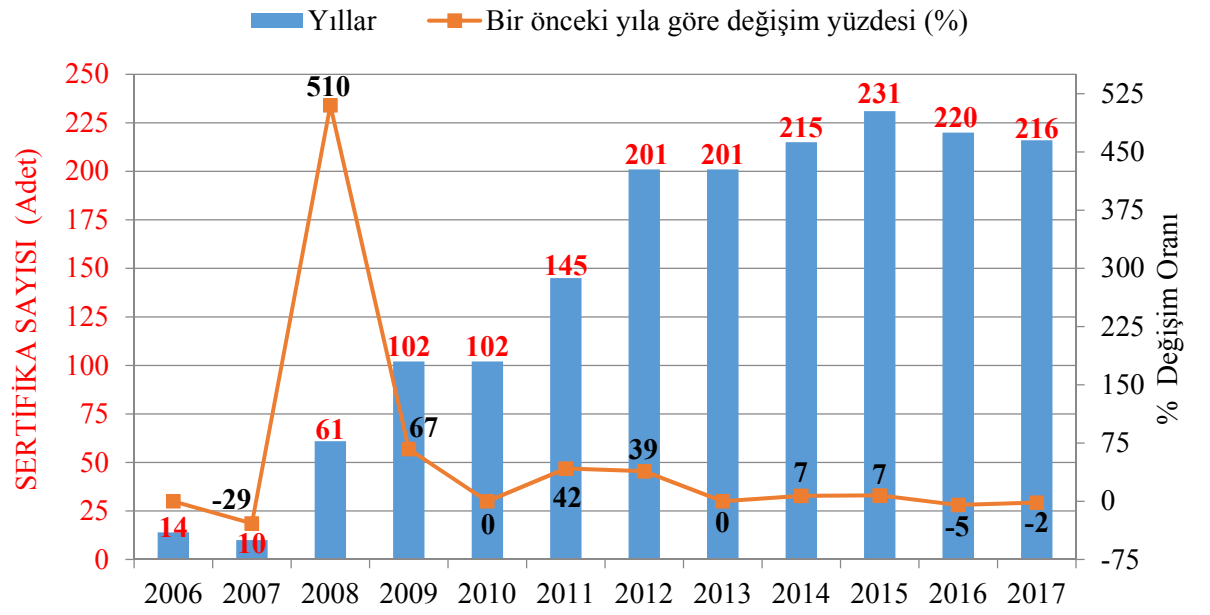

**Şekil 13. Mühendislik Hizmetleri Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)




**Şekil 14. Kamu Yönetimi Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)




**Şekil 15. Sağlık ve Sosyal İşler Sertifika Sayıları Ve Değişim Oranları**

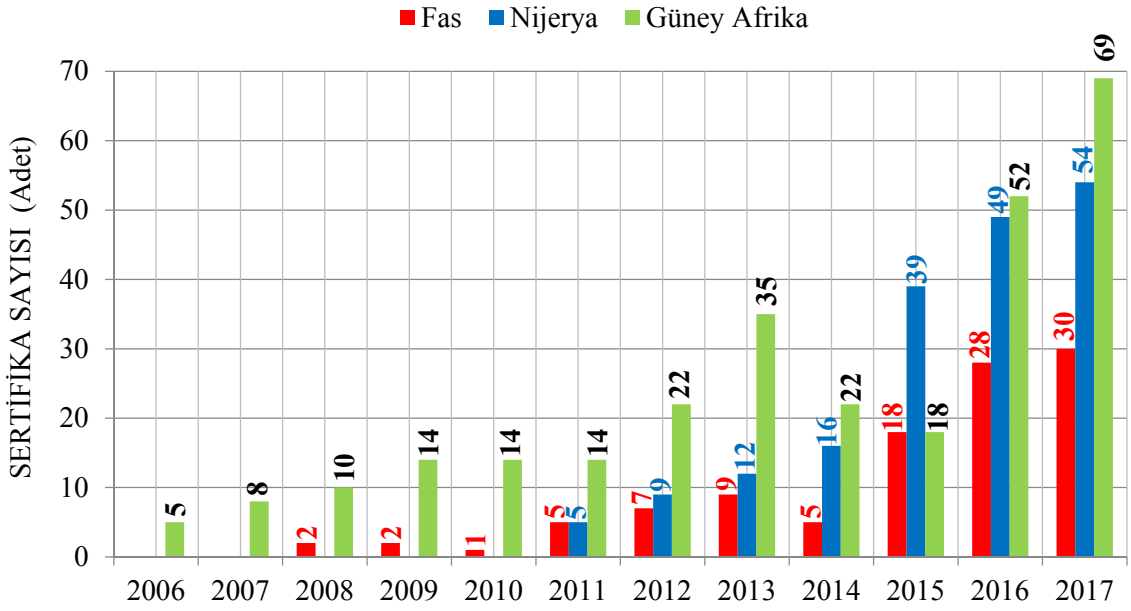
Kaynak: (International Organization for Standardization, 2018)

Bu konuda yayınlanan araştırma raporuna bakıldığında ise; inşaat, tekstil, eğitim, matbaa, makine, geri dönüşüm, gıda ürünleri, uzay ve diğer sektörlerinin de yer aldığı görülmekte, bu dağılım Dünya'daki ülkelere, yıllara ve sektörlerin önceliklerine göre sıralaması değişebilmekte, farklılık gösterebilmektedir.

### 4.1.2. Dünya'da ISO 27001 Standardının Bölgesel Ülke Dağılımı

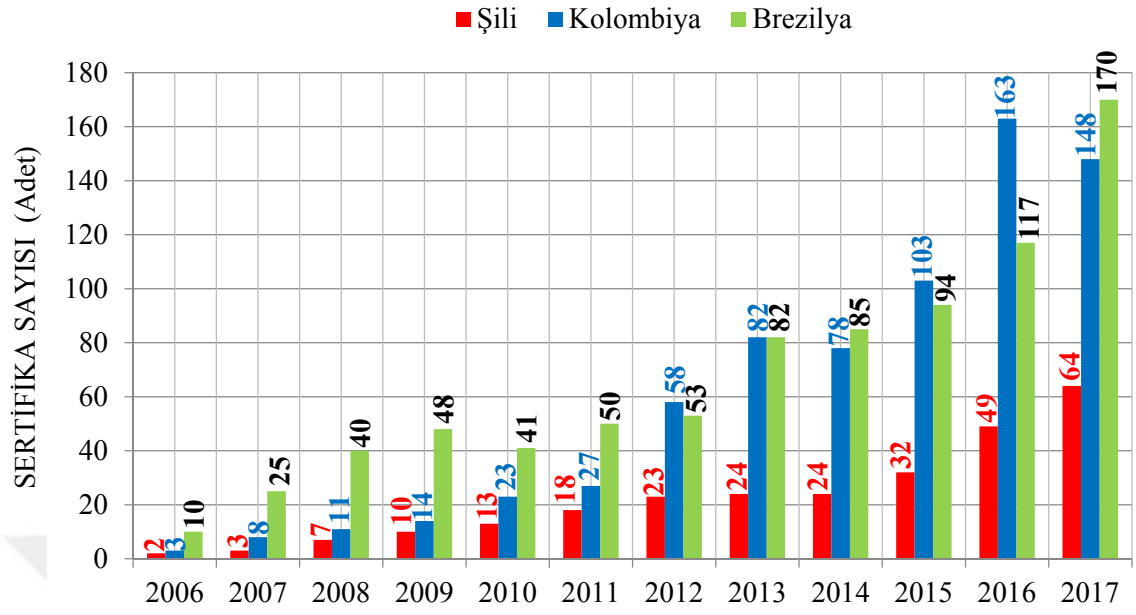
Dünya genelinde bölgesel farklı kıtaların sertifika dağılımına bakıldığında ISO/IEC 27001 sertifika sayısının fazla olan bölgelerde, iş gücü yoğunluğu, Gayrisafi yurt içi hasıla (GSYİH) ile satın alma gücü, para birimi, ülkenin ekonomisi ve ekonomik performans arasındaki ilişki gözlemlenmektedir. Bu duruma ülkenin teknolojik kullanım düzeyi, refah düzey seviyesi, politik ve kültür yapısı da etkili olmaktadır (Shojaie, 2018).

Afrika bölgesinde yer alan ülkeler incelendiğinde; Fas'ın 2006 ve 2007 yıllarında hiç sertifikaya sahip olmadığı, Nijerya'nın ise 2011 yılından sonra 5 adet sertifika sayısına ulaştığı görülmektedir. Sertifika konusunda Güney Afrika ülkesinin 2006 - 2017 yılları arasında diğer ülkelere nazaran iki kat daha fazla sertifikaya sahip olduğu gözlemlenmiştir (Şekil 16).




**Şekil 16. Sertifika Sayısına Göre Afrika'daki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

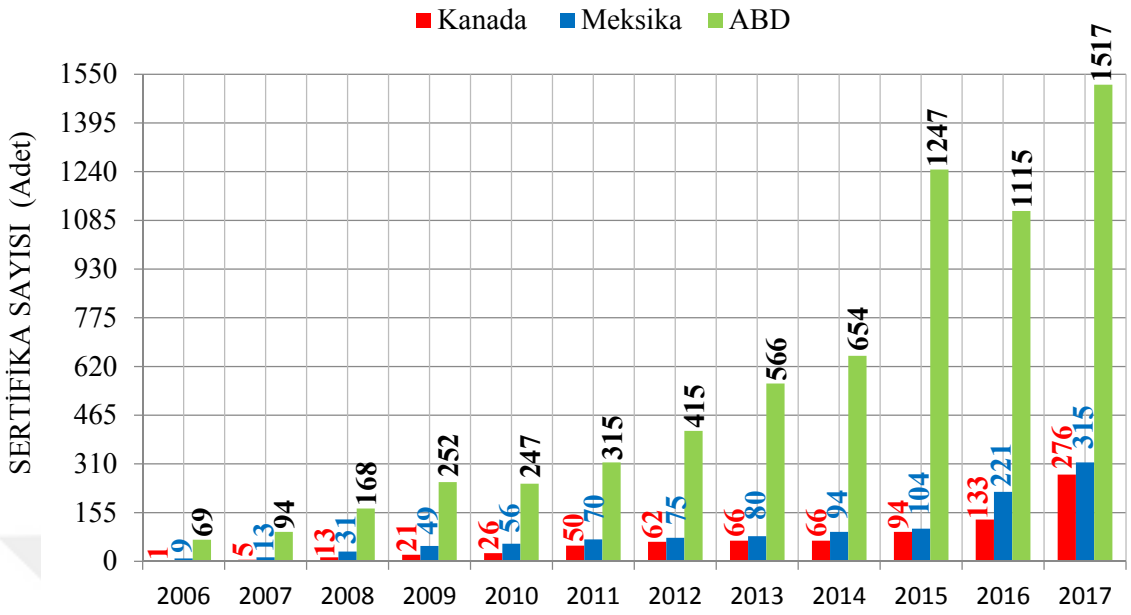



**Şekil 17. Sertifika Sayısına Göre Güney Amerika'daki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

Şekil 17'de Güney Amerika'da bulunan üç ülkenin 2006 - 2017 yılları arasında sertifika sıralamasında; Brezilya'nın birinci sırada 170 adet, Kolombiya'nın ikinci sırada 148 adet ve Şili'nin son sırada 64 adet sertifika sayısına ulaştığı tespit edilmiştir. Kolombiya'nın 2015 ve 2016 yıllarında Brezilya'yı geçtiği görülmekte fakat 2017 yılında sertifika sayısındaki gerileme nedeniyle birinciliği kaybetmiştir.

Kuzey Amerika'da ABD'nin Dünya'da en büyük ekonomiye, teknolojiye sahip olması nedeniyle sertifika sayısı ve dağılımında Kanada ve Meksika'nın önünde yer aldığı gözlenmektedir (Şekil 18). 2006 yılından 2014 yılına kadar sertifika sayısının nispeten düşük olduğu görülen ABD'nin bu yıldan sonraki sertifika sayısında ciddi oranda artış yaşanmıştır. Kanada'nın 2006 yılında 1 adet olan sertifika sayısının 2017 yılında 276 adet; Meksika'nın ise 2006 yılında 9 adet, 2017 yılında sahip olduğu sertifika sayısı 315 adet olmuştur.

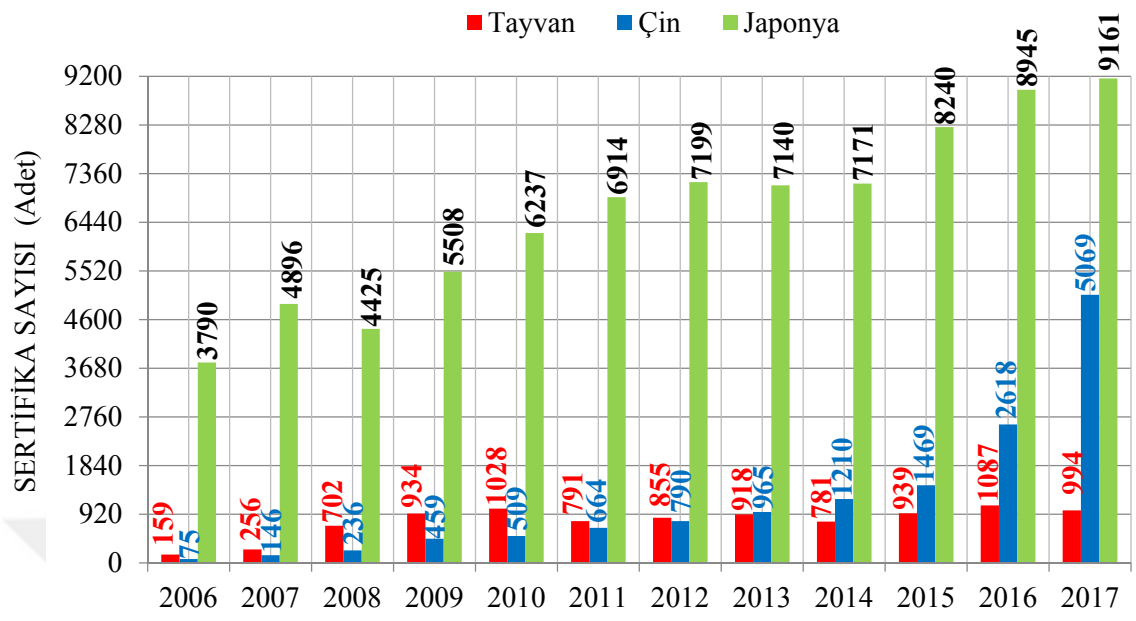



**Şekil 18. Sertifika Sayısına Göre Kuzey Amerika'daki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

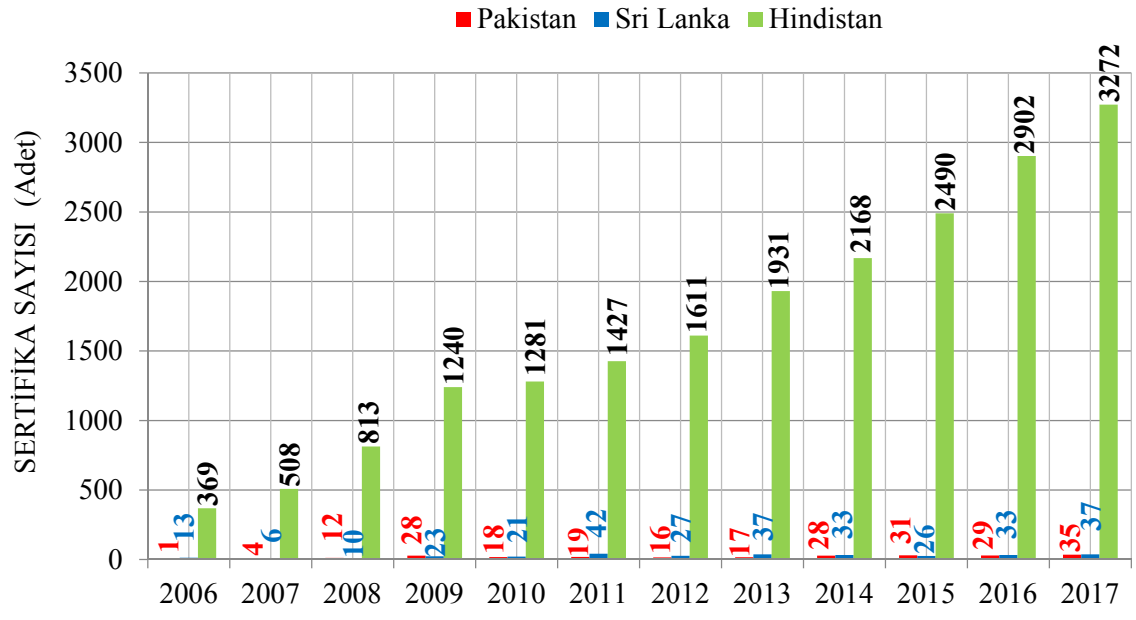
Doğu Asya ve Pasifik bölgesinde (Şekil 19) yer alan ülkelerden Japonya'nın Dünya'da en çok sayıda ISO 27001 sertifikasına sahip olduğu, yükselen ekonomisi ve teknolojisi ile Çin'in son yıllardaki sertifika sayısındaki artış nedeniyle bilgi güvenliği konusunda yakından ilgilendiği görülmektedir. Son yıllarda Dünya'da meydana gelen siber saldırılar, fidye yazılımları konusunda yayınlanan istatistiklerde Çin Devletinin üst sıralarda yer almakta, en fazla siber saldırıya maruz kalan ülkeler arasındadır. Tayvan bilgi güvenliği konusunda yıllar içerisinde istikralı bir şekilde ilerleme kaydettiği görülmekte; Dünya sıralamasında sertifika sayısına göre üst sıralamada yer almaktadır.

Orta ve Güney Asya ülkelerinden olan Hindistan'ın yazılım endüstrisinde yer alması bu konuda çalışmalar yapması nedeniyle ISO 27001 BGYS konusunda Dünya'da ilk beş ülke içinde yer almaktadır. Grafikte de (Şekil 20) görüldüğü gibi Pakistan ve Sri Lanka bilgi güvenliği standardizasyonu konusunda zayıf kaldıkları görülmektedir.



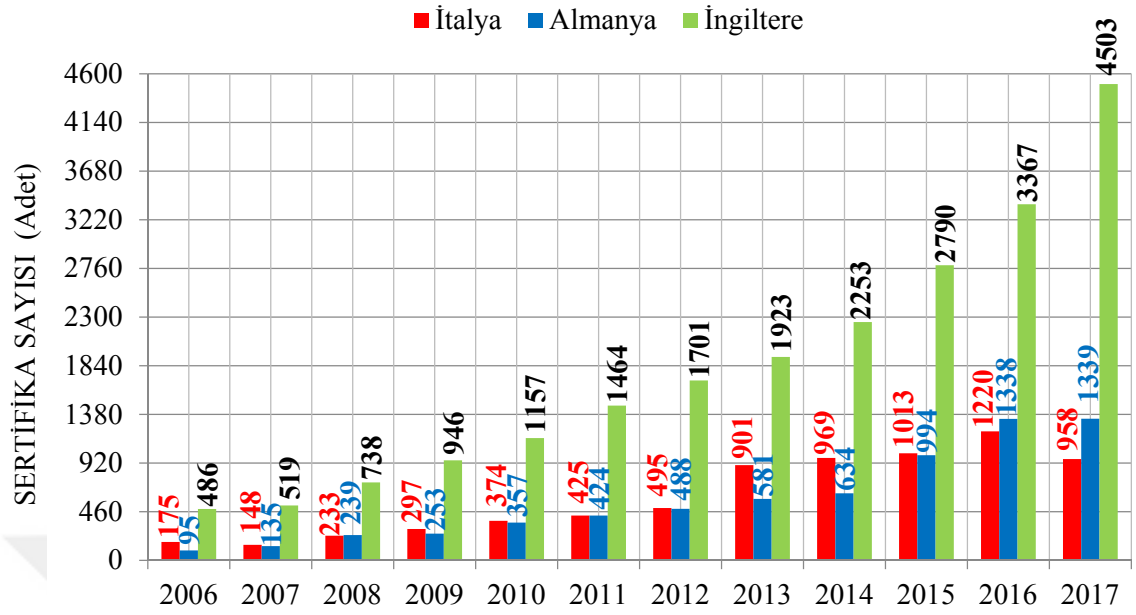

**Şekil 19. Sertifika Sayısına Göre Doğu Asya ve Pasifik'teki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)




**Şekil 20. Sertifika Sayısına Göre Orta ve Güney Asya'daki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

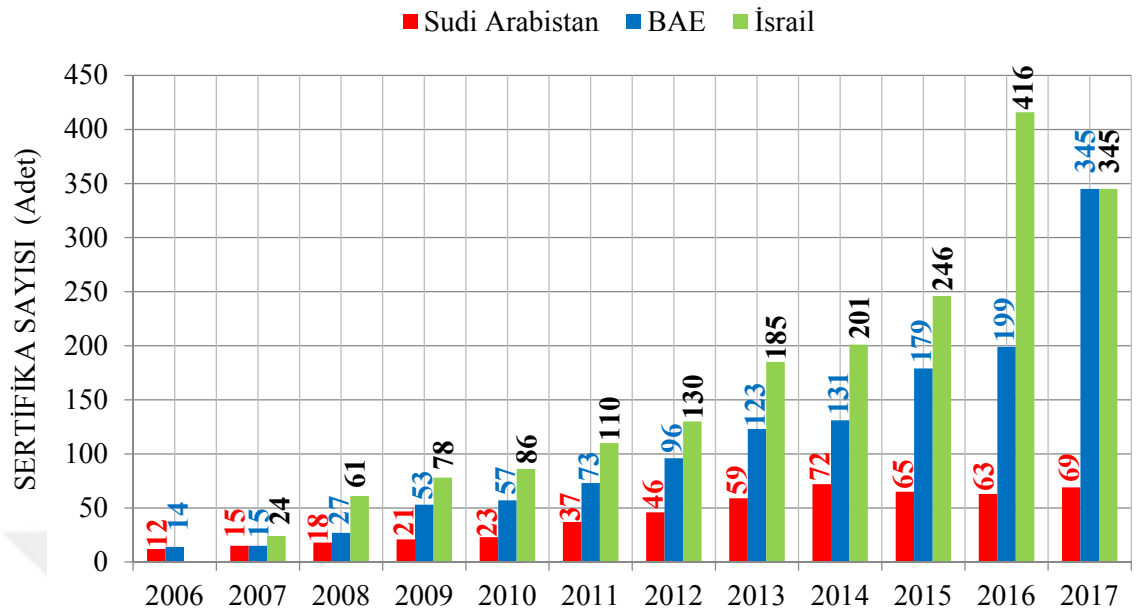



**Şekil 21. Sertifika Sayısına Göre Avrupa'daki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

Şekil 21'de Avrupa'nın sertifika dağılımında İngiltere'nin standartlarla ilgili çalışmalarda öncü olması sebebiyle sertifika sayısı diğer ülkelere göre oldukça yüksektir. Avrupa'nın en güçlü sanayi bölgesine sahip olan Almanya'nın son iki yılda sertifika sayısında artış sağladığı gözlemlenmektedir. ISO 27001 sertifika sayısına göre 2006 ile 2016 yıllarında Almanya'nın önünde olan İtalya'nın son yıllarda yaşamış olduğu ekonomik kriz nedeniyle sertifika sayısında düşüş yaşanmıştır.

Ortadoğu'da yer alan İsrail'in 2007 yılından sonra bilgi güvenliği, güvenlik yazılımları ve siber güvenlik konusunda atılımlar yaptığı Şekil 22'teki sertifika sayısındaki artıştan da görülmektedir. Petrol, enerji sektörünün yoğun olduğu ülkeler arasında yer alan Birleşik Arap Emirlikleri ve Sudi Arabistan'ın 2006 ve 2008 arasında sertifika sayıları birbirlerine yakın iken 2009 yılı sonrasında BAE sertifika sayısında artış yaşanmıştır. Sudi Arabistan'ın bölgede sertifika durumu nedeniyle üçüncü sırada yer almaktadır.



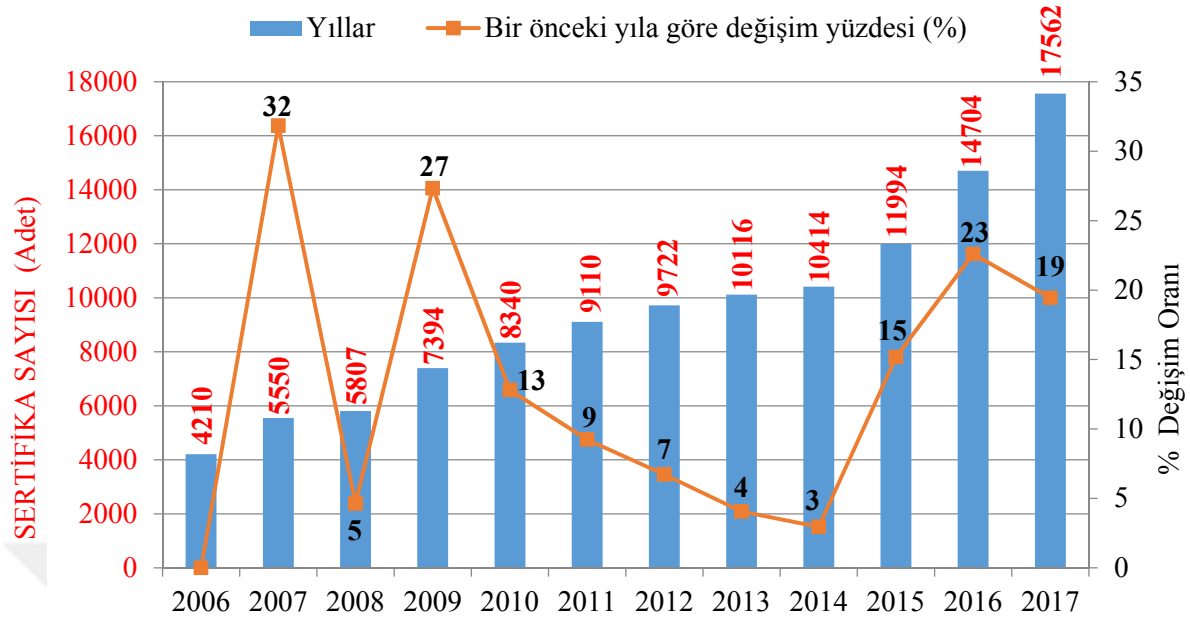

**Şekil 22. Sertifika Sayısına Göre Ortadoğu'daki İlk Üç Ülkenin Yıllara Göre Dağılımı**

Kaynak: (International Organization for Standardization, 2018)

### 4.1.3. Dünya'da ISO 27001 Standardının Bölgesel Sertifika Sayıları ve % Değişim Oranları

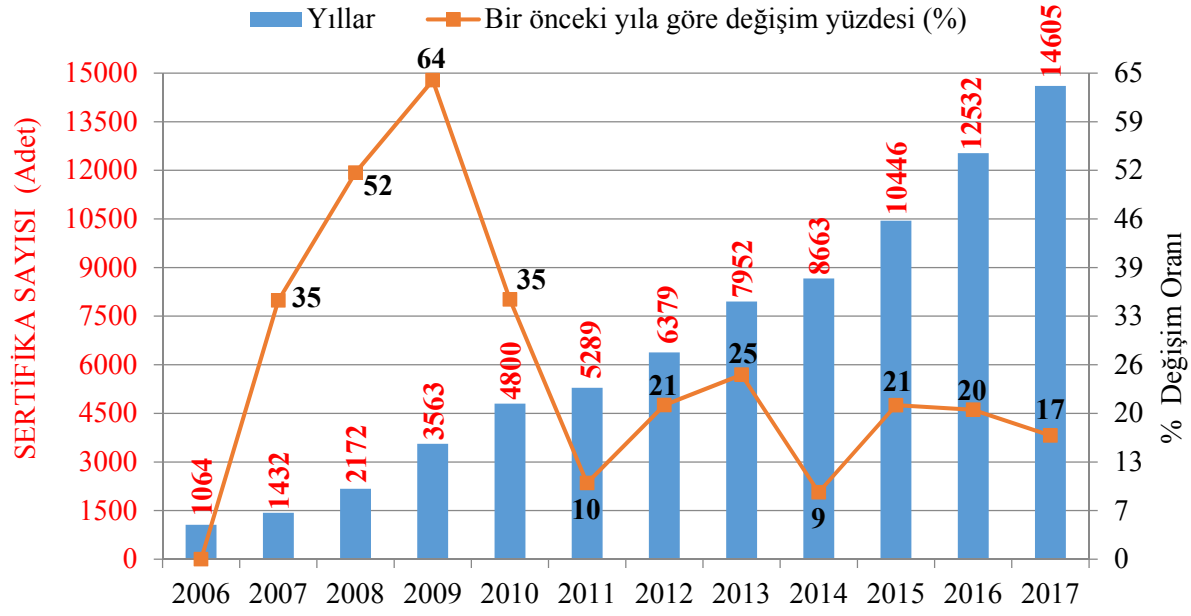
Doğu Asya ve Pasifik bölgesinde Japonya ve Çin gibi ülkelerin bulunması nedeniyle Dünya'da 17562 adet sertifika sayısı ve bölgesel sertifika dağılımıyla da ilk sırada yer almaktadır. 2006 - 2017 yılları arasındaki sertifika verileri analiz edildiğinde ise; 2007 ve 2009 yıllarında bir önceki yıla göre sertifika değişim oranlarının en yüksek seviyeye ulaştığı görülmektedir (Şekil 23).

Şekil 24'de Avrupa'nın bölgesel olarak sahip olduğu sertifika sayıları ve değişim oranları verilmektedir. ISO tarafından yayınlanan araştırma raporu verilerine göre 2017 yılında %37 bölgesel sertifika dağılım oranı ve sertifika sayısı sıralamasında Dünya'da ikinci olduğu görülmektedir. 2007'de %35, 2008'de %52, 2009'da ise %64 değişim oranıyla en yüksek seviyeye eriştiği gözlenmektedir.



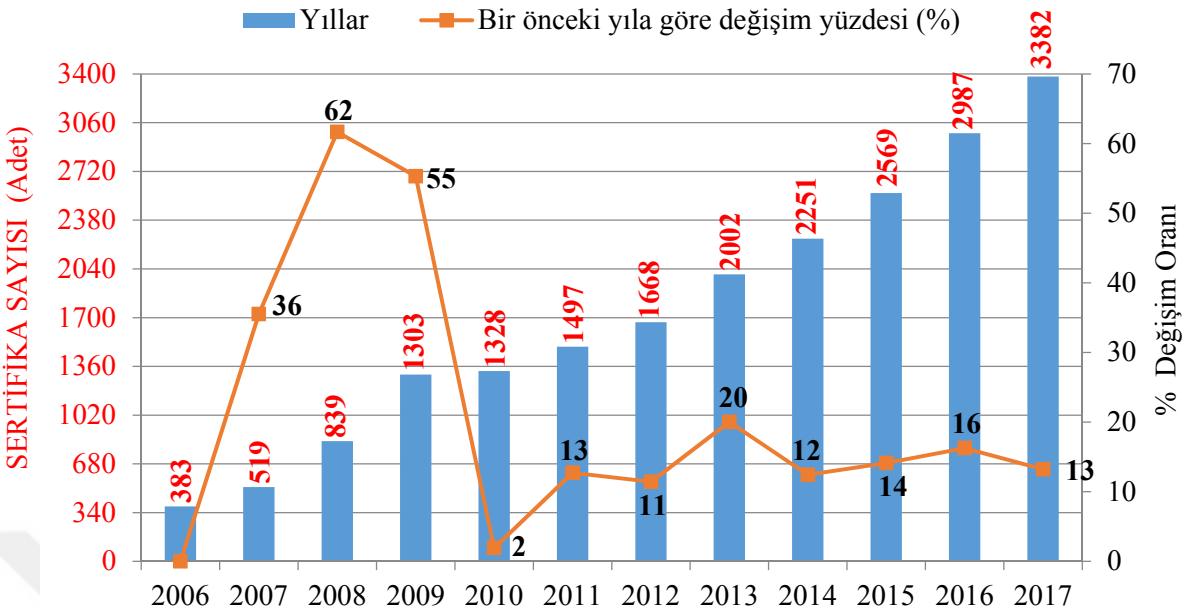

**Şekil 23. Doğu Asya ve Pasifik Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)




**Şekil 24. Avrupa Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

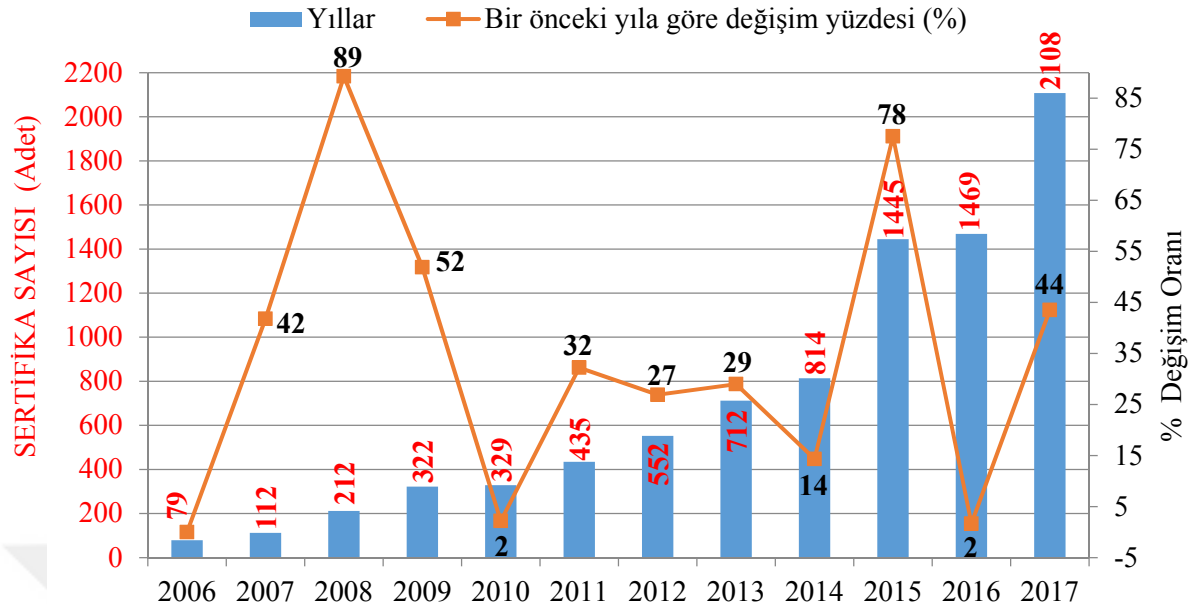



**Şekil 25. Orta ve Güney Asya Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

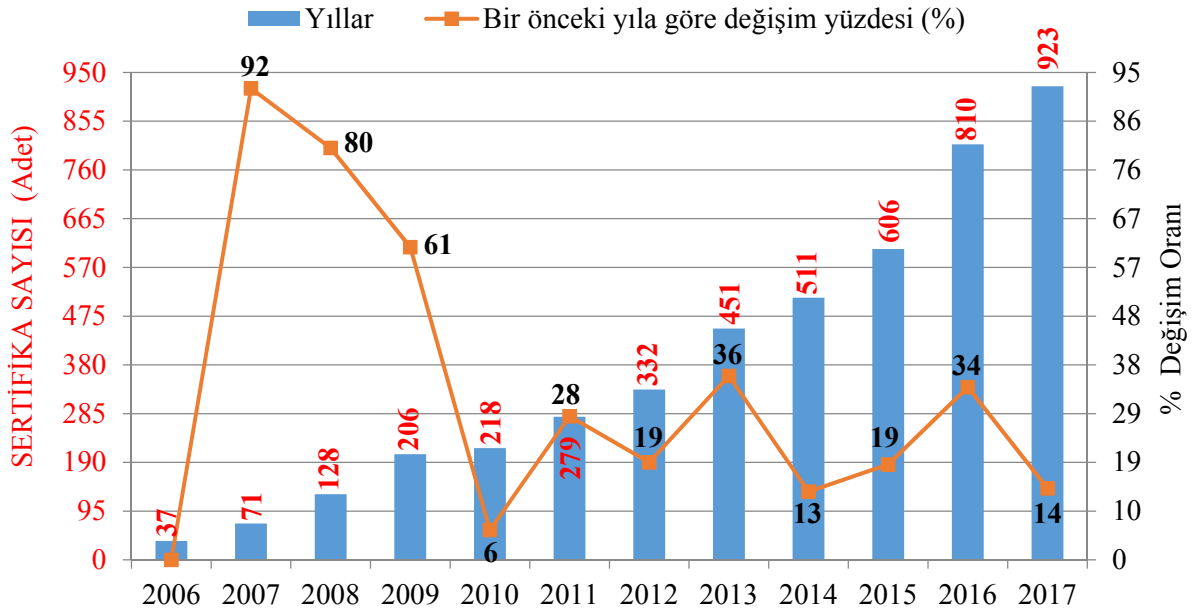
Orta ve Güney Asya sertifika sayıları Şekil 25'de incelendiğinde bir önceki yıla göre % 62 değişim oranıyla 2008 yılında en yüksek seviyeye ulaşmıştır. Bölgesel sertifika sayısına göre Dünya'da üçüncü sırada yer almaktadır. Bu bölgede yer alan Hindistan'ın sertifika sayısı nedeniyle önemli bir etki oluşturduğu ortaya çıkmaktadır. 2017 yılı itibariyle bölgenin toplamda 3382 adet sertifikaya sahip olduğu gözükmektedir.

Şekil 26'da yer alan Kuzey Amerika'nın bölgesel sertifika dağılımına göre Dünya'da dördüncü basamakta yer aldığı görülmektedir. Bir önceki yıla göre değişim oranlarına bakıldığında ise en yüksek seviyeye 2008 yılında ulaşmıştır. 2010 ve 2016 yıllarında sertifika değişim oranının en düşük seviyeye gerilediği ilerleyen yıllarda bilgi güvenliği konusunda ilginin arttığı gözlemlenmektedir. Yayınlanan araştırma raporuna göre Kuzey Amerika'da 2006'da toplam 79 olan sayının 2017 yılı itibariyle toplam 2108 adet sertifikaya sahiptir.




**Şekil 26. Kuzey Amerika Sertifika Sayıları Ve Değişim Oranları**

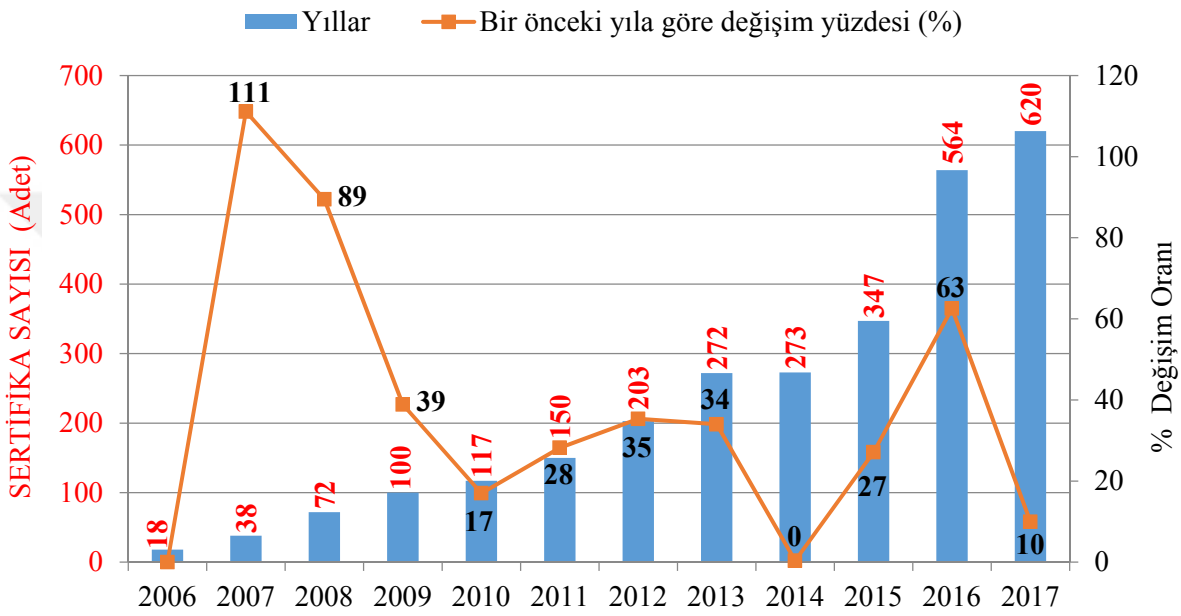
Kaynak: (International Organization for Standardization, 2018)




**Şekil 27. Ortadoğu Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

Ortadoğu'nun bir önceki yıla göre değişim oranlarına bakıldığında %92 oranı ile en yüksek seviyeye 2007 yılında ulaşmış, en düşük değişim oranın ise 2010 yılında olduğu görülmektedir (Şekil 27). Bölgesel sertifika dağılımına göre Ortadoğu Dünya'da beşinci sırada yer almaktadır.



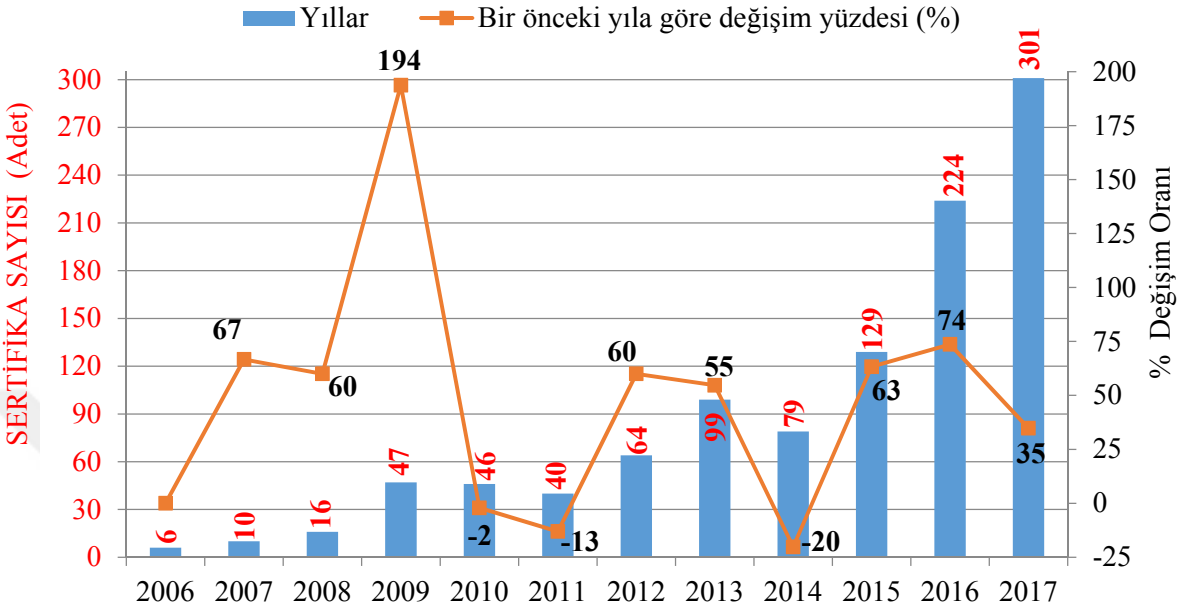

**Şekil 28. Orta Güney Amerika Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

Şekil 28'de yer alan Orta ve Güney Amerika bölgesinde 2006 yılında 18 adet sertifikaya sahip olduğu ilerleyen yıllarda artış yaşanmış ve 2017 yılında toplamda 620 adet ISO 27001 sertifikası bulunmaktadır. Bir önceki yıla göre en fazla değişim oranının 2007 yılında gerçekleştiği görülmektedir.

Afrika'nın bilgi güvenliği konusunda en düşük kapasiteye sahip olduğu Şekil 29'da görülmektedir. 2006 yılında 6 adet olan sertifika sayısının 2017 yılında ise toplamda 301 âdete ulaşmıştır. En fazla değişim oranının 2009'da %194 oranında yükseldiği gözlenmekte, değişim oranındaki en düşük % -20 oranıyla 2014'de

yaşanmıştır. Dünya'da Afrika'nın bölgesel sertifika dağılımında ortalama %0,8 oranla temsil ettiği tespit edilmiştir.




**Şekil 29. Afrika Sertifika Sayıları Ve Değişim Oranları**

Kaynak: (International Organization for Standardization, 2018)

### 4.1.4. Dünya'da ISO 27001 Standardının İlk 10 Ülke Dağılımı

ISO/IEC 27001 standardı tüm ülkeler ve kuruluşlar için genel bir standart olsa da bazı ülkelerde bu standardın geniş kapsamlı bir şekilde yaygınlaşmadığı ve benimsenmediği görülmektedir. ISO 27011 sertifika sayılarında ise her geçen yıl düzenli olarak artmaktadır. Örnek olarak ISO'nun yayınlamış oluğu araştırma raporuna göre 2016 yılına göre 2017 yılında sertifika sayısında %19 oranında artış göstermiştir. 2017 yılında ISO 27001 sertifikasına sahip olan ilk on ülkelere bakıldığı zaman; (Tablo 12.) hemen her ülkenin sertifika sayısının artış gösterdiği, sertifika sayısının yüksek olduğu Japonya ve İngiltere'nin küresel faaliyetleri nedeniyle bilgi güvenlik standardına yoğun ilgi göstermektedir. Çin'in büyüyen ekonomi ve teknolojisi sayesinde son iki yılda % 93,6 oranında sertifika sayısında en fazla artış olmuştur. Dünyanın büyük ekonomisine sahip olan Amerika Birleşik Devletleri sertifika 1517 adet sayısı ile % 36,1 oranında bir artış görülmektedir. Ülkeler arasında 8. sırada olan İtalya'nın ise diğer

yıllara göre % -21,5 sertifika oranıyla en çok düşüş yaşamıştır. Diğer ülkelere bakıldığı zaman ise Hindistan, Almanya, Tayvan, İspanya ve Hollanda'nın yer aldığı görülmektedir.

**Tablo 12. 2015-2017 Yıllarına Ait İlk 10 Ülkenin Sertifika Sayıları Ve % Değişim Oranları**

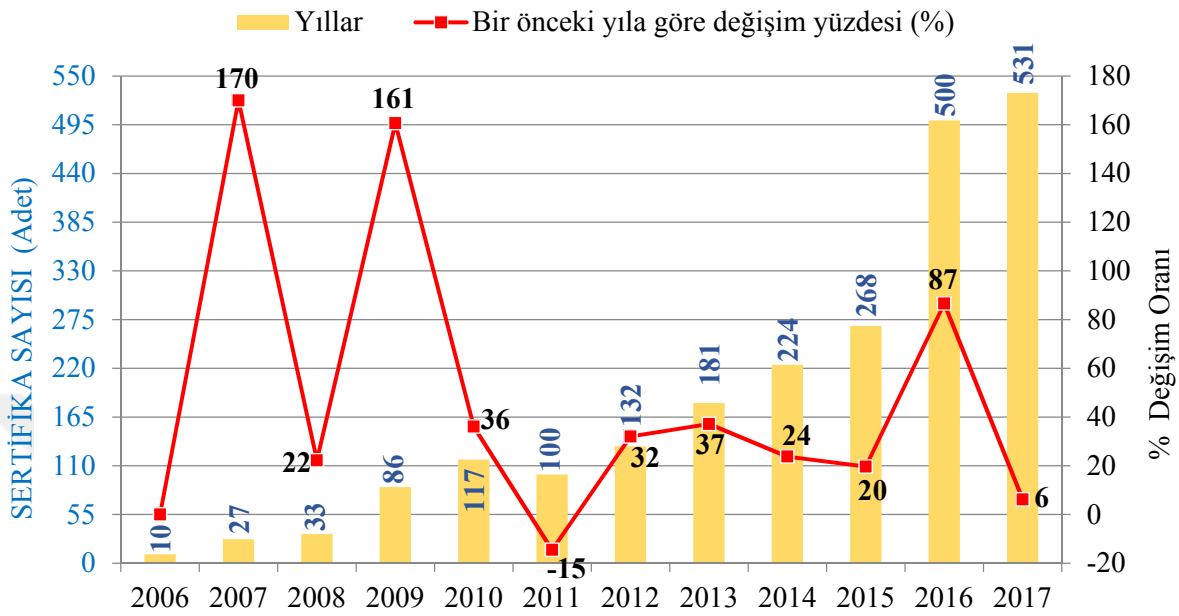
| | ÜLKE | 2016 | 2017 | % |
|---|---|---|---|---|
| **1** | Japonya | 8945 | 9161 | 2,4 |
| **2** | Çin | 2618 | 5069 | 93,6 |
| **3** | İngiltere | 3367 | 4503 | 33,7 |
| **4** | Hindistan | 2902 | 3272 | 12,7 |
| **5** | Amerika Birleşik Devletleri | 1115 | 1517 | 36,1 |
| **6** | Almanya | 1338 | 1339 | 0,1 |
| **7** | Tayvan | 1087 | 994 | -8,6 |
| **8** | İtalya | 1220 | 958 | -21,5 |
| **9** | Hollanda | 670 | 913 | 36,3 |
| **10** | İspanya | 752 | 803 | 6,8 |

Kaynak: (International Organization for Standardization, 2018)

## 4.2. ISO/IEC 27001 BİLGİ GÜVENLİĞİ STANDARDININ TÜRKİYE' DEKİ YERİ

Türkiye'deki sertifika sayısı bilgisine ulaşmak için bu konuda belgelendirme veren şirket ve kurumlara e-mail ve telefon ile başvuruda bulunulmuştur. Fakat bu konuda kuruluşların ilgili firma isimleri ve kapsamını ticari kaygılar nedeniyle her hangi bir veri paylaşımında ve yardımda bulunulmamıştır. Yapılan yoğun araştırmalar sonucunda ISO tarafından yayınlanan araştırma raporundan yararlanılarak 2006 - 2017 yılları arasında Türkiye'de verilen sertifika sayıları ve yıllara göre % değişim oranları aşağıdaki grafikte (Şekil 30) verilmiştir. Ülkemizde 10 yıl öncesi 10 adet olan sertifika sayısının ilerleyen yıllarda artış gösterdiği görülmekte bunun nedeni ise; işletmelerde kalite algısının ve bilgi güvenliğinin öneminin giderek artması, jenerik bir standart olmasıdır. Bunun yanı sıra bilgi güvenliği konusunda çıkarılan kanun, yönetmelik ve genelgelerin etkisi ile ülkemizdeki işletmeler ve kurumlar TS ISO/IEC 27001

standardına olan ilgisinin her geçen gün giderek artacağı görülmekte ve tahmin edilmektedir.




**Şekil 30. Türkiye'deki sertifika sayıları ve değişim oranları**

Kaynak: (International Organization for Standardization, 2018)

Şekil 30'da 2006 yılında Türk Standartları Enstitüsü'nün TS ISO/IEC 27001 standardın yayınlanmasından sonraki ilk yılda % 170 oranında artış yaşanmıştır. 2008'de Resmi Gazete'de yayımlanan Elektronik Haberleşme Güvenliği Yönetmeliği ile yıllarda e-devlet kapısı projesi, TUBİTAK, üniversiteler tarafından düzenlenen bilgi güvenliği konferansları ve etkinliklerinin neticesinde belediye, kamu kuruluşların ve özel şirketlerin bilgi güvenliği sertifikasına yönelmeleri sonucunda özellikle 2011 yılından itibaren sertifika sayısının düzenli olarak artığı görülmektedir.

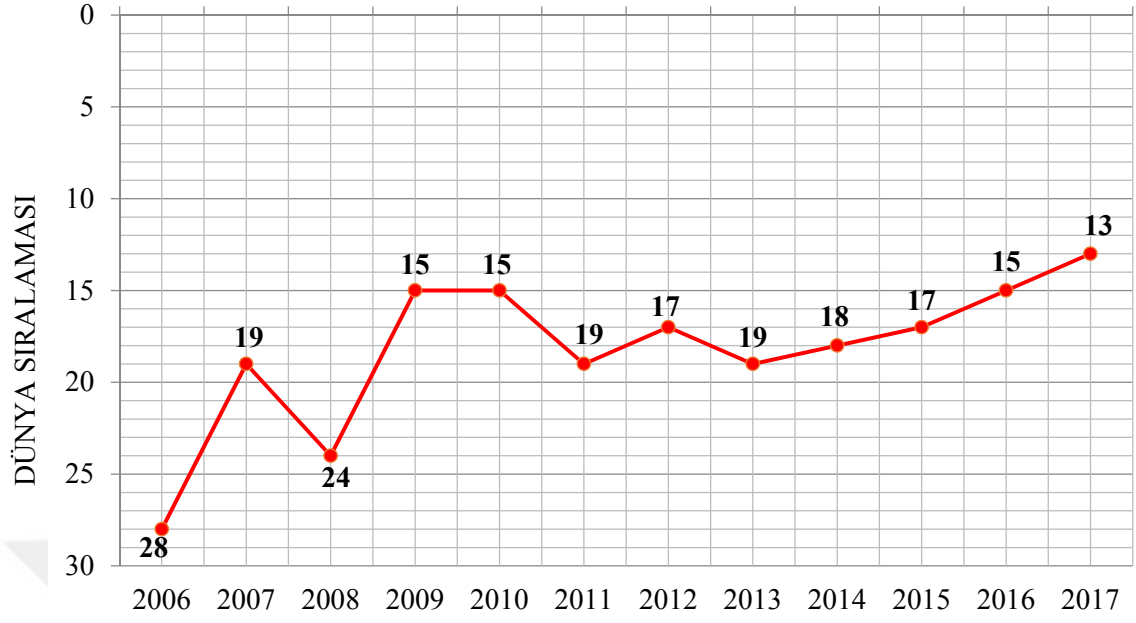
ISO'nun araştırma raporundan elde edilen verilerle oluşturulan 25 ülkenin ISO 27001 BGYS sertifika sayıları Tablo 13'de verilmektedir. Uluslararası düzeyde bakıldığı zaman Türkiye'nin 531 adet sertifika sayısı ile 2017 yılında Dünya genelinde ilk 25 ülke içerisinde 13. sırada yer almaktadır. Türkiye'nin sıralamadaki yerine bakıldığı zaman gelişmekte olan ülkelere nispeten daha üst sıralarda yer aldığı görülmektedir.

**Tablo 13. ISO/IEC 27001 Standardına Göre Sertifikalandırma Sayıları Ülke Sıralaması (2017)**

| S. No | Ülke Adı | Sertifika sayısı |
|---|---|---|
| 1 | Japonya | 9161 |
| 2 | Çin | 5069 |
| 3 | İngiltere | 4503 |
| 4 | Hindistan | 3272 |
| 5 | Amerika Birleşik Devletleri | 1517 |
| 6 | Almanya | 1339 |
| 7 | Tayvan | 994 |
| 8 | İtalya | 958 |
| 9 | Hollanda | 913 |
| 10 | İspanya | 803 |
| 11 | Yunanistan | 727 |
| 12 | Polonya | 705 |
| **13** | **Türkiye** | **531** |
| 14 | Macaristan | 472 |
| 15 | Çek Cumhuriyeti | 463 |
| 16 | Romanya | 440 |
| 17 | Avustralya | 404 |
| 18 | Güney Kore | 369 |
| 19 | İsrail | 345 |
| 20 | Birleşik Arap Emirlikleri | 345 |
| 21 | Fransa | 342 |
| 22 | Malezya | 317 |
| 23 | Meksika | 315 |
| 24 | Tayland | 287 |
| 25 | Kanada | 276 |

Kaynak: (International Organization for Standardization, 2018)

Dünya genelinde yıllara göre ülkelerin ISO/IEC 27001 sertifika sıralamasında Türkiye'nin (Şekil 31) 2006 yılında sertifika sayısına göre 28. sırada yer alırken, 2008 yılında bu sıralamada 24. sıraya gerilerken, son on bir yıl istatistiğine bakıldığında ise 15 basamak atlayarak 2017 yılında; ülkeler arasında 13. sırada yer almaktadır. Dünyadaki teknolojik gelişmelere ayak uydurmak, Avrupa Birliği aday ülke olması nedeniyle meydana gelebilecek siber saldırılara ve bilgi kayıplarını önlemek için ülkemizde gerekli BGYS çalışmaları devam etmektedir.




**Şekil 31. Türkiye'nin sertifika sayısına göre Dünya'daki sıralaması**

Kaynak: (International Organization for Standardization, 2018)

### 4.2.1. Türkiye'de ISO 27001 Standardının Şehirlere Göre Dağılımı

Türkiye'de ISO 27001 standardı sertifika sayısı konusunda literatür araştırmaları ve internette çeşitli kaynaklarda aramalar yapılmış fakat bu yapılan araştırmalar sonucunda güncel verilere erişilememiştir. Bu nedenle çalışmamızda farklılık oluşturması için, sertifikasyon ve akreditasyon konusunda tek yetkili kuruluş olan TÜRKAK'a dilekçe ile başvuru yapılarak bu konudaki istatistiki bilgiler talep edilmiştir. Yapılan başvuru kabul edilerek gizlilik ilkesi dahilinde; TÜRKAK tarafından mevcut istatistiki bilgiler tarafımıza ulaştırılmıştır. TÜRKAK tarafından belgelendirme konusunda akredite yapılan kurum ve kuruluşlara ilişkin bazı bilgi ve kayıtların girildiği TÜRKAK Belge Doğrulama Sistemi (TBDS) portalından elde edilmiştir. Bu platform 2017 yılında oluşturulmuş ve hizmete sunulmuştur. Sunulan bilginin güncel ve doğruluğu akredite olan firmalar tarafından girilen bilgilerden oluşmaktadır. 2015-2017 yılları arasında BGYS sertifikası konusunda ilk üç şehrin istatistiki bilgileri Tablo 14.'de verilmiştir. Şehirlerin sertifika dağılımına bakıldığında; tıpkı bölgesel olarak ülke dağılımında olduğu gibi burada da şehirlerin teknoloji kullanımı, gelişmiş sanayisi, iş ve nüfus yoğunluğunun etkili olduğu görülmektedir. Türkiye'nin gelişmiş sanayisi ve

ekonomisinde etkili olan İstanbul'un birinci sırada yer aldığı görülmekte, ikinci sırada ise Ankara'nın geldiği, otomotiv sektöründe öncü olan Bursa ise üçüncü sıradadır.

**Tablo 14. ISO 27001 Standardının 2015-2017 Yılları Şehirlere Göre Dağılımı**

| Sıra No | Şehir | 2015 | 2016 | 2017 |
|---|---|---|---|---|
| 1 | İstanbul | 72 | 228 | 315 |
| 2 | Ankara | 32 | 75 | 150 |
| 3 | Bursa | 3 | 11 | 18 |

Kaynak: (Türk Akreditasyon Kurumu, 2018)

Dünya'da sektör bazında sunmuş olduğumuz sertifika sayısı ve dağılım konusundaki benzer çalışma için; Ülkemizde bu konu ile ilgili internette çeşitli kaynaklarda aramalar yapılmış fakat bu yapılan araştırmalar sonucunda bu verilere rastlanılmamıştır. Bu konu ile ilgili olarak TÜRKAK' başvuru yapıldığında ise mevcut veri tabanında sektör bilgisinin olmadığı görülmüştür. Bu nedenle bu konuda ISO/IEC 27001 standardı sektörel dağılımına rastlanamamıştır. TÜRKAK'a yaptığımız başvuru gibi diğer ISO/IEC 27001 standardı konusunda belgelendirme yapan özel şirketlere de e-mail, telefon aracılığıyla ulaşılmış bu konudaki bilgiler, istatistikler onlardan da talep edilmiştir. Fakat bu konuda gelen cevapların çoğunluğunda ise ticari kaygılar sebebiyle üçüncü şahıslarla paylaşılamayacağı ifade edilmiştir.

### 4.2.2. Ülkemizde BGYS Belgelendirmesi Yapan Kuruluşlar

Türkiye'de uluslararası akreditasyon yapan aynı zamanda Avrupa Akreditasyon Kurumu (EA)'nın üyesi olan kuruluş TÜRKAK'tır. 27.10.1999 tarih ve 4457 sayılı yasa ile kurulan görevleri arasında; belgelendirme, uygunluk değerlendirme kuruluşlarını akredite edilmesi, bu kuruluşların uluslararası standartlara göre faaliyetlerde bulunmaları sağlamak, bu suretle uygunluk değerlendirme kuruluşlarınca düzenlenen belgelerin uluslararası alanda kabulünü temin etmek amacıyla tüzel kişiliğe sahip olan kar amaçlı olmayan bir kurumdur (Demirtaş, 2013). Türkiye'de uluslararası geçerliliğe sahip olan ve TÜRKAK tarafından akredite edilen BGYS Belgesini veren belgelendirme kuruluşları aşağıdaki Tablo 15.'teki gibidir.

**Tablo 15. TÜRKAK'a Akredite ISO/IEC 27001 Belgelendirme/Tescil Kuruluşları**

| | **Belgelendirme Kuruluşu Adı** |
|---|---|
| **1** | A1 Belgelendirme Ve Muayene Hizmetleri Ltd. Şti. |
| **2** | AND Uluslararası Denetim Ve Gözetim Hizmetleri Ticaret Ve Limited Şirketi |
| **3** | Artıbel Belgelendirme Teknik Kontrol Gözetim Ve Eğitim Hizmetleri Ltd. Şti. |
| **4** | ASB Uluslararası Belgelendirme Gözetim Denetim Ve Eğitim Hizmetleri Ltd. Şti. |
| **5** | BBS Belgelendirme Eğitim Ve Gözetim Hizmetleri A.Ş. |
| **6** | BSI Group Eurasıa Belgelendirme Hizmetleri Ltd. Şti. |
| **7** | Bureau Veritas Gözetim Hizmetleri Ltd. Şti. |
| **8** | Cicert Belgelendirme Hizmetleri Ltd. Şti. |
| **9** | CTR Uluslararası Belgelendirme Ve Denetim Ltd. Şti. |
| **10** | Denetik Uluslararası Belgelendirme Ve Gözetim Hizmetleri Ltd. Şti. |
| **11** | Digicert Belgelendirme Ltd. Şti. |
| **12** | DQS Denetim Ve Belgelendirme Ltd. Şti. |
| **13** | DSR Uluslararası Gözetim Ve Belgelendirme Hizmetleri Ltd. Şti. |
| **14** | EAC Belgelendirme Ve Eğitim Hizmetleri A. Ş. |
| **15** | IFC GLOBAL Sertifikasyon Muayene Ve Eğitim Hizmetleri A.ş. |
| **16** | INSPECT Uluslararası Belgelendirme Ve Gözetim Hizmetleri Tic. Ltd. Şti. |
| **17** | IQNORM Uluslararası Belgelendirme ve Muayene Test Hizmetleri Tic. A.Ş. |
| **18** | Kalitest Belgelendirme Ve Eğitim Hizmetleri Ltd. Şti. |
| **19** | KBM Teknik Kontrol Ve Belgelendirme Limited Şirketi |
| **20** | Kiwa Belgelendirme Hizmetleri A.Ş. |
| **21** | MSC Uluslararası Belgelendirme Teknik Kontrol Ve Özel Eğitim Hiz. Dış Tic. Ltd. Şti. |
| **22** | Naviga Uluslararası Belgelendirme Ve Eğitim Hizmetleri Ltd. Şti. |
| **23** | Proks Belgelendirme Ve Özel Eğitim Hizmetleri Ltd. Şti. |
| **24** | ROYALCERT Belgelendirme Ve Gözetim Hizmetleri Anonim Şirketi |
| **25** | S.G.S. Supervise Gözetme Etüd Kontrol Servisleri A.Ş. |
| **26** | TGS Uluslararası Belgelendirme Teknik Kontrol Ve Gözetim Hizmetleri Ltd. Şti. |
| **27** | TRB Uluslararası Belgelendirme Teknik Kontrol Ve Gözetim Hizmetleri Tic. Ltd. Şti. |
| **28** | Türk Loydu Uygunluk Değerlendirme Hizmetleri A.Ş. |
| **29** | Türk Standardları Enstitüsü |
| **30** | TÜV Austria Türk Belgelendirme Eğitim Ve Gözetim Hizmetleri Ltd. Şti. |
| **31** | TÜV Teknik Kontrol Ve Belgelendirme A.Ş. |
| **32** | UKS Uluslararası Kalite Sistemleri Ve Belgelendirme Ltd. Şti. |
| **33** | Universal Sertifikasyon Ve Gözetim Hizmetleri Tic. Ltd. Şti. |
| **34** | VERİCERT Belgelendirme Ve Gözetim Hizmetleri Ltd. Şti. |
| **35** | Yönetim Belgelendirme Merkezi Test Ve Gözetim Hizmetleri Ltd. Şti. |

Kaynak: (Türk Akreditasyon Kurumu, 2018)

### 4.2.3. Ülkemizde BGYS Uygulamaları ve Yasal Şartlar

Yasal şartlar aşağıda belirtilen yönetmeliklerde açıklanmıştır:

**1.** Kamu kurum ve kuruşlarının KamuNet ağına dahil olmaları ile ilgili Başbakanlık Genelgesi (2016/28), 3 Aralık 2016 tarihinde Resmi Gazete 'de yayımlanarak yürürlüğe girmiştir. Genelgeye göre; "KamuNet (Kamu Sanal Ağı); kamu kurum ve kuruluşları tarafından içerik güvenliği sağlanan veri iletişiminin, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun altyapının tesis edilmesi ve oluşturulması, planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi amacıyla oluşturulmuştur." KamuNet Ağı'na Dahil Olmak İçin Asgari Güvenlik Gereksinimlerinden biri olan "Bilgi Güvenliği Yönetim Sistemi (BGYS) kurularak tüm süreçler ile ilgili siber güvenlik politikaları ve prosedürleri oluşturulmalı (ISO 27001 standardına uyumlu hale getirilmeli)," maddesi kamu kurum ve kuruluşlarında bir Bilgi Güvenliği Yönetim Sistemi kurulması gerekliliğini ortaya koymuştur.

**2.** Elektronik haberleşme şebekesi sağlayan ve altyapısını işleten sermaye şirketlerin/kurumların, BTK tarafından elektronik haberleşme hizmeti sunan ve/veya 20.07.2010 tarihinden itibaren TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alması zorunlu hale getirilmiştir (Elektronik Haberleşme Yönetmeliği'nin ilgili, "İşletmecilerin Yükümlülükleri Elektronik Haberleşme Güvenliğini Sağlama Yükümlülüğü" maddesinde; İşletmeci, TS ISO/IEC 27001 veya TS ISO/IEC 27001 standardına uygunluğu sağlamakla yükümlüdür" denmektedir).

**3.** Gümrük İşlerini Kolaylaştırma Yönetmeliği Kapsamında Yetkili Yükümlü Sertifikası (YYS) alacak ithalat ve ihracatçıların ISO/IEC 27001:2013 Belgesi alması zorunluğu; Gümrük ve Ticaret Bakanlığı'na bağlı Risk Yönetimi ve Kontrol Genel Müdürlüğünün Yetkili Yükümlü Sertifikası alacak firmalarda başvurularda arayacağı belgeler arasında ISO/IEC 27001 Belgesi alma zorunluluğu getirilmiştir. 10 Ocak 2013 tarihli "Gümrük İşlemlerini Kolaylaştırma Yönetmeliği" tüm ihracat ve ithalatçıları ilgilendiren maddeler içermektedir. İlgili yönetmeliğin 10. maddesinde yer alan, "Başvuru için aranacak belgeler" kısmında, istenen belgeler arasında, "Avrupa Akreditasyon Birliğinin karşılıklı tanıma anlaşmalarına imza atmış akreditasyon

kurumları tarafından akredite edilmiş uygunluk değerlendirme kuruluşlarınca düzenlenecek ve akreditasyon kurumunun markasını taşıyan, güncel ISO 9001 ve TS ISO/IEC 27001 sertifikalarının aslı veya düzenleyen kuruluş tarafından onaylı örneği" yer almıştır.

**4.** Maliye Bakanlığı Gelir İdaresi Başkanlığı E-fatura Özel Entegratörlük için başvuru yapan firmalara TS ISO/IEC 27001 Belgesi alınması zorunluluğu getirilmiştir (Maliye Bakanlığı Gelir İdaresi Başkanlığı e-Fatura Uygulaması Kılavuzunda; "Özel entegratör bilgi güvenliği için TS ISO IEC 27001 veya ISO 27001 Belgesi'ne sahip olmalıdır" ifadesi yer almıştır).

**5.** Elektrik Piyasası Düzenleme Kurulu (EPDK) Elektrik Piyasası Lisans Yönetmeliği'ne göre TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alınması zorunluluğu; Enerji Piyasası Düzenleme Kurumu (EPDK) Lisans Yönetmeliklerinde değişiklik yaparak, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi'ni zorunlu hale getirmiştir. 26.12.2014 tarihli ve 29217 sayılı Resmi Gazete 'de yayımlanan değişikliklerle, lisans sahiplerine 01.03.2016'dan itibaren Türk Akreditasyon Kurumu'ndan (TÜRKAK) akredite bir belgelendirme kuruluşundan ISO/IEC 27001 Belgeli olma zorunluluğu getirilmiştir.

### 4.3. ISO/IEC 27001 BİLGİ GÜVENLİĞİ STANDARDININ KONYA'DAKİ YERİ

ISO/IEC 27001 BGYS sertifika sahip firmaların listesi konusunda istatistiksel bilgiler için TSE ye başvuruda bulunmuştur. Bunun yanı sıra tez çalışmasında kullanılmak üzere sertifika ya olan kurum ve işletmeler araştırma yapılarak tespit edilmiştir. Bu çalışma neticesinde Konya ilinde sertifikaya sahip firmaların sektörleri; makine imalatı, enerji ekipmanları imalatı, hidrolik ekipmanları imalatı, enerji dağıtımı, tarım gübre ilaç üretimi yapan 5 adet firmaya ulaşılarak bu konuda mülakat ve görüşmeler yapılmıştır. Bu bölüme tezin ilerleyen kısımlarında yer verilmiştir. Bu firmalar incelendiği zaman sertifikasyon işlemlerini belgelendirme kuruluşları olan Kiwa -Meyer Danışmanlık, INSPECT Uluslararası Belgelendirme, TSE ve Kalitetürk danışmanlık firmalarından destek aldıklarını ifade etmişlerdir.

# BEŞİNCİ BÖLÜM
# ISO 27001 BGYS HAKKINDA YAPILAN MÜLAKAT SONUÇLARI

## 5.1. ARAŞTIRMANIN KONUSU

Konya'daki kurum, işletmelerin bilgi güvenliği yönetim sistemleri konusunda uygulama sorunlarının incelenmesi, bu konuda yapılan çalışmaları ve farkındalıklarının ne düzeyde olduğunun belirlenmesi ve çözüm önerileri sunmaktır.

Dünya'da, Türkiye'de standartla ilgili bilinirliğinin ve mevcut istatistiki bilgilerin analiz edilmesi bu konuda yapılmış çalışmaların incelenmesidir. Uluslararası kabul gören standardın tanınmasını sağlamak, bu konuda işletmelerde yapılan çalışmaların uygulama aşamaları inceleme yapılmıştır.

## 5.2. ARAŞTIRMANIN AMACI

Bilgi güvenliği, bilginin öneminin her geçen gün artması nedeniyle Konya'daki kurum ve işletmelerin belgelendirme kuruluşlarından aldıkları sertifikasyon süreçlerinin incelenmesi bilgi güvenliği konusunda çalışma yapabilecek kurum, işletmeler için bir yol gösterilmesi amaçlanmıştır. Bilgi güvenliği konusunda yapılmış akademik çalışmalar arasında elle tutulur istatistiki verilerin daha anlaşılır olması için bir inceleme örneği kazandırılması için nitel bir çalışma amaçlanmıştır.

İşletmelerin bilgi güvenliği yönetim sistemlerini kurma gerekçeleri, kurulum çalışmaları ele alınmış mevcut kurulu yönetim sistemlerinin uygulama sorunlarının araştırma yapılarak çözüm önerileri sunulmaya çalışılmıştır. Bilgi güvenliğinin işleyişi işletmelerin günlük yaşamın bir parçası halinde olması sağlanarak sistemin sürekli olması amaçlanmıştır. Bu konuda işletmeler için bilgi güvenliği modellemesi yapılarak risk değerlendirmesi konusunda tahmin yapılabilmesi, bilgi güvenliği analizleri ile zayıf ve güçlü noktaların tespitini sağlamaktır.

## 5.2. ARAŞTIRMANIN YÖNTEMİ

Araştırma Konya ilinde bulunan ISO/IEC 27001 sertifikasına sahip olan işletmelerin tespitinin ardından mülakat konusunda gerekli izinlerin alınması ile başlanılmıştır. BGYS konusunda çalışma yapan işletmelerin yönetim, toplam kalite yöneticisi veya sorumlusu ile görev alan personeller ile yüz yüze görüşme yapılarak veriler toplanmıştır. Sertifika sahibi olan işletmelerin farklı sektörlerde olması araştırmanın çeşitliliğini ve zenginliğini arttırmıştır. Tez çalışmasında daha tutarlı veriler, istatistiki bilgiler elde etmek için, ISO'nun Dünya genelinde her yıl yayınlamış olduğu araştırma raporu incelerek analizi ve dökümü yapılmıştır. TÜRKAK, TSE, TÜBİTAK ve ISO 27001 konusunda yetkilendirilmiş belgelendirme kuruluşların yapmış olduğu faaliyetler incelenmiştir. Araştırmamızda TSE'nin TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi temel eğitimi dokümanları ve TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü'nün hazırlamış olduğu kılavuzlar tez çalışmasında yararlanılan başlıca kaynaklardan biri olmuştur. Bilgi güvenliği konusunda yayınlanmış olan doktora, tez, makalelerin taraması yapılarak incelenmiş araştırmanın geniş kapsamlı olması için bu konuda düzenlenen seminerler, konferanslardan yararlanılmıştır.

## 5.3. ARAŞTIRMANIN MÜLAKAT SONUÇLARI

Araştırmamızda Konya'da bulunan ISO/IEC 27001 sertifikasına sahip olan beş işletmelerin hepsinde, toplam kalite yöneticisi, bilgi işlem personeli ve yönetim temsilcisi ile görüşmeler yapılmış, yapılan çalışmalar hakkında bilgiler alınmıştır. Konu ile ilgili olarak mülakat analiz sonuçları aşağıda verilmiştir.

Mülakat yapılan işletmelerin mevcut sektörleri ile Avrupa Topluluğunda Ekonomik Faaliyetlerin İstatistiki Sınıflamasına göre (NACE) kodları Tablo 16'da verilmiştir. NACE kodlarına göre sınıflandırılmış aynı sektörde faaliyet gösteren diğer işletmelerin tespiti için araştırma yapılmıştır. Bu araştırmada Konya Ticaret Odası'na kayıtlı üyelerin bulunduğu veri tabanı kullanılmıştır. A işletmesinin bulunduğu sektörde dokuz, B işletmesinin bulunduğu sektörde on dört, C, D işletmelerinin bulunduğu

sektörde yüz üç, E işletmesinin bulunduğu sektörde ise üç adet işletme olduğu tespit edilmiştir.

**Tablo 16. Mülakat Yapılan İşletmelerin Sektörleri ve Nace Kodları**

| Firmalar | Firma Sektörü | Nace Kodu |
|---|---|---|
| A İşletmesi | Enerji dağıtım | 35.13.01 |
| B İşletmesi | Enerji ekipmanları imalat | 28.21.10 |
| C İşletmesi | Hidrolik ekipmanları imalat | 28.12.05 |
| D İşletmesi | Makine imalat | 28.12.05 |
| E İşletmesi | Tarım gübre ilaç üretimi | 20.20.11 |

Bilgi güvenliği yönetimi hangi işletmeler uygulayabilir bölümünde değinildiği gibi, sektörlerin risk grubuna bakıldığında ise makine imalat, enerji ekipmanları imalatı, hidrolik ekipmanları imalatı, enerji dağıtımı orta risk grubunda, tarım gübre ilaç üretiminin yüksek risk grubunda faaliyet gösterdiği ortaya çıkmıştır.

Bilgi güvenliği yönetim sistemleri sadece; bilişim teknolojilerini kapsadığı gibi; bilgisayar kullanan, kullanmayan bilginin hangi formda olursa olsun buna bir şekilde erişebilen ve kullanan tüm personelleri de kapsadığı görülmektedir. Mülakat yapılan tüm işletmeler incelendiğinde bu konuya titiz bir şekilde yaklaşıldığı görülmüştür. İşletmelerin çalışan sayılarına bakıldığında Tablo 17'de dört işletmede 100 ila 250 kişi çalışırken, bir işletmede ise 2500 üzeri çalışanı olduğu tespit edilmiştir.

**Tablo 17. Mülakat Yapılan İşletmelerin Çalışan Sayıları**

| Firmalar | Çalışan Sayısı |
|---|---|
| A İşletmesi | 2800 |
| B İşletmesi | 100 |
| C İşletmesi | 150 |
| D İşletmesi | 220 |
| E İşletmesi | 250 |

Bilginin günümüzde her geçen gün değerli olması nedeniyle işletmelerin iş sürekliliğinin devam etmesi, prestij kaybının önlenmesi, risklerin en düşük seviyeye indirilmesi, rekabet avantajı sağlamak, işletmelerin oluşan hata veya kasıtlı durumlar sonucunda telafisi zor olan bilgi kayıpları ve olayların neticesinde oluşan tecrübelerle bu konuda önlemler almaya gitmişlerdir. Diğer bir durum ise; işletmelerin faaliyet göstermiş oldukları sektörlerin risk durumlarına, devletlerin bilgi güvenliğine özel yasa ve yönetmeliklerle bu konunun teşvik edilmesi veya zorunlu hale getirilmesi sonucunda işletmeler bilgi güvenliği yönetim sistemlerine yönelmişlerdir.

BGYS kurulma amacına göre mülakat yapılan işletmelerin (Tablo 18) durumları incelendiğinde; % 80 oranındaki işletmelerini, 4458 sayılı Gümrük Kanunu Yönetmeliğine istinaden işletmelerin kendi bünyelerinde ithalat, ihracat yapabilmeleri için tercihleri % 80 gibi bir oranla bu yönde olmuştur. A işletmesinin enerji dağıtım sektöründe olması nedeniyle EPDK'nın yayınlamış olduğu yönetmeliklerin yanı sıra işletmelerin kurumsal kimlik çalışmaları bu konuda karar alınmasında oldukça etkili olduğu ortaya çıkmıştır.

**Tablo 18. BGYS Kurulma Amacının Nedenleri**

| **Firmalar** | **BGYS Kurulma Amacının Nedeni** |
|---|---|
| A İşletmesi | EPDK Yönetmeliği, Kurumsal Kimlik ve Bilgi Güvenliği |
| B İşletmesi | 4458 sayılı Gümrük Kanunu Yönetmeliğine istinaden |
| C İşletmesi | 4458 sayılı Gümrük Kanunu Yönetmeliğine istinaden |
| D İşletmesi | 4458 sayılı Gümrük Kanunu Yönetmeliğine istinaden |
| E İşletmesi | 4458 sayılı Gümrük Kanunu Yönetmeliğine istinaden |

İşletmelerin kuruluş amaçlarına bakıldığı zaman varlıklarını uzun süre sürdürmek, en önemli amaçları ise kar elde etmek ve arttırmaktır. Aynı amaç doğrultusunda BGYS uygulayan işletmelere iş dünyasında ayrıcalıklar sağladığı gibi bir takım kazanımlar sağlamaktadır. Mülakat yapılan işletmelerin cevap ve kazanımları Tablo 19.'da verilmiştir. İşletmelerin geneline bakıldığında risk analizi ve yönetimi hakkında yapmış

oldukları çalışmaların değer kattığı, bunun yanında ise iki kuruluşun imaj konusunda kazanımları oldukları görülmektedir. İşletmelerin BGYS belli bir disiplin, politika ile yürütülmesi sonucunda kazanımlar sağlamaktadır. Örneğin; bilgi işlem sistemlerinin daha iyi yönetilmesi, yasal yükümlülüklerden doğabilecek sorun ve sorumluluklara karşı işletmeleri koruma, güvence altına almaktadır. İşletmelerin uluslararası geçerlilikte sahip oldukları BGYS sertifikasının kuruluş tarafından uygulama amacına, ilgili olduğu sektörüne göre hemen her alanda mutlaka fayda ve kazanımlar sağlayacaktır.

**Tablo 19. BGYS Uygulayan İşletmelerin Kazanımları**

| **Firmalar** | **BGYS Uygulayan İşletmelerin Kazanımları** |
|---|---|
| A İşletmesi | Risklerin analizi, kurumsal imaj, bilgi güvenliği yönetimi |
| B İşletmesi | Risk analizi, imaj ve prestij kazanımı, güvenlik politikaları |
| C İşletmesi | Bilgi güvenliği yönetimi, risk analizi |
| D İşletmesi | Bilginin önemi ve değeri, rekabet gücünü arttırması, risk analizi |
| E İşletmesi | Bilgi işlem sistemlerinin iyi yönetimi, risklerin yönetimi |

BGYS bazı işletmeler tarafından bir proje olarak görülmekte, temeline bakıldığında ise canlı bir süreç olduğu gözükmektedir. Sistemin kurulum aşamaları, adımları hedef süreleri belirlenmeli buna göre kaynak yönetimi planlanmalıdır. İşletmelerin büyüklüklerine, yapılarına, bulunduğu sektör, varlık envanteri ve risk yapısına göre BGYS kurulum süreleri farklılık gösterebilmektedir.

Mülakat yapılan firmalardan A işletmesinin çalışan sayısı ile büyüklüğü göz önünde bulundurulduğunda kurulum süresinin 2 yıl gibi bir sürece yayıldığı görülmektedir. İşletme içerisinde etkin, bilgi güvenliği yönetim sistemi temel eğitimlerinin yanında, dokümantasyon ve iç tetkik eğitimlerini tamamlamış bu konularda yönetimin temsilcisi olabilecek yetkili personel veya bir ekip var ise konuda danışmanlık hizmeti alıp alınmaması konusunda sistem sekteye uğramamaktadır. Aksi taktirde eğitim ve yetkinlik konusunda yeterli personel olmadığı durumlarda danışmanlık alındığı görülmüştür.

D işletmesinde olduğu gibi ISO 9001 sertifikasyonu vb. diğer kalite belgesinin olması durumunda bu sürecin daha hızlı işlediği, dokümantasyon çalışmasının daha kolay yapıldığı görülmektedir. İşletmelerin BGYS kurulum süreleri ve harcamış oldukları zaman Tablo 20'de verilmiştir.

**Tablo 20. BGYS Kurulum Süresi**

| Firmalar | BGYS Kurulum Süresi |
|---|---|
| A İşletmesi | 2 Yıl |
| B İşletmesi | 5 Ay |
| C İşletmesi | 1 Yıl |
| D İşletmesi | 3 Hafta |
| E İşletmesi | 3 Ay |

İşletmelerin genel yapılarında, amaçları arasında yer alan kurumsal hedeflere yönelik yapılan çalışmalar her zaman kalite olgusu içindir. Mülakat yapılan tüm işletmelere bakıldığında bünyelerinde mutlaka toplam kalite yöneticisi bulunmaktadır. ISO/IEC 27001 belgelendirmesi diğer kalite sertifikasyon çalışmalarının üzerine inşa edilerek, kalite yönetiminin canlı tutulması amaçlanmıştır. Tablo 21.'de işletmelerin ISO/IEC 27001 standardından önce uyguladıkları ve sahip oldukları kalite belgeleri verilmiştir.

**Tablo 21. Mülakat Yapılan Firmaların Diğer Kalite Belgeleri**

| Firmalar | Diğer Kalite Belgeleri |
|---|---|
| A İşletmesi | ISO 9001 |
| B İşletmesi | ISO 9001, ISO 14001, ISO 18001, TSE 12975, TSE-HYB, CE |
| C İşletmesi | ISO 9001, TSE-HYB |
| D İşletmesi | ISO 9001, EN ISO 3834-2, EN1090-2 |
| E İşletmesi | ISO 9001, OHSAS 18001, ISO 14001, TSE 17025 |

Her ne kadar işletmelerin kendi bünyelerinde toplam kalite yöneticisi bulunduğu halde; BGYS standardının sürekli genişleyen, gelişen ve güncel olması nedeniyle bir işletme haricindeki tüm işletmeler bu konuda tecrübeleri olan bir danışmanlık firması ve TÜRKAK tarafından akredite edilen belgelendirme kuruluşlarıyla çalıştıkları tespit edilmiştir. (Tablo 22).

**Tablo 22. BGYS Kurulum Sürecinde Çalışılan Belgelendirme Ve Danışman Firmaları**

| **Firmalar** | **BGYS Kurulum Sürecinde Çalışılan Kuruluşlar** |
|---|---|
| A İşletmesi | Gizlilik anlaşması nedeni ile paylaşılmadı |
| B İşletmesi | Mc Meda Danışmanlık - INSPECT Uluslararası Belgelendirme |
| C İşletmesi | Kalitetürk Danışmanlık, Yönetim Belgelendirme Merkezi |
| D İşletmesi | Kiwa - Meyer Danışmanlık |
| E İşletmesi | Danışman firması ile çalışılmamış, TSE den belgelendirme konusunda destek alınmış |

A işletmesi danışmanlık ve belgelendirme kuruluşu ile yapmış olduğu gizlilik anlaşması nedeniyle bu konuda bir isim paylaşımında bulunmamıştır E İşletmesi bu konuda herhangi bir danışmanlık firması ile çalışmamış fakat belgelendirme konusunda TSE ile çalışma yapılmıştır. Diğer üç işletme ise sertifikasyon konusunda danışmanlık ve belgelendirme kuruluşlarıyla çalışma yaptıkları belirlenmiştir. Belgelendirme sürecinde tüm işletmeler daha önce beraber çalışmış oldukları ve işletmelerinin yapısını, işleyişini bilen danışmanlık ve belgelendirme kuruluşlarını özellikle tercih etmişlerdir.

# SONUÇ VE ÖNERİLER

## SONUÇ

Günümüzde bilgi teknolojisinin baş döndürücü şekilde büyümesi ile birlikte internetin yaygınlaşması bilgiye erişimin kolaylaşması bilgiye olan bağımlılığı arttırmıştır. Bu bağımlığın giderek artması bilginin ekonomik bir varlık olarak değer kazanmasına, sistemin bir parçası haline gelmesine yol açmıştır. Bilginin öneminin her geçen gün giderek artması sonucunda, işletmeler, kurumlar, devletler bilginin korunması, yönetilebilmesi tehdit ve risklerin en az seviyeye indirilmesi için en uygun bilgi güvenliği çalışmalarına, çözüm arayışlarına yönelmişlerdir. Bilgi güvenliği konusunda yapılan çalışmalar neticesinde ortaya çıkan bazı standartları işletmeler, kurumlar kendi strateji ve süreçleri için en uygun olanı tercih etmeye ve kullanmaya başlamışlardır.

Dünya'da ve Türkiye'de genel olarak kabul görmüş olan standartlar arasından ITIL, COBIT, ISO/IEC 27001 standartlarıdır Bu standartlardan ITIL bilgi güvenlik yönetimi süreci bilgi güvenliğinin uygulanması konusunda tanımlama yapmaktadır. İşletmeler süreç içerisinde basit seviyede bilgi güvenliği sağlamanın yanında ayrıca servis yönetimi kavramlarını tanımlamakta, sağlanan servis, hizmetlerin en iyi şekilde yürütülmesi, yönetilmesi ve süreçleri için rehberlik etmektedir. ITIL'ın bilgi güvenliği yaklaşımına felsefesinde işletmelerin büyüklüğüne bakılmaksızın bilgi teknolojileri organizasyonlarına süreç merkezli ve ölçeklenebilir bir yaklaşım sergilediği görülmektedir. Diğer bir standart olan COBIT ise bilgi teknolojileri yönetiminde elde edilecek hedefleri ortaya koymakla beraber, hedeflere ulaşmasını sağlamak için uygun bir yöntem tasarım önermektedir. COBIT'in temelini yönetim kurulu kararları ile birlikte yönlendirmek ve kontrol üzerine kurulmuş geniş kapsamlı kontrol odaklı bir yapısı bulunmaktadır. COBIT, bankacılık sektöründe, iş dünyasında, teknolojik çevrelerde, bütün iş modellerinde ve kurumsal kültürlerde kullanılabilir. Bankacılık işlemleri dışında; işletmelerin finans, finansal işlemler, denetim, üretim sektörlerinde, analiz ve raporlamada kullanılabilmektedir.

ISO 27001 standardı bilgi güvenliği yönetim sisteminin ihtiyaçlarını tarif eden, uygulanabilen ve denetlenebilen bir standarttır. Amacı bir Bilgi Güvenliği Yönetim

Sistemi kurmak için bir model sağlamaktır. Bunun yanında yönetim sisteminin uygulanması, işletilmesi, izlenmesi, bakımı, gözden geçirilmesi ve iyileştirilmesi için destekleyici hedefleri sunmaktadır. İşletmelerin büyüklüklerine, ihtiyaçlarına amaçlarına göre bilgi güvenliği yönetim sisteminin tasarımı esnek olması nedeniyle işletmelerin hedeflerine uygun olarak tasarlanabilmektedir. Bilgi teknolojileri güvenlik yönetimi için iyi sınıflanma yapılmış, yeterli derecede güvenlik denetimlerinin seçiminin yapılmasının yanında kolay uygulanabilme özelliğine de sahiptir.

Küçük, orta ve büyük işletmelerin kurumsallaşması veya markalaşma yönünde yapacağı çalışmalar için BGYS uygulaması ve benimsemesi işletmelerin geleceği açısından büyük önem taşımaktadır. Bilgi güvenliğinin işletmelerde verimli olabilmesi için kurulum ve tüm aşamalarında üst yönetimin bilgi güvenliği konusunu sahiplenmesi, gerekli sorumluklarını üstlenmesi işletmelerin bu konuda atacağı en önemli adımlardan biridir. Kurum ve kuruluşlarda bilgi güvenliği konusunun teknik bir konu olarak görüldüğü bu konunun sadece bilgi işlem birimi tarafından yürütülmesi gerektiği konusunda yanlış bir durum anlayış söz konusudur. Bilgi güvenliği konusunda işletmenin tüm paydaşları, (personel, yönetici, taşeron, müşteri, stajyer, misafir) Bilgi Güvenliği Yönetim Sistemini sahiplenmeleri, inanmaları uygulama konusunda yardımcı olmaları ve katılım sağlamaları gerekmektedir. İşletme çalışanlarının bilgi güvenliği sistemi konusunda farkındalığı artırmak için eğitimler almalarının yanında, günlük yaşantılarında kullanmış oldukları internet üzerinde yapılan e-devlet, bankacılık işlemleri yanı sıra yaygın olarak kullandıkları sosyal medya hesaplarının bilgi güvenliklerinden birey olarak sorumlu oldukları bilinci oluşturulmalıdır.

Tez kapsamında ISO Standart kuruluşunun her yıl yayınlamış olduğu araştırma raporundan faydalanılarak; ISO/IEC 27001 standardının Dünya'da 2017 yılında verilen sertifika sayısı bir önceki yıla göre %19 oranında artış göstermiştir. Standardın Dünya'da hangi sektörler tarafından nasıl kullanıldığı, en çok yaygın olarak kullanılan yedi sektörün değişim yüzdesine bakıldığında en çok 2009 yılında sertifika oranlarında artış yaşanmış, standardın en çok sertifika sayısına sahip olan sektörün ise bilişim teknolojileri olduğu sonucuna ulaşılmıştır. Dünya'daki bölgesel dağılımında ise 7 bölge incelenmiş yapılan analizin sonucunda Doğu Asya ve Pasifik bölgesinin 17562 adet sertifika sayısı ilk sıralarda olduğu, aynı bölgede olan Japonya'nın ise hem bölgesel

hem de diğer ülkeler arasında en fazla ISO/IEC 27001 BGYS sertifikasına sahip olduğu ortaya çıkmıştır. 2016-2017 yıllarına ait sertifika sayıları konusunda Dünya'daki ilk on ülke içinde 8. sırada olan İtalya'nın 2017 yılında yaşamış olduğu ekonomik kriz nedeniyle bir önceki yıla oranla % -21,5 azalma olduğu tespit edilmiştir. Ülkemizde 10 yıl öncesi 10 adet olan sertifika sayısının yıllara göre artış göstermiş, 2006 yılında 28. sırada Türkiye, 2017 yılında ise Dünya sıralamasında 15 basamak atlayarak 13. sıraya yükselmiştir. Ülkemizde en fazla sertifikaya sahip şehirler konusunda araştırma yapılmış İstanbul'un 2016 yılına göre % 38,16 Bursa'nın 2016 yılına göre % 63,64, ve Ankara'nın ise 2017 yılında %100 sertifika sayısında artış sağlamıştır.

Ülkemizde BGYS Uygulamaları ve Yasal zorunlulukların gıda, inşaat, tarım enerji, kimya, otomotiv elektronik, biyomedikal, kamu kurumu ve savunma sanayisinde faaliyet gösteren sektörleri kapsamaktadır. Özellikle ticaret odaları, sanayi odaları, meslek odaları tarafından ilerleyen yıllarda bu sektörlerinde genişlemesi, bir zorunluluk haline gelmeden önce ilgili sektörlere özel ISO/IEC 27001 seminerleri, toplantıları, eğitimleri düzenlenmeli, kamuoyunda, iş ve sanayi dünyasında farkındalık artırılmalıdır.

Tez çalışmasında Türkiye'deki mevcut ISO/IEC 27001 sertifika sayısı konusunda istatistiksel güncel verilere ulaşmada çok zorluklar yaşanmıştır. Uluslararası Standartlar Örgütü'nün her yıl yayınlamış olduğu araştırma raporundaki gibi kalite belgelerinin sayısı, sektör ve şehir dağılımları vb. kayıtların oluşturulması konusunda zafiyetler olduğu standartlara uygun bir raporlandırma için zamana ihtiyaç olduğu tespit edilmiştir. İstatistiki verilerin kayıt edilerek saklanması konusunda T.C. Sanayi ve Teknoloji Bakanlığına, TUİK'e, sivil toplum örgütleri, TOBB'a bağlı odalar ve borsalar bu konuda farkındalık çalışmalarının genişletilmesi uygun olmaktadır.

Bilgi güvenliği konuları arasında yer alan veri tabanın ne kadar önemli olduğu 2018 Eylül ayında bir kamu bankasında meydana gelen teknik hata nedeniyle yanlışlıkla düşük kurdan döviz alımları yaşanmıştır. Meydana gelebilecek teknik hataların kullanılan yazılım veya veri tabanı kaynaklı olasılığı bilgi güvenliğinin ne derece önemli olduğu göz önüne alınması gereken örneklerden birisidir. Ülkemizin yerli işletim sistemi ile tamamen yerli veri tabanı (database) konusunda hızla destek ve teşvik etmesi gereken konular arasındadır.

Türkiye'de birçok işletmelerin bilgi teknolojilerine, sunuculara sahip oldukları, her seviyede olan kullanıcıların sürekli olarak bu sistemlere erişim sağlamaktadırlar. İşletmelerin mutlaka oluşabilecek veya oluşan bilgi güvenlik ihlallerini sürekli takip etmesi, raporlanması, belirli periyodik zamanlarda bu raporların analiz edilmesi bu olasılıklara karşı önlem alınması olası veri ve bilgi kaybının önüne geçecektir. Artık küçük ve büyük ölçekli bütün işletmeler olası bir siber saldırıya veya bilgilerinin şifrelenmesiyle (ransomware saldırısı) karşı karşıya kaldığı görülmektedir. Saldırılar sebebiyle mevcut bilgi, verilere ulaşılmaması durumunda ekonomik kayıpların yaşandığı görülmüştür. Dünya çapında 2017 yılı sonu itibariyle (ransomware) zararlı yazılımların yol açtığı hasarın 5 milyar doları aştığı tahmin edilmektedir.

Türkiye'de devlet kurumlarına ait hemen hemen bütün hizmetlerin e-devlet üzerinden sunulması, toplum olarak dijital bir dönüşüm içerisinde olduğumuz görülmektedir. Bu durum maalesef bilgi güvenliği konusunda hem kamu kurumları ve işletmeler tarafından kavranmadığı görülmektedir. Bu konuda ilköğretimden, üniversitelere kadar bilgi güvenliği konusunda eğitimler verilmelidir. Özellikle meslek yüksekokullarında ve fakültelerde her bölüm, branşlarına özel bilgi güvenliği eğitimlerini verilmesi uygun olacaktır.

Her yıl İstanbul Sanayi Odası tarafından yayınlanan Türkiye'nin 500 sanayi kuruluşu listesinde, ilk onda yer alan işletmelerin Bilgi güvenliği yönetim sistemlerini uyguladıklarının tespiti konusunda çalışmalar yapılmıştır. BGYS uygulayan kurum, işletmelerin bilgi güvenliği politikasını internet sayfalarında yayınlama zorunluğu bulunması nedeniyle bu işletmelerin mevcut web sayfalarına bakılması sonucunda listede bulunan tüm işletmelerin ISO/IEC 27001 sertifikasına sahip oldukları belirlenmiştir. Aynı şekilde yayınlanan listedeki Konya'da yer alan işletmeler için aynı yöntem kullanarak yapılan tespit sonucunda, Konya'da ilk yirmide yer alan BGYS konusunda mülakat yapmış olduğumuz tarım gübre ilaç üretimi sektöründe bulunan bir işletmeye rastlanılmıştır. Bu durum sermaye bakımından büyük işletmelerin kurumsal anlamda BGYS ile ilgili çalışma yapmadıkları, bu konuda ciddi olarak eksikleri olduğunu göstermektedir.

Tez çalışmasının ana amaçlarından biri olan Konya örneği çalışmasında Konya ilinde bulunan ISO/IEC 27001 sertifikasına sahip olan işletmeler tespit edilmiştir. ISO/IEC 27001 belge sahibi beş işletme ile irtibata geçilerek bilgi güvenliği yönetim sistemlerini kurma gerekçeleri, mevcut kurulu yönetim sistemleri konusunda karşılaştıkları uygulama sorunları, vb. konularda araştırma yapılmıştır. Araştırmada, mülakat yöntemi kullanılmıştır. Bilgi güvenliği konusunda mülakat yapılması planlanan işletmelerin, verilerini paylaşmama isteklerine karşın işletmeleri koruma adına gizlilik sözleşmesi yapılmıştır (EK2). Bilgi güvenliği konusunda işletmelere çeşitli sorular yönetilmiş, elde edilen, verilen cevapların analizi ve dökümü yapılmıştır(EK3). BGYS'nin ülkemizde, ilimizde yeni bir alan olması nedeniyle saha çalışmalarında zorluklarla karşılaşılmıştır. İşletmelerin bilgi güvenliği yönetim sistemlerini kurma gerekçeleri, mevcut kurulu yönetim sistemlerinin uygulama sorunlarının araştırma yapılarak çözüm önerileri sunulmaya çalışılmıştır.

Mülakat yapılan firmaların karşılaştıkları sorunlardan birisi de Konya'da belgelendirme yapan belgelendirme ve denetleme konusunda uzman kuruluşların yeterli olmadığı; bunun yanı sıra bu konuda yetişmiş personel eksikliği gözlemlenmiştir.

Penetrasyon testi; işletmelerin ve kurumların bünyesinde bulunan bilişim sistemlerindeki güvenlik açıklıklarının, uzman bir üçüncü göz veya kişiler tarafından risklerin tespit edilmesi, bu konudaki açıklıkların raporlanmasını kapsamaktadır.

Mülakat yapılan firmaların karşılaştıkları problem ve sorunlardan biriside ISO/IEC 27001 sertifikası için zorunlu olan penetrasyon testi yapabilecek, Konya'da bu konuda uzman olan firma ve işletmelerin bulunmadığı tespit edilmiştir. Bu konudaki uzman kurum ve işletmelerin İstanbul ve Ankara'da olması nedeniyle test yaptıracak işletmelere ekstra bir maliyet getirdiği gözlemlenmiştir.

NACE kodlarına göre işletmeleri sınıflandırma yaptığımızda A işletmesinin bulunduğu sektörde dokuz, B işletmesinin bulunduğu sektörde on dört, C ve D işletmelerinin bulunduğu sektörde yüz üç, E işletmesinin bulunduğu sektörde ise üç adet işletme olduğu tespit edilmiştir. Mülakat yapılan işletmelerin bulunduğu sektörlerde BGYS kurulumu ve uygulaması konusunda öncü oldukları saptanmıştır. Bu durum işletmeler de ISO/IEC 27001 standardı hakkında fazla bir bilgiye sahip olunmadığı görülmekte, özellikle bilgi güvenliğinin bir teknik konu ve içerikten ibaret olduğu

sanılmaktadır. Fakat ISO 9001 kalite yönetim sistemine sahip olan işletmelerin hedef ve politika uygulamaları var olması nedeniyle BGYS'nin ana süreçlerini kolaylıkla uygulayabilecekleri konusunda eğitimcilerin ve uzmanların bilgilendirme yapılması gerekmektedir. İşletmeler tarafından BGYS planlaması, kuruluş adımları, emek ve zaman kaybı olarak görülmekte, bu çalışmanın kısa vadeli olarak değil uzun süreli olarak fayda sağlayacağının farkındalığı yok denecek kadar azdır. BGYS bir kereye mahsus olmadığı sürecin yönetim sistemi mantığı ile sürekli iyileştirmeye yönelik olması gerekmektedir. Bilgi güvenliği konusunda en zayıf halkanın insan faktörü olduğu göz önünde bulundurmalı bu konuda düzenli olarak işletme ve kişisel bilgi güvenliği farkındalık eğitimleri verilmeli risklerin azaltılması konusunda hedefler konulmalıdır.

ISO/IEC 27001 genel özelliği itibariyle teknik bir standart değildir, içerik prosedürlerine göre açıklayıcı bir yapıya sahiptir. Her işleme, kurum için güvenlik gereksinimleri belirlemekte, uygulama konusunu ve şeklini işletmelere bırakmaktadır. Bu nedenle işletme, kurumlar mevcut yapılarının ihtiyaçlarına uygun kontrol hedeflerini tespit etmeli, bunu üst yönetim kurulu karar ve desteğiyle uygulamalıdır. Bilgi güvenliği yönetimine sahip beş işletme ile yapmış olduğumuz mülakat sonucunda; bir işletme haricinde ISO/IEC 27001 sertifikası ile ilgili işletme, kurumlardan danışmanlık konusunda herhangi bir başvuru olmadığı gözükmektedir. İşletmelerin standart çalışması yapmadan önce mutlaka kendi yapıları ve sektörleri ile ilgili araştırma yapması gereklidir. Daha önce BGYS kurmuş, ISO/IEC 27001 sertifikasına sahip aynı sektördeki veya diğer işletme ve kurumların tespit edilerek, bu konudaki çalışmalar hakkında bilgi alınması, ortaya çıkan tecrübelerin paylaşımı, karşılaşılan problemlerin çözümü konusunda fikir alışverişinin yapılması iş gücü ve zamandan tasarruf etmelerini sağlayacaktır.

Kişisel veri sahibi olan tüm işletme ve kurumları ilgilendiren Kişisel Verilerin Korunması Kanunu (KVKK) 7 Nisan 2018 de sonraki tarihten sonra uyum sürecini tamamlamış bu konuda birçok işletmenin süreçle ilgili çalışmalarının devam etmekte olduğu görülmektedir. Buradaki önemli noktalardan biri bünyesinde ISO/IEC 27001 BGYS olmayan işletme ve kurumların KVKK uyum çalışmasına ilave olarak mutlaka

BGYS zorunluluklarına ait bazı önemli kriterleri de karşılaması gerekmektedir. ISO/IEC 27001 BGYS sistemine sahip olan işletme ve kurumların bu sürece geçişlerde daha uyumlu olacağı gözlemlenmiştir.

Bilgi güvenliği bir zincir gibidir. Zincirin en zayıf noktasında meydana gelen kopma tüm Bilgi Güvenliği Yönetim Sistemini etkiler. Bu nedenle Bilgi güvenliği konusunda, belgelendirilmesi ve akreditasyon süreçlerini titizlikle kanunlara ve standartlara göre hareket edilmelidir.

# KAYNAKLAR


9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı. (2016). 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, (s. 265, 156). Ankara.

Aktan, Ç. C., & Vural, İ. Y. (2005). Bilgi Çağında Bilgi Yönetimi. Konya: Çizgi Kitabevi.

Aktaş, F., & Soğukpınar, İ. (2010). Bilgi Güvenliğinde Uygun Risk Analizi ve Yönetimi Yönteminin Seçimi İçin Bir Yaklaşım. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi,, 39,46.

Akyol, F. (2013). COBIT (Bilgi ve ilgili teknolojiler için kontrol hedefleri) uygulayan şirketlerdeki bilgi güvenliği politikalarının şirket, personel ve süreçlere etkileri. Yüksek Lisans. Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul .

Artinyan, E. (2009). COBIT Çerçevesi. Deloitte İç Yayın,, 1-6.

Aslandağ, K. (2010). Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performansı ilişkisine dair bir uygulama. Yüksek Lisans Tezi. Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Kocaeli.

Atılgan, D. (2009). Bilgi yönetimi kavramı ve gelişimi. Türk Kütüphaneciliği, 23(1):201-212.

Başbakanlık Hazine Müsteşarlığı Sigorta Denetleme Kurulu. (2016). İç Sistemler Denetim Rehberi. Ankara: Başbakanlık Hazine Müsteşarlığı Sigorta Denetleme Kurulu.

Bilgin, B. Ö. (2016). Bilgi teknolojileri denetimi ve bir uygulama. Yüksek Lisans Tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Bingöl, U. (2010). ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu. Yüksek Lisans Tezi. Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

BMC Software, Inc. (2016). 05 21, 2018 tarihinde https://www.bmc.com: https://www.bmc.com/guides/itil-introduction.html adresinden alındı

Cantürk, S. (2013). Bilgi Teknolojileri Yönetişimi İçin Yeni Bir Adım: COBIT 5. KPMG Gündem, 37.

Ceauşu, I., Ilie, C., & Ionescu, R. (2018). Proceedings of the 12th International Conference on Business. Considerations on the implementation steps for an information security management system. The Bucharest University of Economic Studies,.

CTR Uluslararası Belgelendirme ve Denetim Ltd. Şti. (2018, 4 2). http://belgelendirme.ctr.com.tr/enerji-altyapilari-iso-iec-tr-27019-duyurusu_2_375.html adresinden alınmıştır

Çek, E. (2017). Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. Yüksek Lisans Tezi. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

Daşdemir, A. (2016). ISO 27001:2013 Bilgi Güvenliği Yönetim Standardı Ve Uygulama Süreci. Yüksek Lisans Semineri. Selçuk Üniversitesi Fen Bilimleri Enstitüsü, Konya.

Demirok, E. (2016). Kurumsal Bilgi Güvenliği Yönetim Sistemi; Vakıf Üniversitesi Örneği. Yüksek Lisans Tezi. Okan Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Demirtaş, H. (2013). Bilgi Güvenliği Yönetiminin Gerekleri Ve Başarı Dayanakları: Bir Uygulama Örneği. Yüksek Lisans Tezi. Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

Djapić, M., & Lukić, L. (2007). ISO/IEC 27000 Series Standards The Best Business Practice For Information Security. 1. International Quality Conference .

Ersoy, E. V. (2012). ISO/IEC 27001 Bilgi Güvenliği Standardı. ODTÜ Yayıncılık.

Eskiyörük, D. (2007). BGYS-Risk Yönetim Süreci Kılavuzu. TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü.

Evrin, V., & Demirer, M. (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları:ISO/IEC-27001 Örneği. IV.Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu. Ankara: TMMOB Elektrik Mühendisleri Odası.

Fussell, R. (2005). Protecting Information Security Availability Via Self-adapting Intelligent Agents. Military Communications Conference, IEEE, (s. 297).

Ganbat, O. (2013). Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması. Yüksek Lisans Tezi. Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir.

Gencer, K. (2015). ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım. Yüksek Lisans Tezi. Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.

Government of Mauritius. (2018, 08 08). ISO 27001 Controls and Objectives. 08 08, 2018 tarihinde Ministry of Gender Equality, Child Development and Family Welfare:http://gender.govmu.org/English/Documents/activities/gender%20infsys/AnnexIX1302.pdf adresinden alındı

Gülmüş, M. (2010). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği . Yüksek LisansTezi. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

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

Güngör, U., & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği Ve Siber Savaş. Karadeniz Arştırmaları Dergisi, 131-146.

Hacısüleymanoğlu, E. (2010). Bilgi teknolojileri yönetişim yöntemleri ve COBIT ile ulusal bir bankada uygulaması. Yüksek Lisans Tezi. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Humphreys, T., & Plate, A. (2005). Guide To the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001. British Standards Institution.

İnnova Bilişim Çözümleri. (2013, 11 11). 01 05, 2018 tarihinde http://www.innova.com.tr/blog/yazi.asp?ID=136&baslik=ISO-27001-standardinin-2013-revizyonunda-neler-degisiyor adresinden alındı.

International Organization for Standardization. (2009). ISO/IEC 27000:2009. Information Technology - Security Techniques - Information Security Management Systems. Switzerland: International Organization for Standardization.

International Organization for Standardization. (2018, 09 03). 09 03, 2018 tarihinde ISO Web Sitesi: www.iso.org/the-iso-survey.html adresinden alındı.

International Organization for Standardization. (2018, 02). Internatıonal Standard ISO/IEC 27000. Information Technology - Security Techniques - Information Security Management Systems. Switzerland: International Organization for Standardization.

ISO27k Infosec Management Standards. (2017). 4 25, 2018 tarihinde www.iso27001security.com: www.iso27001security.com adresinden alındı.

IT Governance Institute, The Office of Government Commerce. (2008). Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. IT Governance Institute, The Office of Government Commerce.

Kahraman, S. (2006). Yönetimde bilgi güvenlik sisteminin yapısı işleyişi ve ASELSAN A.Ş.'de uygulaması. Yüksek Lisans Tezi. Eskişehir: Anadolu Üniversitesi, Sosyal Bilimler Enstitüsü, Eskişehir.

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2006). Information Security Standards and Global Business. 2091-2095.

Koç, F. (2008). BGYS-Varlık Envanteri Oluşturma Ve Sınıflandırma Kılavuzu. TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü.

Kumaş, E. (2009). Bilgi Güvenliğinin Sağlanmasında Risk Yönetimi: E-Devlet Kapısı Uygulaması. Yüksek Lisans Tezi. Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü.

Mete, H. (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması. Yüksek Lisans Tezi. Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya.

Mitnick, K. D. (2003). The Art Of Deception: Controlling The Human Element Of Security, Wiley Publishing.

Odabaşı, S. Y. (2011). Implementation of information technology infrastructure library (ITIL) processes (Bilgi teknolojileri alt yapı kütüphanesi (ITIL) süreçlerinin uyarlanması). Yüksek Lisans Tezi. Kadir Has Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Önel, D., & Dinçkan, A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü.

Özbilgin, İ. G., & Özlü, M. (2010, Eylül 22-25). 27. Ulusal Bilişim Kurultayı. ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve Ağ Yönetimi Politikası. Ankara.

Özgener, Ş. (2002). Global ölçekte değer yaratan bilgi yönetimi stratejileri. 1. Ulusal Bilgi Ekonomisi ve Yönetim Kongresi Bildirileri, (s. 483-496). Kocaeli.

Öztürk, G. (2008, 03 21). Bilgi Güvenliği Politikası Oluşturma Kılavuzu. TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü.

Pehlivan, İ., & Marttin, V. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetim Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları üzerine Bir İnceleme. Mühendislik Bilimleri ve Tasarım Dergisi, 49-56.

Perendi, Ü. (2008). BGYS Kapsamı Belirleme Kılavuzu. TÜBİTAK Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. Second Asia International Conference on Modelling & Simulation, 749-753.

Schmidt, A. H. (2004). Building a Mosaic of Securityfor a Betterworld, Security. AspatoreBooks.

Shojaie, B. (2018, 02 20). Implementation Of Information Security Management Systems Based On The ISO/IEC 27001 Standard In Different Cultures. Doctoral Degree. Faculty of Mathematics, Informatics and Natural Sciences Department of Informatics of Universitat Hamburg.

Spremic, M., Zmirak, Z., & Kraljevic, K. (2008, 06 23-26). IT and Business Process Performance Management: Case Study of ITIL Implementation in Finance

Service Industry. Proceedings of the ITI 2008 30th Int. Conf. on Information Technology Interfaces, 243-250. Cavtat, Hırvatistan.

Susanto, H., Almunawar, M., & Tuan, Y. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05, 1-7.

Şahinaslan, E., Kandemir, R., & Kantürk, A. (2010). Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme. Ankara: TMMOB Elektrik Mühendisler Odası.

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri (s. 719-723). Antalya: Akademik Bilişim Konferansları .

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

Tuğlular, T. (2003, Ekim). Üniversitelerde Bilgi Güvenliği Politikaları. Ulaknet Sistem Yönetimi Konferansı .

Türk Akreditasyon Kurumu. (2018, 09 11). Bilgi Talebi - Dilekçe Cevap Sayı: 50264901-000-5772 . Ankara: Türk Akreditasyon Kurumu.

Türk Akreditasyon Kurumu. (2018, Eylül 01). 09 01, 2018 tarihinde Akredite Kuruluş Arama: https://secure.turkak.org.tr/kapsam/search adresinden alındı

Türk Standardları Enstitüsü. (2013). TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi.

Türk Standartları Enstitüsü. (2018). 05 20, 2018 tarihinde https://intweb.tse.org.tr: https://intweb.tse.org.tr/Standard/Standard/Standard.aspx adresinden alındı

Tvrdíková, M. (2008). Information system integrated security. 7th Computer Information Systems and Industrial Management Applications, 153-154.

Uzun, H., & Durna, U. (2008). İşletmelerde Rekabet Unsuru Olarak Bilgi Yönetimi. Niğde Üniversitesi İİBF Dergisi, 33-40.

Uzunay, V. (2007). COBIT (Control Objectives for Information and related Technology). Yayınlanmamış Mesleki Yeterlilik Tezi. İç Kontrol Merkezi Uyumlaştırma Dairesi, Ankara.

Vural, Y., & Sağıroğlu, Ş. (2007). Kurumsal Bilgi Güvenliği: Güncel Gelişmeler. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, (s. 192). Ankara.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23(2), 507-522.

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

Yılmaz, O. (2014). ITIL ve COBIT yönetim standartları ve bir uygulama. Yüksek Lisans Tezi. Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Zaim , H. (2005). Bilginin Artan Önemi ve Bilgi Yönetimi. İşaret Yayınları.

# EKLER

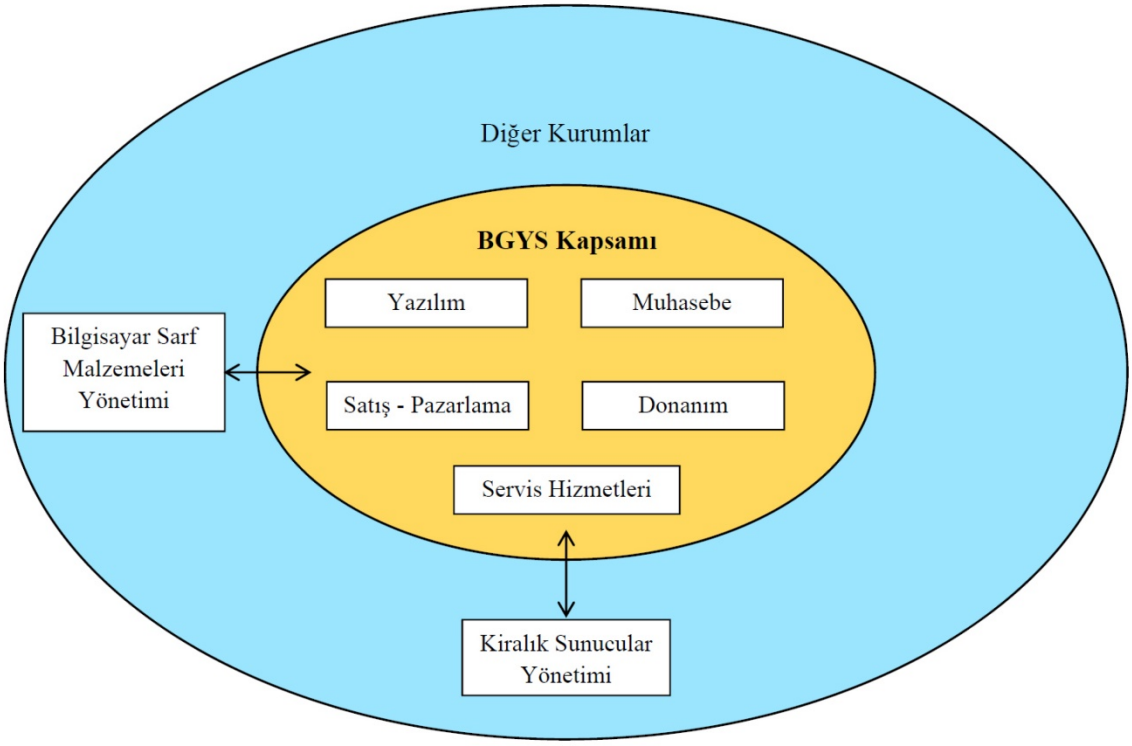
## EK 1. Örnek BGYS Kapsam Dokümanı

| ABY BİLGİSAYAR YAZILIM LTD.ŞTİ.<br>BGYS KAPSAM DOKÜMANI | | |
|---|---|---|
| YAYIN NO :<br>27001- POL- 01 | DOKÜMAN ADI:<br>DOK-POL-V1 | VER: 0.1 |

**ABY BİLGİSAYAR YAZILIM LTD. ŞTİ. BGYS KAPSAMI**

**Amaç ve Kapsam**

2006 yılında Konya'da kurulan ABY Bilgisayar Yazılım Ltd. Şti. müşterilerine, kendine ve alt yüklenicilere ait olan bilgilerin korunması için ISO/IEC 27001 standart kapsamına uygun Bilgi Güvenliği Yönetim Sisteminin kurulmasına karar verilmiştir. Kurulacak ve uygulanacak sistem ABY Bilgisayar Yazılım Ltd. Şirketin tüm departmanlarını kapsayacaktır.




**ABY Bilgisayar Yazılım Ltd. Şti. BGYS Kapsamı**

Kaynak: (Perendi, 2008)

(devam)

**Organizasyon**

ABY Bilgisayar Yazılım Ltd. Şti. 5 bölümden oluşmaktadır.

- Yazılım
- Muhasebe
- Satış pazarlama
- Servis hizmetleri

**Yerleşke**

Innopark Konya Teknoloji Geliştirme Bölgesi Büyük Kayacık Mah. 101. Cad. No:13 Selçuklu/KONYA

Depo ve şubesi bulunmamaktadır.

**Varlıklar ve Teknoloji**

ABY Bilgisayar Yazılım Ltd. Şti. Bilgisayar sarf malzemeleri ve kiralık sunucular haricindeki kendi bünyesinde verilmekte olduğu, yazılım, satış - pazarlama, servis hizmetleri, muhasebe işlemlerini kendi bünyesinde sağlanmaktadır. BGYS aşağıda belirtilen tüm varlıkları kapsamaktadır.

**1)** Şirkete ait bütün ticari bilgiler
**2)** Bilgi teknolojileri, sunucular ve bilgisayar sistemleri
**3)** Tüm müşterilerin kişisel özel bilgileri
**4)** Şirketin çalışma ekibine ait olan bilgiler
**5)** Tüm Dokümantasyon Bilgileri

| HAZIRLAYAN | KONTROL EDEN | ONAYLAYAN |
|---|---|---|
| | | |

Kaynak: (Perendi, 2008)

## EK 2. GENEL GİZLİLİK SÖZLEŞMESİ

Bu mülakat KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı'nda yürütülmekte olan **"İşletmelerde Bilgi Güvenliği Uygulama Sorunları ve Çözüm Önerileri; Konya Örneği"** isimli yüksek lisans tez çalışmasında kullanılmak üzere hazırlanmıştır.

**Mülakat sonucunda;**

1- Yapılan görüşmeler sonucunda işletmelerden kaynak olarak alınan doküman, veri vb. bilgilerin 3. sahış ve kişilerle paylaşılmayacağını;
2- Aynı sektörde bulunan rakip ve diğer firmalarla paylaşılmayacağını;
3- Yapılan mülakat ve görüşmelerinin dökümünün tez çalışmasında yayınlanmadan önce mutlaka görüşme yapılan firmadan onay alınacağını;
4- Mülakat sonrasında yetkili ve firmaların izin verilen bilgi ve dokümanların sadece tez çalışmasında paylaşacağını
5- Yapılan mülakat soruları EK-1'de yer almaktadır.

Bu mülakatta elde edilen bilgilerin sadece bilimsel amaçlar ve tez çalışmasında kullanılacağını taahhüt ederim.

Mülakat Yapılan Firma

Mülakatı Yapan
Mustafa YILMAZ

## EK 3. ISO 27001 BGYS SERTİFİKASI HAKKINDA İŞLETMELERLE YAPILAN MÜLAKATLAR

### A İŞLETMESİ

**Sektörü :** Enerji Dağıtım

**Nace Kodu :** 35.13.01

**1- Bilgi Güvenliği Yönetimini uygulayan kuruluşların kazanımları nelerdir?**

Kurumlar için bilginin bütünlüğü (güvenilirliği), ihtiyaç duyanlar tarafından ulaşılabilirliği ve istenmeyen erişimlere karşı gizliliği önemlidir. Kurumumuzda bilgi güvenliği temelde bu üç felsefeye dayanır. Bilgi güvenliği yönetiminde temel amacımız riskleri azaltmak için bilgi sahibi olmaktır. Para ve itibar kayıplarına etki eden risklerin belirlenmesi için bilgi güvenliği yönetimi şarttır.

**2- İyi günler öncelikle bize Bilgi Güvenliği Yönetim Sistemini kurma kararınızı nasıl aldığınızı anlatır mısınız?**

BGYS kurulması mevzuat ve Düzenleme Kurulu kararları ile belirlenmektedir. Kurmama serbestliği bulunmamaktadır. Kamu adına çalışan kurumlar bu konuda risklerini belirleyerek bağlı oldukları kurula bildirmekle yükümlüdür.

**3-Bilgi Güvenliği Yönetim Sistemini kurulumuna ilk hangi konulardan nasıl başladınız?**

Öncelikle bilgi güvenliğine dokunan sistemlerdeki envanterin çıkarılması gerekmektedir. Riskler bu envantere göre çıkarılmaktadır. Daha sonra kurum çalışanlarının farkındalığını artıracak eğitimler düzenlenmiş ve afişler görünür yerlere asılmıştır.

**4-Hangi danışmanlık firması ile beraber çalıştınız?**

Danışmanlık firmaları ile gizlilik anlaşmaları yapılmaktadır. Paylaşılmaması daha uygundur.

**5- Bilgi Güvenliği Yönetim Sistemini kurulumunda yararlandığınız kaynaklar nelerdir?**

Öncelikle internet üzerindeki bilgi kaynaklarından faydalanılmaktadır. Danışman firmalarla çalışarak bilgimizi disipline ediyoruz.

**6- Bilgi Güvenliği Yönetim Sistemini kurum çalışanları dışında kimlerle etkileşim içindedir?**

Mevzuat düzenleyici kurumlarla etkileşim bulunmaktadır. Örneğin envantere göre riskler belirlendikten sonra periyodik olarak yapılan düzeltme ve iyileştirmeleri gönderiyoruz. Bununla birlikte Security Operation Center (SOC) hizmeti alınan yerlerde gözetim yapan kişiler de etkileşimdedir.

7- **Bilgi Güvenliği Yönetim Sistemini sadece bilgi işlem personeli ile mi yürütülmektedir?**

BGYS her ne kadar bilgi teknolojileri çalışanları tarafından koordine ediliyor olsa da, insan kaynakları, sertifikasyon birimleri, idari işler başta olmak üzere kurumdaki tüm departmanları ilgilendirmektedir. Temizlik görevlileri de zincirin parçasıdır. Bununla birlikte departman yetenekleri nedeni ile bilgi teknolojileri birimleri daha fazla sorumluluk sahibi olmaktadırlar.

**8- Aldığınız danışmanlık, eğitim ve denetim hizmetleri için ne kadar bir ücret ödediniz?**

BGYS ile ilgili envanterin büyüklüğü, şube sayısı ve çalışan farkındalığı seviyesine göre değişmekle birlikte 30.000 TL ile 150.000 TL arasında danışmanlık fiyatları görülebilir. Gizlilik anlaşmaları nedeni ile fiyat bilgisi paylaşılması uygun değildir.

**9- BGYS işletmenizde ne kadar bir süre ile kurulmuştur?**

Kurumumuzda 2 yıl sürmektedir. Yoğun çalışma dokümantasyon 21 gün sürmüştür, kalan zamanda periyodik test ve değerlendirme çalışmaları yapılmaktadır.

**10- Bilgi Güvenliği Yönetim Sistemini kurulum süreci nasıl ilerledi?**

Bilgi teknolojileri ekibi tarafından oluşturulan siber olaylara müdahale ekibi, envanterin çıkarılması, danışman raporları ve risk belirleme çalışmalarını yürütmektedir. Süreç belirlenmesinden ziyade mevzuat hükümlerinin yerine getirilmesi çabası gösterilmektedir.

**11- Eğitim faaliyetlerinden de bize biraz bahsedebilir misiniz? Katılımlar nasıldı?**

Şirket içinde hem yüz yüze hem de online eğitim platformu üzerinden birden fazla eğitim düzenlenmiştir. Katılım mecburiyeti getirildiğinden katılım oranı yüksektir. Farkındalığın sürekli gündemde kalması için 6 ayda bir online eğitim ataması yapılmaktadır. İlgili kişiler online eğitimdeki soruları cevaplamaktadırlar.

**12- Varlıklar belirlenirken dikkat edilmesi gereken hususlar nelerdir?**

Öncelikle varlıkların kurum için değerli olan unsurlardan oluşması gerekmektedir. Bilginin kendisi de varlık olarak kabul edilmeli özellikle varlıkların sahipleri (departmanları) net bir şekilde belirlenmelidir. Her varlığın sahipliği bilgi teknolojileri ekibine bırakılırsa gerekli özen gösterilemeyecektir. Örn: Kurum araçlarının yetkisiz kullanımı idari işler ekibi tarafından denetlenmelidir.

**13- Bilgi Güvenliği Yönetiminde yaşanan sorunlar nelerdir?**

Kaliteli insan kaynağı eksikliği en büyük problemdir. Risklerin belirlenmesinde aşırı paranoyak yaklaşım ve sonucunda yönetim desteğinin yitirilmesi de ayrı bir problemdir. BGYS ilgili kişilerin dedikasyonuna (sürekli ilgisine) ihtiyaç duyar ve genellikle sağlanması zordur. Ayrıca BGYS yetkililerinin işten ayrılması, know-how kaybı da sorun olmaktadır.

**14- Kurum personeli BGYS kurulmasına nasıl bakıyor, herhangi bir tepkileri oluyor mu?**

Aşırı paranoyak yaklaşım gösteren BGYS yöneticileri kurum çalışanlarını bıktırabiliyor. Örneğin insan kaynakları yetkilisini her toplantıya çağrılır ve kendi sorumluluk alanında bir şey konuşulmazsa tepki doğurmaktadır.

**15- Politikalar ve prosedürler neleri kapsıyordu nasıl bir sistemle bunları hazırladınız?**

Gizlilik, bütünlük ve erişilebilirlik temel ilkelerinden yola çıkarak, kurum için farkındalığı artırıcı ve risk belirleme kapsamında politikalar düzenlenmiştir. Genelde standartlara uyum maddeleri politika olarak uygulanmaktadır. Prosedürler genelde bilgi teknolojileri yöneticileri tarafından belirlenerek uygulanmaktadır.

**16- Bilgi Güvenliği Yönetiminin eksiklikleri nelerdir?**

BGYS bir ekip işidir. Genellikle bilgi teknolojileri çalışanları tarafından yerine getirilmesi gereken önlemler olarak algılanmaktadır. Oysa kurumdaki yönetim dahil tüm departmanlar tarafından ele alınması gereken bir konudur. Örneğin: Henüz kişisel verilerin korunması yeterince anlaşılamamıştır. Bilgi teknolojileri departmanı tarafından yürütülmesi gerektiği algısı vardır. Oysa hukuk departmanı daha fazla sorumludur.

**17- ISO27001 standartlarının hepsini birebir uygulamamız gerekir mi?**

Standartta tanımlanmış varlıklarımız var ve bu varlıklar için gizlilik, bütünlük ve erişebilirlik ihtiyaçlarımız varsa ilgili her standart uygulanmaktadır. Bununla birlikte aşırı maliyetli önlemler, elde olmayan sebepler (örn: ilgili personelin işten ayrılması) nedeni ile prosedürler aksatılabilmektedir.

**18- Kontroller nasıl yapıldı ve kontroller bittikten sonra ne olur?**

Kurumun sertifikasyon işleri ile ilgili departman tarafından denetim hizmeti satın alınmıştır. Denetimi akredite bir firma gerçekleştirmiştir.

**19- BGYS kurulum aşamasından sonra belgelendirme kuruluşunun yaptığı kontrollerde her hangi bir eksiklikle karşılaştınız mı?**

Belgelendirme firması elindeki prosedüre göre çalışmaktadır. Hizmet satın alma sürecinde taahhüt ettiği hizmetleri sağlamaktadır. Bulgulara bir örnek olarak, kurum şubelerinde network switchlerinden bazılarının masa üstünde bulunduğu, bunların dolap içinde olması gerektiği belgelenmiştir.

**20- Danışmanlık ve eğitim firmasıyla çalışmak bir zorunluluk mu yoksa size kalmış bir tercih midir? Sizin belge almak isteyen kurumlar için tavsiyeniz ne yöndedir?**

Tercihtir. Yeterli insan kaynağı varsa kurum bünyesinde gerekli hazırlıklar yapılabilir. Standartlar edinildikten sonra gereği yerine getirilirken belgelendirme başvurusu yapılabilir. Danışmanlar kurum tecrübe eksikliği durumunda elzemdirler ve işi disipline etmeye ve konuya odaklanmaya yardımcı olurlar. Belge almak için tüm zafiyetlerin kapatılmış olması zorunluluğu bulunmamaktadır. Risklerin belirlenerek kurum yönetimi tarafından anlaşılması ve bunun belgelendirme kuruluşu tarafından kabul edilebilir seviyede olduğunun görülmesi sonrasında da belge süreci devam edebilir.

**21- Sertifikayı aldıktan sonra herhangi bir kurumdan size danışmanlık anlamında başvurular oldu mu?**

Oldu. Büyük kurumların periyodik sızma testi gerçekleştirmesi ve bulgulara göre risk raporunu ve aksiyon planlarını güncellemeleri gerekmektedir.

**22- Bilgi Güvenliği yönetimi İnsan Kaynakları gelişimine katkı sağlar mı?**

İnsan kaynakları departmanı bilgi güvenliğinde kritik departmanlardan birisidir. Hem BGYS hem de Kişisel Verilerin Korunması Kanunu için iç prosedürlerini uyumlu hale getirmelidirler.

**23- Kurumunuz isminin geçmesinde bir sakınca var mı? Uygun değil ise isim belirtmeden yayınlayabiliriz?**

Lütfen isim belirmeden yayınlayınız. Kurum politikalarımızdan birisi de hedef olmamaya çaba göstermektir.

**24- Peki, tüm çalışanlarınızın sayısını öğrenebilir miyiz?**

Yüklenici çalışanları dahil 2.800 personel bulunmaktadır.

**25- Kurumunuzun oluşturduğu BGYS organizasyonunda kimler görevlidir?**

Bu bilginin paylaşılması uygun bulunmamıştır. Sosyal mühendislik riski bulunmaktadır.

**B İŞLETMESİ**

**Sektörü :** Enerji ekipmanları imalat

**Nace Kodu :** 28.21.10

**1- Bilgi Güvenliği Yönetimini uygulayan kuruluşların kazanımları nelerdir?**

Bilgi Güvenliği Yönetim Sistemine geçmeden önce işletmemizde dokümantasyonumuz, bunun devamında ise risk analizi, grupları ve yazılı olarak politikalarımız bulunmamaktaydı. Bu sistemle birlikte eksik yönlerimizi görmüş, eksiklikleri tamamlamış ve gidermiş olduk. ISO 27001 sertifikasına sahip olmanın firmamıza getirdiği imaj ve prestij kazandırmış aynı zamanda rekabet gücümüzde artış sağlanmıştır. Bu sistem sayesinde bilgi işlem birimizin yapmak istediği güvenlik politikalarını kolaylıkla uygulama imkânına sahip olmuştur.

**2- İyi günler; öncelikle bize Bilgi Güvenliği Yönetim Sistemini kurma kararınızı nasıl aldığınızı anlatır mısınız?**

Firmamızın hedef ve politikalarında yer alması, oluşturduğumuz marka ve ürünlerin imajının korunması için ve üst yönetimden gelen talep doğrultusunda kurma kararı alınmıştır. Bu karar alınırken firmamızın %80 oranında dış ticaret satışı olması sebebiyle Gümrük Yönetmeliğinde yayınlanan Bilgi Güvenliği konusundaki madde nedeniyle etkili olmuştur.

**3- Bilgi Güvenliği Yönetim Sistemini kurulumuna ilk hangi konulardan nasıl başladınız?**

İlk olarak standardın maddelerinin taraması yapılmış ve bu konuda danışman firma ile çalışma kararı alınmıştır. Danışman firma ile birlikte işletmemizin süreçlerini ve tüm departmanların analizi yapılmıştır. Bu kapsamda Bilgi Güvenliği Yönetim Sistemi kapsamına hangi süreçlerin dahil edileceğinin analizi yapılmıştır. Daha sonraki adımlarda ise standardın öngördüğü politikalar, dokümantasyonlar ile başlanılmıştır.

**4- Hangi danışmanlık firması ile beraber çalıştınız?**

Konya'da bulunan Mc Meda Danışmanlık Firması ile çalışmıştır. Sertifika için de İnspect Uluslararası Belgelendirme firması ile birlikte çalışılmıştır.

**5- Bilgi Güvenliği Yönetim Sistemini kurulumunda yararlandığınız kaynaklar nelerdir?**

Bu konuda TSE ve ISO'nun yayınlamış olduğu yayınlardan ve danışman firmamızdan yararlanılmıştır. Ayriyeten 1 personelimiz bu konuda Bureau Veritas'dan eğitim almıştır.

**6- Bilgi Güvenliği Yönetim Sistemini kurum çalışanları dışında kimlerle etkileşim içindedir?**

Hizmet aldığımız tedarikçi firmalarımızla gizlilik sözleşmesi bulunmakta ve bu konuda etkileşim içinde bulunulmaktadır. Mavi ve beyaz yakalı olmak üzere ayrı ayrı olmak üzere personellerimizle de gizlilik sözleşmesi yapılmaktadır.

**7- Bilgi Güvenliği Yönetim Sistemini sadece bilgi işlem personeli ile mi yürütülmektedir?**

Bu konuda ilk başlangıçta yönetim kurulunun atamış olduğu bir temsilci ve bilgi işlem personeli ile yürütülmüş daha sonraki süreçlerde tüm departmanların katılımı ve uyumu ile yürütülmektedir.

**8- Aldığınız danışmanlık, eğitim ve denetim hizmetleri için ne kadar bir ücret ödediniz?**

Danışmanlık ücreti konusunda üst yönetim görüştüğü için bu konuda bir bilgimiz bulunmamaktadır. Eğitim için 1 kişi için 1000 TL. ücret ödenmiştir.

**9- BGYS işletmenizde ne kadar bir süre ile kurulmuştur?**

Dokümantasyon ve standardın gerekliğinin sağlanması için ortalama olarak 5 ayda süreç tamamlanmıştır. Sertifikanın alınması ise Ocak 2017'de tamamlanmıştır.

**10- Bilgi Güvenliği Yönetim Sistemini kurulum süreci nasıl ilerledi?**

Yönetim Sisteminin kurulum aşamasında takvim danışmanlık firması tarafından oluşturulmuştur. Bu takvim ve program dahilinde süreçler, politikalar, varlıklar, risk analizlerinin yapılması ve dokümantasyonların tamamlanması ile aşama olarak ilerlenmiştir. Daha sonraki süreçlerde kurum içi bilgi güvenliği yönetim sistemleri eğitimleri ile devam edilmiştir.

**11- Eğitim faaliyetlerinden de bize biraz bahsedebilir misiniz? Katılımlar nasıldı?**

Danışmanlık firmasının konu ile ilgili verdiği eğitim 4-5 ay sürmüştür. Bunun haricinde firmamızda kalite yöneticisi olan bir personelimiz danışmanlık firmasının verdiği eğitimin haricinde dokümantasyon, iç denetçi eğitimi konusunda Ankara'da 3 günlük eğitim almıştır. Bu eğitimlere daha sonra firmamızdaki tüm departmanların katılımları sağlanmıştır.

**12- Varlıklar belirlenirken dikkat edilmesi gereken hususlar nelerdir?**

Bizim için en önemli kaynak bilgidir. Daha sonra çalışan personellerimiz, teknik resim, projelerimiz, donanımlar, bilgisayarlar, sunucular ve kameralar şeklinde belirlenmiştir. Daha doğrusu bizim için varlık firmamız için değerli olan yetkisiz erişim olmaması gereken bilgi ve materyaller diyebiliriz.

**13- Bilgi Güvenliği Yönetiminde yaşanan sorunlar nelerdir?**

Bu konuda yaşanan problemlerden birisi risk yönetimi ve analizidir. Risk analizi yapılırken ilgili standartların maddelerinin anlaşılmaya çalışılması ve tamamlanması konusunda sorunlar yaşanmıştır. Yönetim kurulu bilgi güvenliği konusunda bize baştan destek verdiği için temiz ekran, temiz masa uygulamalarında fazla sorun yaşanmadan geçişler sağlanmıştır.

**14- Kurum personeli BGYS kurulmasına nasıl bakıyor, herhangi bir tepkileri oluyor mu?**

Bu konuda yönetimin desteği ve uyguladığı sıkı kural ve politikası olması nedeniyle her hangi bir tepki olmamıştır.

**15- Politikalar ve prosedürler neleri kapsıyordu nasıl bir sistemle bunları hazırladınız?**

TS EN ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi firmamızın bilgi işlem altyapısını kullanmakta olan tüm birimler ve üçüncü taraf olarak bilgi sistemlerine erişen kullanıcılara bu konuda standardın getirdiği; bilgi varlıklarının gizlilik, bütünlük, erişilebilirliğinin, temiz masa, temiz ekran politikasını, şifre oluşturma politikasını ve tüm yükümlülükleri kapsamaktadır. Sadece elektronik ortam da tutulan verilerin değil; yazılı, basılı, sözlü ve benzeri ortam da bulunan tüm verilerin güvenliği ile ilgilenmek.

**16- Bilgi Güvenliği Yönetiminin eksiklikleri nelerdir?**

Bu konuda Konya'da yeterli bir danışmanlık firması bulunmamaktadır. Bilgi güvenliği yönetim sistemini bilen çok az olduğu ve Türkiye'de bu istemin tam oturmadığı gözükmektedir. Bu nedenle bizi tam olarak yönlendirebilecek kurum kuruluş ve kişiler bulunmamaktadır.

**17- ISO 27001 standartlarının hepsini birebir uygulamamız gerekir mi?**

Bilgi güvenliği yönetim sisteminde ISO 27001 standartlarının kapsadığı maddelerinin tümünün uygulanacağına dair taahhütte bulunulmuştur.

**18- Kontroller nasıl yapıldı ve kontroller bittikten sonra ne olur?**

Mevcut durum analizleri yapıldıktan sonra kontrollerimiz dokümantasyon sürecinin tekrar kontrol edilerek eksik dokümanların tamamlanması ile uygulama olarak risk analizlerinin değerlendirilmesi eksiklikleri tekrardan giderilmiştir.

**19- BGYS kurulum aşamasından sonra belgelendirme kuruluşunun yaptığı kontrollerde her hangi bir eksiklikle karşılaştınız mı?**

İlk denetim sonrasında toplamda 8 minor uygunsuzluk tespit edilmiştir. Bununla ilgili iki uygunsuzluk durum maddeleri sizinle paylaşılabilir. Bunlar; 1-Risk değerlendirme metodunun tam olarak açıklanmadığı ile ilgili, 2- Web sitesinde bilgi güvenliği ile ilgili olarak politikalarımızın bulunmamasıdır.

**20- Danışmanlık ve eğitim firmasıyla çalışmak bir zorunluluk mu yoksa size kalmış bir tercih midir? Sizin belge almak isteyen kurumlar için tavsiyeniz ne yöndedir?**

Bizim danışmanlık firması ile çalışmamız birlikte standart maddelerinin öğrenilmesi ve uygulanması ile olmuştur. Danışmanlık firma ile çalışmak bir zorunluluk değildir. Fakat bu konuda mutlaka eğitim almak gereli ve şarttır. Bilgi güvenliği yönetim sistemi konusunda belge almak isteyen firmalara tavsiyemiz şirket içinde ham standartları ve teknik konulara hakim, kalite yönetimi konusunda en az bir elaman istihdam etmeleri gereklidir. Şirketin büyüklüğüne göre bu sayı artabilir.

**21- Sertifikayı aldıktan sonra herhangi bir kurumdan size danışmanlık anlamında başvurular oldu mu?**

Bu konuda şu ana kadar herhangi bir başvuru olmamıştır.

**22- Bilgi Güvenliği yönetimi İnsan Kaynakları gelişimine katkı sağlar mı?**

Firmamız bünyesinde bulunan insan kaynakları departmanı ile birlikte yeni işe alınan personele yönelik bilgi güvenliği yönetim sistemi hakkında bilgilendirme, farkındalık eğitimi ve gizlilik sözleşmesi yapılmaktadır. Bu sözleşme sayesinde personelimizin farkındalığı artmakta ve bu konu hakkında gerekli önlemlerin alındığı gözlenmiştir.

**23-Kurumunuz isminin geçmesinde bir sakınca var mı? Uygun değil ise isim belirtmeden yayınlayabiliriz?**

Bu konuda yönetimin vereceği karar önemlidir. Şu an için firma politikası gereği ismimizin geçmesi uygun olmamaktadır.

**24- Peki, tüm çalışanlarınızın sayısını öğrenebilir miyiz?**

Toplamda 100 çalışanımız bulunmaktadır.

**25- Kurumunuzun oluşturduğu BGYS organizasyonunda kimler görevlidir?**

Bu organizasyonda; Toplam kalite yöneticisi, Bilgi işlem sorumlusu ve yönetim temsilcisi olarak 3 kişi görev almıştır.

**C İŞLETMESİ**

**Sektörü :** Hidrolik ekipmanları imalat

**Nace Kodu :** 28.12.05

**1-Bilgi Güvenliği Yönetimini uygulayan kuruluşların kazanımları nelerdir?**

Bilgi varlıklarını en uygun metotlarla gizliliğini, bütünlüğünü kullanılabilirliğini, erişebilirliğini ve kabul edilebilir risk seviyesinin üzerinde bulunan tüm varlıklar için gerekli kontrollerin yapılmasını sağlar. Bunun yanında bilginin gizliliği, imaj ve firma üzerinde olan etkisi ve kazanım sağlamasıdır.

**2- İyi günler öncelikle bize Bilgi Güvenliği Yönetim Sistemini kurma kararınızı nasıl aldığınızı anlatır mısınız?**

Öncelikli kararımız gümrüklemedeki ayrıcalık belgesi olan YYS (Yetkilendirilmiş Yükümlü Statüsü) almaktı. Ayrıca metotlarını da belirlemek de isteğimizdi. Kuruluşumuz bünyesinde bulunan Bilgi güvenliği bilgi varlıklarımızın korunması ve kontrolünün sağlamak için bu kararı almış bulunmaktayız.

**3- Bilgi Güvenliği Yönetim Sistemini kurulumuna ilk hangi konulardan nasıl başladınız?**

İlk olarak, yeni fabrikamızın fiziksel altyapısının bu standardın gereksinimlerine göre tasarlanmış, almış olduğumuz eğitimler ve ilgili danışman firmasının yönlendirmesi sonucunda başlanılmıştır.

**4- Hangi danışmanlık firması ile beraber çalıştınız?**

Bu konuda eğitim ve danışmanlık firmaları ile ilgili araştırmalar yapılmış, tespit ettiğimiz firmalar ile görüşmeler yapılmış, danışmanlık süreçleri konusunda, bilgi edinilmiş ve firmamız hakkında fikir alışverişinde bulunulmuştur. Yapılan görüşmeler sonucunda belirlemiş olduğumuz 3 danışmanlık firmalarıyla daha iyi bir görüşme yapılabilmesi ve süreci yerinde görmeleri için fabrikamıza davet edilmiştir. Firmamız hakkında bu konudaki destek ve taahhütleri sonucunda firmalar hakkında puanlama

yapılmıştır. Yönetimin almış olduğu sonuç ile Kalitetürk Danışmanlık firması ile çalışılmaya karar verilmiştir.

**5- Bilgi Güvenliği Yönetim Sistemini kurulumunda yararlandığınız kaynaklar nelerdir?**

TSE dokümanları, Kalitetürk yardımcı dokümanları ve örnek çalışmaları, çeşitli internette yapılan ilgili paylaşımlar vb. kaynaklar incelenmiştir.

**6- Bilgi Güvenliği Yönetim Sistemini kurum çalışanları dışında kimlerle etkileşim içindedir?**

Üçüncü taraf olan, müşteriler, tedarikçiler, yasa koyucular, bazı kurum ve kuruluşlar

**7- Bilgi Güvenliği Yönetim Sistemini sadece bilgi işlem personeli ile mi yürütülmektedir?**

Bilgi Güvenliği Yönetim Sistemimiz BGY Temsilcisi (BT Müdürü) ve BGY Komitesi tarafından yürütülmekte ve tüm yönetim ve çalışanlar ile desteklenmektedir.

**8- Aldığınız danışmanlık, eğitim ve denetim hizmetleri için ne kadar bir ücret ödediniz?**

Yaklaşık olarak 3 bin Euro kadar ödeme yapılmıştır.

**9- BGYS işletmenizde ne kadar bir süre ile kurulmuştur?**

Süreç kademeli olarak bir yıl sürmüştür.

**10- Bilgi Güvenliği Yönetim Sistemini kurulum süreci nasıl ilerledi?**

a) İlk olarak fiziki yapı BGYS gereksinimlerini karşılayacak şekilde tasarlandı ve yapıldı,

b) Amaç ve hedefler çerçevesinde bir Bilgi Güvenliği Politikası hazırlandı, BGYS kapsamı belirlendi,

c) Envanter Listesi / Bilgi Varlıkları yönetim sistemi gereksinimlerine göre tanımlandı,

d) Tehditler, açıklar ve olasılıklar belirlenerek Risk analizi ve İşleme Planı hazırlandı,

e) Bilgi güvenliği el kitabı, prosedürler, talimatlar, planlar, listeler, destek dokümanlar ve formlar hazırlandı,

f) Gerekli kontroller oluşturularak Uygulanabilirlik Bildirgesi oluşturuldu,

g) Belgelendirme denetimi ve belgelendirme.

**11- Eğitim faaliyetlerinden de bize biraz bahsedebilir misiniz? Katılımlar nasıldı?**

a) Belgelendirme çalışmaları yapacak personele dış kaynaklı eğitimler verildi.

b) Tüm çalışanlarımıza BGYS hakkında genel bilgilendirme ve farkındalık eğitimleri verildi.

c) Belirlenen personele dış kaynaklı iç tetkikçi ve BGYS genel bilgilendirme eğitimleri verildi.

d) Farkındalık eğitimleri ve genel bilgilendirme eğitimleri yıllık olarak tekrarlı verilmektedir.

**12- Varlıklar belirlenirken dikkat edilmesi gereken hususlar nelerdir?**

Firmamız bilgisayar sistemleri bünyesinde bulunan Active Directory yapısının olması nedeniyle bünyemizde bulunan bilgi varlıkların listesinin kullanılması ile. bunun haricinde ise mevcut zimmet, stok envanterinden yararlanılarak oluşturulmuştur. Varlıklar belirlenirken işletmemizde bulunan makine ekipmanlarını değil sadece Bilgi Teknoloji varlıkları; bilgisayar, sunucu, güvenlik kamerası, internet erişimi ve santral ekipmanları baz alınmıştır. Varlıklar belirlenmesinde dikkat edilmesi gerekenler ise, ait olduğu süreci, varlık sahibi, varlık emanetçisi, gizlilik, bütünlük ve erişebilirlik değerlerinin tanımlanması önemlidir.

**13- Bilgi Güvenliği Yönetiminde yaşanan sorunlar nelerdir?**

Gereksinimleri ve kontrolleri zor olan bu sistemde tarafların uyum göstermesinde zorluklar yaşanır.

**14- Kurum personeli BGYS kurulmasına nasıl bakıyor, herhangi bir tepkileri oluyor mu?**

Kurum personelinin gizlilik, bütünlük ve kullanılabilirlik konusunda sınırlama getirmesi ve gereksinimlere uyma konusunda getirdiği iş yükü nedeniyle tepkileri olmaktadır.

**15- Politikalar ve prosedürler neleri kapsıyordu nasıl bir sistemle bunları hazırladınız?**

Politika ve prosedürler, genel itibariyle bilgi varlıklarını tanımlamayı, tehditleri, açıkları ve olasılıkları tanımlamayı, risk analizi yapmayı bunun, bilgi varlıklarının gizliliğine, bütünlüğüne ve erişebilirliğine olan etiklerini tanımlamayı, kontrol ve önlemleri ve bunların nasıl ve kiminle uygulanacağı tanımlamaktadır.

**16- Bilgi Güvenliği Yönetiminin eksiklikleri nelerdir?**

Tarafların kültürel yapıları bu sistemin gereksinimlerine çok uzak olması ve dirençler.

**17- ISO27001 standartlarının hepsini birebir uygulamamız gerekir mi?**

Gerekmektedir. Ancak Ek-A kontrollerinin tamamı kapsama alınmayabilir fakat bütünlük açısından tamamının alınması gerekir.

**18- Kontroller nasıl yapıldı ve kontroller bittikten sonra ne olur?**

Kontroller Ek-A'ya göre belirlenir. Politika, prosedür, talimat çerçevesinde sistemin uygulanıp uygulanmadığı gözlemlerle, yıl içinde yapılan iç ve dış tetkiklerle kontrol edilir. Aksayan kısımlar tekrar gözden geçirilir ve sistem sürekli iyileştirilerek sürekliliği sağlanır.

**19- BGYS kurulum aşamasından sonra belgelendirme kuruluşunun yaptığı kontrollerde her hangi bir eksiklikle karşılaştınız mı?**

Minör uygunsuzluklar tespit edildi, kısa zamanda tamamlandı ve kanıtları ilgili denetim firmasına gönderilerek uygunsuzluklar kapatıldı.

**20- Danışmanlık ve eğitim firmasıyla çalışmak bir zorunluluk mu yoksa size kalmış bir tercih midir? Sizin belge almak isteyen kurumlar için tavsiyeniz ne yöndedir?**

Danışmanlık firmasıyla çalışmak bir tercihtir. Firmanın kaynakları bu sistemi kurmaya, uygulamaya ve kontrol etmeye yeterliyse danışmanlık almayabilir. Öncelikle fiziksel yapıların ve bilgi varlıkların olduğu ortamların sistem gereksinimlerine göre yapılandırılması ve bilgi varlıklarının doğru ve etkin bir şekilde tanımlanması gerekir.

**21- Sertifikayı aldıktan sonra herhangi bir kurumdan size danışmanlık anlamında başvurular oldu mu?**

Hayır

**22- Bilgi Güvenliği yönetimi İnsan Kaynakları gelişimine katkı sağlar mı?**

Sağlar. Eğer Kalite Yönetim Sistemi yoksa istihdam öncesi, istihdam ve istihdam sonrasının bir sistematiğe göre yapılması, görev tanımları ve iş gereksinimleri şartlara uygun bir şekilde tanımlamayı ve uygulamayı sağlar.

**23- Kurumunuz isminin geçmesinde bir sakınca var mı? Uygun değil ise isim belirtmeden yayınlayabiliriz?**

Sanırım bir sakınca yoktur.

**24- Peki, tüm çalışanlarınızın sayısını öğrenebilir miyiz?**

Yaklaşık 150 kişi

**25- Kurumunuzun oluşturduğu BGYS organizasyonunda kimler görevlidir?**

Uygulanması ve uyulması itibariyle tüm personel ve yönetim kurulu, iyileştirme, geliştirme ve sürekliliğinden BGYS Temsilcisi, BGYS Komitesi ve Üst Yönetim sorumludur.

**D İŞLETMESİ**

**Sektörü :** Makine imalat

**Nace Kodu :** 28.12.05

**1- Bilgi Güvenliği Yönetimini uygulayan kuruluşların kazanımları nelerdir?**

En önemli kazanımı bilginin öneminin ve değerinin anlaşılması bence. Kurumsal bilginin güvenliğini sağlamak rekabet gücünü artıran ve koruyan bir uygulama. Yetkilendirilmiş yükümlü statüsü de, özellikle ithalat-ihracat yapan firmalar için büyük kazanım.

**2-İyi günler öncelikle bize BGYS kurma kararınızı nasıl aldığınızı anlatır mısınız?**

Bilgi Güvenliği Yönetim Sistemini kurma kararını; şirketlerin kendi bünyesinde gümrükleme yapılması konusunda çıkan 4458 sayılı Gümrük Kanunu Yönetmeliğine istinaden, bakanlık tarafından sadece ISO 27001 (Bilgi Güvenliği Yönetim Sistemi) ve ISO 9001 (Kalite Yönetim Sistemi) sertifikasyonlarını tamamlamış olan firmalara verilmektedir. Bu konuda gereklilik olduğu için firma olarak hem ithalat ve ihracat yaptığımız için, bu konuyu nasıl firmamız lehine çevirebilir diyerek bu konuda araştırmalar yapılmıştır. Firma Bilgi Güvenliği Yönetim Sisteminin kurulması konusunda gereken koşulların sağlanabilmesi için yapılan tanıtım toplantılara ve eğitimlere katılarak firmamızda ISO 27001 Bilgi Güvenliği Yönetim Sistemi kurma kararı alınmıştır.

**3- Bilgi Güvenliği Yönetimin Sistemi kurulumuna ilk hangi konulardan nasıl başladınız?**

Hali hazırda ISO 9001, ISO 3834-2, ISO 1090-2 sertifikalarımız bulunmaktadır. ISO 14001, ISO 18001 sertifikalarımız bulunmamasına rağmen bu konudaki bütün gereklilikler yerine getirilmektedir. Bütün bunları tek bir çatı altına toplamak için entegre yönetim sistemini kurma çalışmalarına 2011 yılında başlanılmıştır. Bu konudaki çalışmalar neticesinde firma bünyemizde entegre yönetim sistemi bulunmaktadır. Kalite yönetim sistemleri bildiğiniz gibi yaşayan canlı bir organizasyon yapısı olduğu için sürekli geliştirmek, sürekli iyileştirmek durumundasınız. Bu durumda sürekli

gelişen bir yapıya sahip olduğu için bitmeyen bir süreç olduğu söylenebilir. Bilgi Güvenliği kısmında daha önce yapmış olduğumuz çalışmalarının dışında riskler konusunda bir çalışma yapılmamıştır. Bunun haricideki tüm standartların alt yapısı oluşturulmuş ve gerekli şartlar sağlanmıştır. Bilgi Güvenliği Yönetim Sisteminin kurulması konusuna ISO 9001 ile başlanılmıştır.

**4- Hangi danışmanlık firması ile beraber çalıştınız?**

Meyer Belgelendirme Hizmetleri A.Ş. ile hem belgelendirme çalışmaları ile birlikte danışmanlık hizmeti de alınmıştır. Bunun yanında diğer ISO 9001, EN ISO 3834-2, EN1090-2 belgelerimizde aynı danışmanlık firması ile çalışma yapılarak alınmıştır. (Meyer Belgelendirme A.Ş. 2013 yılında Kiwa Belgelendirme Hizmetleri A.Ş. bünyesine katılmıştır.)

**5- BGYS kurulumunda yararlandığınız kaynaklar nelerdir?**

Bilgi Güvenliği Yönetim Sisteminin kurulmasında daha çok danışmanlık firması yönlendirme yapmıştır. Fakat bu konuda daha Gümrük ve Ticaret Bakanlığının göndermiş olduğu ve yayınlamış olduğu tanıtım materyallerden yararlanılmıştır. Bunun dışında Konya Sanayi Odasının düzenlemiş olduğu seminerlere ve aynı zamanda Konya Ticaret Odası'nın Gümrükleme ve Dış Ticaret Eğitimlerine katılım sağlanılmıştır. TSE'nin yayınlamış olduğu ISO/IEC 27001'in standart maddeleri tek tek incelenerek okunmuş ve bu konuda araştırma yapılmaktadır.

**6- BGYS kurum çalışanları dışında kimlerle etkileşim içindedir?**

Bilgi güvenliği denildiği zaman sadece kurum içindeki bilgi güvenliğini kastetmiyorsunuz. Bizim bir sürü paydaşlarımız bulunmaktadır. En önemlisi müşterilerimiz, müşterilerimizin bilgilerini gizli tutmak zorundayız. Müşterimizle, çalışanlarımızla, taşeron firmalarımızla ve alt yüklenici firmalarımızla gizlilik sözleşmesi yapılmaktadır. Onun dışında yasal yükümlülükleri yerine getirmek içinde her türlü hizmet alımlarında mutlaka gizlilik sözleşmesi yapılmaktadır.

**7- BGYS sadece bilgi işlem personeli ile mi yürütülmektedir?**

Bilgi işlem personelimiz Mustafa Bey'in Bilgi Güvenliği ekip şefi olarak bu organizasyonda katılım sağlamaktadır. Firmamızda Ben toplam kalite yöneticisi olarak

görev yapmaktayım. Bütün yönetim sistemlerimiz entegre olduğu için tek elden tarafımca yürütülmektedir.

**8- Aldığınız danışmanlık, eğitim ve denetim hizmetleri için ne kadar bir ücret ödediniz?**

Daha öncede belirttiğim gibi Toplam Kalite Yöneticisi olarak görev yaptığım için bu konuda daha çok hakim olmamız nedeniyle bir çok işlemler ve prosedürleri kendi bünyemizde yapmış bulunmaktayız. ISO 27001 Bilgi Güvenliği Yönetim Sistemi kurulması için firmadan danışmanlık ücreti olarak 1500$, sertifikasyon içinde 2250$, toplamda ise 3750$ ödeme yapılmıştır. Bu konuda danışmanlık firmasından çok az destek alınmıştır.

**9- Bilgi Güvenliği Yönetim Sisteminin Süreci ne kadar sürdü?**

Firmamız 5 yıldan bu yana kalite entegre yönetim sistemi ve kalite alt yapısının mevcut olması nedeniyle sürecin yönetilmesi ve yapılandırmasında pek zorlanılmamıştır. Bu konuda var olan prosedürlerin kullanılması kendimin de, toplam kalite yöneticisi olmamın avantajı ile birlikte bu sistemin kurulma aşamasını bütün dokümantasyon dahil 2-3 hafta da tamamlanmıştır.

**10- Bilgi Güvenliği Yönetim Sistemini kurulum süreci nasıl ilerledi?**

Bizim için kolay bir süreç oldu; çünkü çok iyi yapılandırılmış bir entegre yönetim sistemimiz vardı. Bazı ilavelerle standart gereklerini kolaylıkla sağladık ve kısa sürede sertifikayı aldık.

**11- Eğitim faaliyetlerinden de bize biraz bahsedebilir misiniz? Katılımlar nasıldı?**

Entegre yönetim sisteminin tamamında eğitim faaliyetleri çok önemli; BG için yaptığımız ilaveler eğitim planımızı daha etkili hale getirdi.

**12- Varlıklar belirlenirken dikkat edilmesi gereken hususlar nelerdir?**

Varlık, kurumunuz için değeri olan her şey olduğu için bütün varlıklarımızın liste hazırlanmıştır. Varlık konusunda sadece bilgi işlem olan varlıklara bakılmamıştır. Bu konuda örnek verecek olursak, içeride bulunan CNC tezgahlarımız, kaynak

makinelerimiz, bütün dokümantasyonumuz, projelerimiz ve değerli evraklarımızın hepsi listede yer almaktadır. Bu konuda varlıklar belirlenirken önemli ve kritik durumlarına göre hareket etmek gereklidir. Oluşturulan varlık envanterinde belirtiğimiz üzere bir sınıflandırma yapılmıştır.

**13- Bilgi Güvenliği Yönetiminde yaşanan sorunlar nelerdir?**

Karşılaştığımız en önemli sorun temiz masa ekranları temiz tutmak ve gerek şifre gerekse otomatik kapanma gibi güvenlik önlemlerini gerçekleştirmek daha kolay. Bilgi İşlem birimi tarafından merkezi bir şekilde sağlanan veri güvenliği işin daha teknik ama daha kolay tarafı. Ancak, kişilerin ortada, masalarında veya yazıcı yanlarında evrak bırakmamalarını sağlamak daha zordur. Bu konuda biraz daha fazla eğitim gerekmektedir.

**14- Kurum personeli BGYS kurulmasına nasıl bakıyor, herhangi bir tepkileri oluyor mu?**

Bildiğiniz üzere personelin kullanıldığı bilgisayarın bir başkası tarafından kullanılmasını önlemek, personelin yerinde olmadığı zaman bilgisayar ekranındaki proje, bilgi vb. materyallerin bir başkası tarafından görülmesini engellemek ve bilginin koruması amacı ile yapmış olduğumuz temiz ekran temiz masa uygulamasında zorluklar yaşanmıştır. Bu konu hakkında personelimize gerekli eğitim ve bilinçlendirilme yapılmıştır. Bu konuda belirli süreler belirlenerek ve ayarlanarak bilgisayarların otomatik olarak oturumun kapatılması sağlanmıştır. Temiz ekran çalışmamızda zorlanan kişilerin bilgisayarlarında gerekli ayarlamalar yapılmıştır.

**15- Politikalar ve prosedürler neleri kapsıyordu nasıl bir sistemle bunları hazırladınız?**

Bu politikalara ISO 9001, EN ISO 3834-2, EN 1090-2 bu standartların içermiş olduğu politikalar prosedürler zaten firmamız da mevcut kalite politikaların var olduğu için, ISO 27001 için ise riskler, varlıklar gibi envanterin çalışmasının sonucunda politikalar oluşturulmuş ve beraber hazırlanmıştır. Firmamızın kalite el kitabında politikalar başlığı altında; kalite, çevre, kaynak, iş sağlığı ve güvenliği ve bilgi

güvenliği yönetim sistemi politikalarımız yer almaktadır. Firmamızın bilgi yönetim politikasının bazıları ise şunlardır. Müşteriler dâhil tüm paydaşlara ait bilgi varlıklarının güvenliğini sağlamak, Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek. Gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda bilgi varlıklarının süreç performanslarını ölçmek ve sürekli iyileştirerek yönetmek,

**16- Bilgi Güvenliği Yönetiminin eksiklikleri nelerdir?**

ISO 9001:2015 standardı ile oldukça uyumlu; çok kolay entegre oldu bizim için. Bu nedenle bir eksiklik varsa da farkında olmadık.

**17- ISO 27001 standartlarının hepsini birebir uygulamamız gerekir mi?**

Tüm standart maddeleri, diğer standartlarla entegre bir şekilde bire bir uygulanmaktadır.

**18- Kontroller nasıl yapıldı ve kontroller bittikten sonra ne olur?**

Denetçilere genel olarak sistemin yapısını ve nasıl işlediği konusunda bilgi verilmektedir. Dokümantasyon kısmına inceleme yapıldıktan sonra ise kontroller yapılmaktadır. Kontroller bittikten sonra ise bünyemizde kalite yönetim sistemi bulunduğu için bu sürecin nasıl işlediğini gözlemliyoruz, her türlü geliştirme faaliyetini yapıyoruz, bu konuda ise 3 ayda bir yönetime durum değerlendirmesi ve raporlama yapılmaktadır. Denetim faaliyetlerimiz ise yılda bir kez olmak üzere iç denetim yapılmaktadır. Yapılan denetimler sonucu çıkan uygunsuzlukları düzenleyici önleyici faaliyet belgeleri (DÖF) düzenliyoruz.

**19- BGYS kurulum aşamasından sonra belgelendirme kuruluşunun yaptığı kontrollerde her hangi bir eksiklikle karşılaştınız mı?**

İlk belgelendirme denetimin sonucunda 4 minor hatamız oluşmuştur. Denetim sonrası bu konuda oluşan hatalar DÖF belgeleriyle tamamlanmıştır. Bir sonraki takip denetiminde ise sıfır hata ile geçilmiştir. En son yapılan denetimlerde ise hiç majör hatamız olmamıştır.

**20- Danışmanlık ve eğitim firmasıyla çalışmak bir zorunluluk mu yoksa size kalmış bir tercih midir? Sizin belge almak isteyen kurumlara için tavsiyeniz ne yöndedir?**

Bu konuda ilk başta sistemi öğrenene kadar danışmanlık alınabilir. Danışmanlık sürecinden sonra bu süreci kendi içerinizde sahiplenilmesi gereklidir. Bu süreç içinde danışmanlık firmasının geldiği 3-5 gün ile sadece belgelendirme denetlemesini atlatırsınız, oysa bu süreç yaşan bir süreç olduğu ve sürekli geliştiği için bu konuda danışmanlık yeterli olmayacaktır.

Yönetim sürecini şirketinizde kalıcı olarak oturmak istiyorsanız mutlaka bu sistemin başında biri olmalıdır. Firmanızda veya bünyenizde toplam kalite yöneticisi bulunuyorsa bu konuda danışmanlık firması ile çalışmak bir zorunluluk değildir. Bizim firmamızda birçok kalite sertifikasyonu kendi bünyemizde hazırlanmış ve bu konuda danışmanlık alınmamıştır. Sadece sertifikasyon eğitim konusunda destek alınmıştır.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikası almak isteyen kurumlar mutlaka kendi bünyelerinde kalite yönetim sistemini kuracak, bu yapıyı takip edecek, denetleyecek yeterlilikte veya toplam kalite yöneticisi istihdam edilmeli ve bulundurmalıdırlar. Bu durumun ne gibi bir faydası olduğuna gelince; kendi bünyenizdeki yapıyı içinde olduğunuz sistemin ne gibi ihtiyaçları olduğunu daha iyi biliyor ve bu konuda her an denetleme yapılarak eksiklikler giderilmektedir.

**21- Sertifikayı aldıktan sonra herhangi bir kurumdan size danışmanlık anlamında başvurular oldu mu?**

Konya'da ISO 27001 Bilgi Güvenliği Yönetim Sistemi pek bilinmediği için bu konuda henüz bir başvuru olmamıştır. Konya'da bu sertifikayı alan ilk firma olduğumuzu sanıyorum.

**22- Bilgi Güvenliği yönetimi İnsan Kaynakları gelişimine katkı sağlar mı?**

Tüm yönetim sistemleri İnsan kaynakları gelişimine olumlu katkı sağladığı görüşündeyim. Daha önce de belirttiğim gibi bizde entegre yönetim sistemi uygulandığından hangi yönetim sisteminin daha fazla faydayı oldu bilemiyorum ama hepsinin çok faydası olduğunu düşünüyorum.

**23- Kurumunuz isminin geçmesinde bir sakınca var mı? Uygun değil ise isim belirtmeden yayınlayabiliriz?**

Bu konuda isim belirtmeden yayınlayabilirsiniz.

**24- Peki, tüm çalışanlarınızın sayısını öğrenebilir miyiz?**

Firmamızda çalışan sayısı 220 kişidir.

**25- Kurumunuzun oluşturduğu BGYS organizasyonunda kimler görevlidir veya görevlendirilmiştir?**

Bilgi İşlem Sorumlumuz, bilgi güvenliği ekip şefimiz, bilgi işlem personeli ve bilgi güvenliği ekibi dışında, toplam kalite yönetimi birimi de standardın yürütülmesinde görev yapmaktadır. Bütün yönetim sistemlerimiz entegre olduğu için, dokümantasyonumuz tek elden toplam kalite yöneticisi tarafından yürütülmektedir.

**E İŞLETMESİ**

**Sektörü :** Tarım gübre ilaç üretimi

**Nace Kodu :** 20.20.11

**1- Bilgi Güvenliği Yönetimini uygulayan kuruluşların kazanımları nelerdir?**

Bilgi güvenliğinin kuruluşlara en büyük faydası şudur; bilgi işlem sistemlerinin profesyonel şekilde yönetmek ve yönlendirmektir. Bunlarla alakalı olarak risklerin ve alınacak tedbirleri profesyonel bir yöntemle ortaya koymaktır.

**2- İşletmenizde öncelikle bize Bilgi Güvenliği Yönetim Sistemini kurma kararınızı nasıl aldığınızı anlatır mısınız?**

Bilgi Güvenliği Yönetim Sistemi kararı firmamızın yetkilendirilmiş gümrükleme sertifikasına sahip olabilmenin şartlarından biri olan ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasının mutlaka alınması gerektiğinden ve işletmemizin genel olarak yürüttüğü faaliyetlerin gereği Bilgi Güvenliği Yönetim Sistemi kurulması gerekmiştir.

**3- BGYS kurulumuna ilk hangi konulardan nasıl başladınız?**

Öncelikle ISO 27001 standardının yönetmelik, kanun ve kapsamının belirlenmesi, kapsama girecek olan hangi bölüm ve birimlerin tespiti ile başlanılmıştır. Daha sonra işetmemizin varlık envanterinin çıkarılması bunların ardından ise sırası ile risk değerlendirmesi, politikaların oluşturulması, formlar ve talimatların hazırlanması ve eğitimler ile devam edilmiştir.

**4- Hangi danışmanlık firması ile beraber çalıştınız?**

Bilgi Güvenliği Yönetim Sistemini kurarken her hangi bir danışmanlık firması ile çalışılmamıştır. Türk Standardları Enstitüsü'nün vermiş olduğu ISO 27001 eğitimlerinin yanında Bilgi Güvenliği Yönetim Sistemi Temel ve İç Tetkik Eğitimi'de alınmıştır.

**5- BGYS kurulumunda yararlandığınız kaynaklar nelerdir?**

Bu konuda yararlanılan tek kaynak TSE'den alına eğitimlerde yer alan dokümanlardan ve ISO/IEC 27001'in standart maddelerinden yararlanılmıştır. Bunu

devamında ise Bilgi Güvenliği Yönetim Sistemi Temel ve İç Tetkik Eğitimi'de alınmış ve bu konudaki kaynaklar yararlanılmıştır.

**6- BGYS kurum çalışanları dışında kimlerle etkileşim içindedir?**

Bu konuda detaylı bir bilgi veremiyoruz. Bu konuda paydaşlarımız Bilgi güvenliği yönetim sistemine göre gizlidir. Bu konuya yüzeysel olarak değinmek gerekirse hizmet aldığımız işletme ve birimlerin yanı sıra müşterimizle, taşeron firmalarımızla ve çalışanlarımızla, firmalarımızla ve çalışmalarımızla ilgili olarak gizlilik sözleşmesi yapılmaktadır. Dışarıdan her türlü mal ve hizmet alımlarında yasal yükümlülük gereği iletişim halinde olmakla beraber her zaman gizlilik sözleşmesi düzenlenmektedir.

**7- BGYS sadece bilgi işlem personeli ile mi yürütülmektedir?**

Bilgi güvenliği yönetim sistemi ekip çalışması olması nedeniyle bu ekipte İnsan kaynakları bölümünden, Kalite kontrol bölümünden ve diğer departmanlardan hangisi ile etkileşim dâhilinde oldukları personeller ile de yürütülmektedir. Örnek olarak Arşiv bölümün giriş çıkışları yetkilendirilmiş kişiler ile ilgili olarak kayıtlar tutulmakta ve bu kayıtlar sürekli eğitim ve etkileşim olarak iç denetime tabi tutulmaktadır. Bu durumda Bilgi Güvenliği Yönetim Sistemine arşiv görevlisinide dahil etmiş oluyoruz.

**8- Aldığınız danışmanlık, eğitim ve denetim hizmetleri için ne kadar bir ücret ödediniz?**

Daha öncede belirtiğimiz gibi dışarıdan bu konu hakkında danışmanlık hizmeti alınmamıştır. Türk Standardları Enstitüsü'nün vermiş olduğu eğitim ücreti konusunda yapılan gizlilik anlaşmaları nedeni ile fiyat bilgisi veremiyoruz.

**9- Bilgi Güvenliği Yönetim Sisteminin Süreci ne kadar sürdü?**

Firmamızın daha önce mevcut olan TSE ISO 9001 kalite yönetim sistemi olması nedeniyle, kuruluşumuz bünyesinde toplam kalite yöneticisi olmasının getirdiği kazanım ile birlikte mevcut alt yapının hazır olması nedeniyle sistemin kurulma aşaması 2 ay sürmüştür.

**10- Bilgi Güvenliği Yönetim Sistemini kurulum süreci nasıl ilerledi?**

Bu konuda kapsama girecek olan bölüm ve birimlerin tespiti, ardından varlık envanterinin oluşturulması ile risklerin analizlerinin sonucunda ortaya çıkan yol haritası baz alınarak ilerleme sağlanmıştır.

**11- Eğitim faaliyetlerinden de bize biraz bahsedebilir misiniz? Katılımlar nasıldı?**

ISO/IEC 27001 eğitimleri firma genelindeki tüm departmanları kapsamadığı halde aldığımız eğitimleri tüm departman ve personele yayarak eğitim verilmektedir. Verilen bu eğitimlerde mavi ve beyaz yakalılara ayrı ayrı eğitimler verilmiştir. Yılda 2 kez eğitim verilmektedir. Firmanın almış olduğu politika ve karar neticesinde eğitime katılımlar zorunludur. Eğitime katılan personelin konuya ilk önceki bakışları ile eğitim aldıklarından sonraki bakış açıları farkındalıkları artmıştır. Bu durum eğitimin getirdiği faydayı hem sahada görülmekte ve göz önüne sermektedir.

**12- Varlıklar belirlenirken dikkat edilmesi gereken hususlar nelerdir?**

Varlıklar belirlenirken bu konuda alınan ISO/IEC 27001 eğitimde de olduğu gibi önem sırasına göre düşük, orta, yüksek ve çok yüksek gibi hususlar dikkate alınarak belirlenmektedir. Gizlilik, bütünlük ve erişebilirlik durumlarına dikkat edilmesi gerekir. Örneğin Önemli bir bilgiyi kaybedildiği zaman işletmenin bütünlüğüne, işlerin aksamasına ve iş kaybına uğramaması gerekmektedir. Bu durumda hem varlıklar hem de sahip olduğunuz bilgilerinin değerlendirilmesi oldukça önemlidir.

**13- Bilgi Güvenliği Yönetiminde yaşanan sorunlar nelerdir?**

ISO 27001 standartlarının uygulamasına geçildiği zaman başlangıçta personel tarafından bir dirençle karşılaşılmış daha sonra ilerleyen zamanlarda bu sorunda ortadan kalkmaktadır. Bilgi güvenliği yönetim sisteminde oluşturduğumuz şifre politikasında belirlenen sürelerde değişmesi gereken şifrelerin değiştirilmesi konusunda bir takım sorunlar yaşanmıştır. Personelin eğitimde almış oldukları tam olarak dinlemedikleri ve öğrenmedikleri konuların uygulama safhasında eksik kalınması gibi sorunlar

olabilmektedir.

**14- Kurum personeli BGYS kurulmasına nasıl bakıyor, herhangi bir tepkileri oluyor mu?**

Bilgi güvenliği yönetim sistemi kurulum aşamasında oluşturulan politikaların en üst yönetim tarafından kabul edilip tavizsiz bir şekilde desteklendiği ve uygulamaya geçildiği için herhangi bir sıkıntı olmamıştır.

**15- Politikalar ve prosedürler neleri kapsıyordu nasıl bir sistemle bunları hazırladınız?**

Firmamızda mevcut olan kalite yönetim sistemi politikasının yanında İşçi sağlığı ve güvenliği ve çevre politikalarımızda bulunmaktadır. Mevcut var olan politikalarımıza birlikte bilgi güvenliği yönetim sistemleri politikası da entegre edilmiştir. Bilgi güvenliği politikalarımıza örnek verecek olursak; şifre politikası, temiz ekran/temiz masa, yedekleme, elektronik posta kullanımı ve güvenliği uygulamalarını sayabiliriz.

**16- Bilgi Güvenliği Yönetiminin eksiklikleri nelerdir?**

Bilgi güvenliği yönetim sistemi ISO 27001'de herhangi bir eksiklik görülmemiştir. Bu konuda içerikler net, açık ve detaylarla birlikte fazlası var denilebilir.

**17- ISO 27001 standartlarının hepsini birebir uygulamamız gerekir mi?**

Standart maddelerinin uygulanması her işletme ve kuruma göre farklılık gösterebilmektedir. Bu durumda bazı konular ve içerikler kapsam dışında kalabilmektedir.

**18- Kontroller nasıl yapıldı ve kontroller bittikten sonra ne olur?**

Firmamızda daha öncede belirttiğimiz gibi İç Tetkik Eğitimi ve sertifikasyonuna sahip olmamız nedeniyle, İç denetçilerimiz tarafından yılda 1 kez kontroller yapılmaktadır. Bu kontroller öncesi ve sonrası ilgili birimlere ve yönetime periyodik olarak raporlar sunulmaktadır.

**19- BGYS kurulum aşamasından sonra belgelendirme kuruluşunun yaptığı kontrollerde her hangi bir eksiklikle karşılaştınız mı?**

Bu konu firmamızın Bilgi güvenliği politikası gereği paylaşılması uygun görülmemektedir.

**20- Danışmanlık ve eğitim firmasıyla çalışmak bir zorunluluk mu yoksa size kalmış bir tercih midir? Sizin belge almak isteyen kurumlara için tavsiyeniz ne yöndedir?**

Her hangi bir danışmanlık firması ile çalışmak bir zorunluluk değildir. Bu konuda firma bünyenizde; toplam kalite yönetimi ve bilgi işlem, network uzmanı bulundurmanız gerekmektedir. Bu konuda bir tarafta dokümantasyon, prosedürlerin hazırlanması, diğer bir tarafta ise uygulama ayağı bulunmaktadır. Uygulamayı yapacak olan bilgi işlem departmanının, kalite yönetimi uzmanına doğru aktarımın yapılması ve uygulanması gerekmektedir. ISO 27001 sertifikası almak isteyen firmalara ilk önerimiz bu konuda detaylı bir eğitim alınması gereklidir. Danışmanlık hizmeti içim; danışman firmaların bünyesinde bulunan uzmanlarının tecrübe ve bilgilerine, hizmet alımı yapılacak olan firmanın bu konuda önceden yaptıkları, uygulamaları, çalışmaları, referansları ve sözleşmeleri, incelenmesi tavsiye ediyoruz.

**21- Sertifikayı aldıktan sonra herhangi bir kurumdan size danışmanlık anlamında başvurular oldu mu?**

ISO 27001 Bilgi Güvenliği Yönetim Sistemi hakkında bize başvuru yapan bir firma olmuştur. Bu gelen talep doğrultusunda yönetimden alınan izin dahilinde ilgili firmanın kalite yöneticisi ve bilgi işlem sorumlusu ile birlikte bilgilendirme toplantısı yapılmıştır.

**22- Bilgi Güvenliği yönetimi İnsan Kaynakları gelişimine katkı sağlar mı?**

Personelin bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak kurum çalışanlarına ve yeni işe giren çalışanlara verilmektedir. Bu konuda hem işe yeni giren ve ayrılan personellerle gizlilik anlaşması yapılmaktadır. Bu durumda insan kaynaklarının hem kontrolünü hem de gelişimine katkı sağlamaktadır.

**23- Kurumunuz isminin geçmesinde bir sakınca var mı? Uygun değil ise isim belirtmeden yayınlayabiliriz?**

Bu konuda isim vermeniz firmamızca uygun görülmemektedir.

**24- Peki, tüm çalışanlarınızın sayısını öğrenebilir miyiz?**

Firmamızda çalışan sayısı 250 kişidir.

**25- Kurumunuzun oluşturduğu BGYS organizasyonunda kimler görevlidir veya görevlendirilmiştir?**

Bilgi güvenliği yönetim sistemi ekibi 4 kişiden oluşturulmuştur. Kimlerin görevli olması konusunda ise bilginin önem derecesi yüksek olan servis ve departman yöneticileri olmalıdır. Bu organizasyonda mutlaka olması gereken birimlerin başında, bilgi işlem, yazı işleri, toplam kalite yöneticisi ve yönetimden mutlaka bir kişi olması gereklidir.

# ÖZGEÇMİŞ

**Kişisel Bilgiler**

| | |
|---|---|
| Adı Soyadı | : Mustafa YILMAZ |
| Doğum Yeri ve Tarihi | : KONYA, 25.01.1975 |

**Eğitim Durumu**

| | |
|---|---|
| Lisans Öğrenimi | : Anadolu Üniversitesi İşletme Fakültesi |
| Bildiği Yabancı Diller | : İngilizce |

**İş Deneyimi**

| | |
|---|---|
| Projeler | : Konya Ticaret Odası, Dijital Arşiv Projesi, Teknik Destek Uzmanı<br><br>Konya Ticaret Odası, Hazır Giyim Projesi, Web Tasarım, Yazılım ve Grafik<br><br>Konya Ticaret Odası, Ayakkabıcılık Eğitim Merkezi Projesi, Web Tasarım, Yazılım ve Grafik<br><br>Konya Ticaret Odası, Otomotiv Mekatroniği Projesi, Web Tasarım, Yazılım ve Grafik |
| Çalıştığı Kurumlar | : - Büyük Konya Dershanesi<br>- Sistem Dershaneleri<br>- Sayha Granit A.Ş.<br>- Konya Ticaret Odası - Bilgi İşlem |

**İletişim**


| | |
|---|---|
| E-Posta Adresi | : myilmaz@kto.org.tr ; bilgiguvenliktr@gmail.com |


| | |
|---|---|
| **Tarih** | : 22/10/2018 |