T.C. DOĞUŞ ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ: ERİŞİM KONTROL POLİTİKASI ÜZERİNE BİR İNCELEME

YÜKSEK LİSANS TEZİ

KÜBRA AKTAŞ

201695008

DANIŞMAN:

DR. ÖĞR. ÜYESİ YASEMİN KARAGÜL

İstanbul, 2020

	YÜKSEK LİSANS TEZ SINAV TUTANAĞI	Doküman No	FR.1.26
		Yürürlük Tarihi	1.11.2017
		Revizyon Tarihi	1.11.2017
		Revizyon No	1
		Sayfa	1 / 1

SOSYAL BİLİMLER / FEN BİLİMLERİ ENSTİTÜSÜ

Tarih 21./02/2020

Anabilim/Anasanat Dalı : Bilgisayar Mühendisliği

Öğrencinin Adı Soyadı : KÜBRA AKTAŞ

Öğrenci No : 201695008

Tez Danışmanının Adı Soyadı : Dr. Öğr. Üyesi Yaşemin KARAGÜL

İkinci Tez Danışmanının Adı Soyadı : —

Tezin Başlığı : ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ: ERİŞİM KONTROL POLİTİKASI ÜZERİNE BİR İNCELEME

Doğuş Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin 32.Maddesi uyarınca yapılan değerlendirmeler sonunda;

☒ **tezin kabul edilmesine** ☐ **tezde düzeltme verilmesine** ☐ **tezin reddedilmesine**

oy birliği / oy çokluğu ile karar verilmiştir.Gereği için arz olunur.

Danışman Üye

Dr. Öğr. Üyesi Yaşemin Karagül

Üye

Dr. Öğr. Üyesi Dilek Tükel

Üye

Dr. Öğr. Üyesi Oğuzhan Kıvrak

Üye

Anabilim/Anasanat Dalı Başkanı Onayı:

Dr. Öğr. Üyesi Yaşemin Karagül

(Form No: FR-001, Revizyon Tarihi:30.09.2016, Revizyon No:00)

YEMİN METNİ

Yüksek Lisans tezi olarak sunduğum "ISO 27001 Bilgi Güvenliği Yönetim Sistemi: Erişim Kontrol Politikası Üzerine Bir İnceleme" adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden eserlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

Kübra AKTAŞ

21.02.2020

ÖNSÖZ

Tez çalışmam süresince engin bilgi ve tecrübelerini esirgemeyen kıymetli danışman hocam sayın Dr. Öğr. Üyesi Yasemin KARAGÜL'e teşekkürlerimi sunarım.

Tez sürecinin değerlendirilmesinde ve geliştirilmesinde değerli katkılar sunan hocalarım Dr. Öğr. Üyesi Oğuzhan KIVRAK'a ve Dr. Öğr. Üyesi Dilek TÜKEL'e teşekkür ederim.

Değerli görüş ve yönlendirmeleriyle çalışmama katkı sağlayarak bana can-ı gönülden destek veren Veysel Bilal ARSLANKARA'ya, tez yazma sürecinde teşvikleri ve destekleriyle her zaman yanımda olan İpek Selek AKGÜN'e teşekkürü borç bilirim.

ISO 27001 BGYS ile ilgili bilgi edinmeme yardımcı olan ve deneyimlerini benimle paylaşan Emir ARSLANTÜRK'e, ISO 27001 BGYS eğitimini veren hocam Sinan TATLIGİLE'e ve anket çalışmaları sırasında destek veren tüm arkadaşlarıma teşekkür ederim.

Destekleriyle beni hiçbir zaman yalnız bırakmayan ve hakkını bu dünyada ödeyemeyeceğimi bildiğim manevi abim Sertan ARSLAN'a sonuz teşekkürler.

Eğitim hayatım boyunca ve sonrasında hiçbir fedakarlıktan kaçınmayan en büyük destekçim sevgili Annem Nuray'a ve sonsuz sevgisi ile her zaman yanımda olan Anneannem Sebiha ÇEVİK'e minnet ve şükranlarımı sunarım. İyi ki varsınız.

İstanbul, 2020 **KÜBRA AKTAŞ**

ÖZET

Küreselleşen dünyada, teknolojinin gelişmesi ile birlikte önem kazanan kavramlardan biri de bilgi güvenliğidir. Bilgi güvenliği, kurum ve kuruluşların sahip olduğu açık ya da gizli bilgi ve belgelerin kurumsal yapı dışına çıkarılmasını önlemek, yetkisiz ya da izinsiz girişimleri engellemek adına erişim yönetimi sisteminin devreye konulması olarak karşımıza çıkmaktadır. Bu süreçlerin yönetiminde bir çerçeve sunan ISO 27001 Bilgi Güvenliği Yönetim Sistemine (BGYS) kurum ve kuruluşların talepleri artmış ve artmaya da devam etmektedir. Bununla beraber ISO 27001 BGYS belgesine sahip olan şirketlerin de bu belgeye sahip olmanın getirdiği uygulama süreçlerinin ne denli etkili işletilip işletilmediğinin belirlenmesi önem arz etmektedir.

Yapılan birçok araştırma, şirketlerde yaşanan bilgi güvenliği vakalarında, şirket çalışanlarının şirket bilgi güvenliğine yönelik tehditlere ortam hazırlayabileceği, bunun neticesinde de birçok maddi ve manevi zararlarla şirketlerini karşı karşıya bırakabilecekleri görülmüştür. Bu durum şirketlerin bilgi sistemlerine yönelik olarak erişim kontrol politikalarının ne kadar önemli olduğunu göstermektedir. Bu bağlamda çalışmanın amacı BGYS standartları içerisinde uluslararası geçerliğe sahip olan ISO 27001 BGYS kapsamında yer alan erişim kontrol protokolünün şirketler için önem düzeyinin, şirketlerin bilgi güvenliğinin sağlanmasındaki etkilerinin incelenmesidir.

Çalışma kapsamında 5'li Likert ölçeği ile hazırlanan ankete, farklı sektör (eğitim, finans vb.) ve seviyeden (üst düzey yönetici, orta düzey yönetici vb.) 343 çalışan katılmıştır. ISO 27001 BGYS'ye sahip olan ve olmayan şirketlerin erişim güvenlik düzeyleri incelenerek, elde edilen veriler üzerinde yapılan istatistiki analizlerle karşılaştırmalar yapılmıştır ve BGYS belgesine sahip olan şirketlerin erişim kontrol politikalarının bilgi güvenliğine ilişkin risklerin en aza indirildiği görülmüştür.

Anahtar Kelimeler: Bilgi Güvenliği Yönetim Sistemi, Erişim Kontrolü, ISO 27001, ISO 27002, Şirket çalışanları

ABSTRACT

Information security is one of the concepts that gain importance with technological innovations in the globalizing world. It can be defined as the application of an access management system to prevent the removal of explicit or confidential information and documents owned by institutions and organizations and to prevent unauthorized or unsanctioned attempts. The demands of institutions and organizations to ISO 27001 Information Security Management System (ISMS) providing a framework for the management of these processes have increased and continue to increase. Additionally, it has importance to what extent effectively the companies that have an ISO 27001 ISMS certificate operate the implementation processes stemming from having this document.

Many studies have indicated that in the events of information security in companies, company employees may pave the way for the threats to information security of the company, and as a result, they may make their company confront with many material and moral damages. This situation shows how important the access control policies of companies for information systems are. In this context, the existing study aims to examine the importance level of the access control protocol which is within the scope of ISO 27001 ISMS, which has international validity within the ISMS standards, and the effects of that on providing the information security of companies.

343 employees from different sectors (education, finance, etc.) and levels (senior manager, mid-level manager, etc.) participated in the questionnaire which was prepared with a 5-point Likert scale. By examining the access security levels of companies with and without ISO 27001 ISMS, comparisons were made with statistical analysis on the data obtained, and it was seen that the risks of information security of the access control policies of the companies that have ISMS certificate were minimized.

Keywords: Information Security Management System, Access Control, ISO 27001, ISO 27002, Company employees

İÇİNDEKİLER

Sayfa No.

TABLO LİSTESİ

Sayfa No.

ŞEKİL LİSTESİ

Sayfa No.

KISALTMALAR

BGYS : Bilgi güvenliği Yönetim Sistemi

BT : Bilgi Teknolojileri

COBIT : Bilgi Teknolojileri İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology)

CSI : Crime Scene Investigation (Olay Yeri İnceleme)

FBI : Federal Soruşturma Bürosu (Federal Bureau Of Investigation)

GFSI : Global Finansal Hizmet Sektörü (Global Financial Service Industry)

GSYİH : Gayrisafi Yurt İçi Hasıla

IEC : Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)

IP : Internet Protokol (İnternet Protokolü)

ISO : Uluslararası Standart Organizasyonu (International Standart Organization)

IT : Bilgi Teknolojileri (Information Technologies)

ITIL : Bilgi Teknolojileri Altyapı Kütüphanesi (Information Technology Infrastructure Library)

KVKK : Kişisel Verilerin Korunması Kanunu

LDAP : Hafif Dizin Erişim Protokolü (Lightweight Directory Access Protocol)

MAC : Ortam Erişim Kontrolü (Media Access Control)

PAM : Ayrıcalıklı Kullanıcı Yönetimi (Privileged User Management)

PUKÖ : Planla-Uygula-Kontrol Et-Önlem Al

SSO : Tek Oturum Açma (Single Sign On)

TBGM : Ticari Bilgisayar Güveliği Merkezi

TDK : Türk Dil Kurumu

TS : Türk Standardı

TÜRKAK : Türk Akreditasyon Kurumu

UBB : Ulusal Bilgisayar Kullanıcıları Birliği

1. GİRİŞ

Teknolojinin gelişmesi ve bilimin ilerlemesi ile bilgi tüm işletmeler için önemli bir faktör haline gelmiştir. Bilgi tek başına bile önemli iken bilginin işlenmesi ve yönetilmesi bilgiyi daha da önemli bir seviyeye getirmiştir. Bu aşamada bilgiyi işlerken diğer yanda bilginin saklanması, korunması, bilginin yönetilmesi ve bu süreçte iş sürekliliğinin güvenliğinin sağlanması işletmelerin öncelikli gündemini oluşturmaktadır.

Bu kapsamda öne çıkan ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), işletmelerin bilgilerini korumaları için oluşturulmuş uluslararası bir standarttır. BGYS politikasının bir süreç olarak işletme yönetimine entegre edilmesi; işletmenin hedefleri doğrultusunda standardın uygulanması, incelenmesi ve gözden geçirme sürecinde düzenli olarak geliştirilmesi gereklidir. Ayrıca tüm yapılan uygulamaların işletmenin diğer iş süreçlerini aksatmayacak şekilde olması önemlidir.

BGYS politikası işletmeler tarafından uygulanırken bu süreçteki adımlardan biri olan erişim politikası olarak karşımıza çıkmaktadır. İşletme çalışanlarının kendi alanları ile ilgili olsun ya da olmasın her kaynağa istedikleri an erişim sağlamamaları gerekmektedir. Erişim kontrol politikasının hedefi doğru kişinin, doğru bilgiye doğru zamanda ulaşmasıdır. Bu sebeple yetkilendirme ve erişim haklarının tanımlanması önemlidir. Bu durum bilginin bütünlüğü, gizliliği ve erişilebilirliğinin korunması açısından önemlidir.

Erişim kontrolü gerek fiziksel gerekse sistemsel olmak üzere kişilerin değer verdiği varlıkları korumaya başladığından bu yana süre gelen önemli bir kavramdır. Çağımızda kullanılan bilgi teknolojilerinde en temel ve yaygın güvenlik düzeyi olan erişim kontrolü, kullanıcıların bilgi sistemlerine erişimi ile ilgili "kimin ne yapacağı" kararının doğru seçimidir. Erişim kontrolü çeşitli biçimlerde karşımıza çıkabilir. Kullanıcının bilgi sistemlerine izninin belirlenmesinin yanında, sistemi ne zaman ve nasıl kullanacağı da sınırlandırılabilir. Örneğin, kullanıcının bilgi sistemlerine belirtilen sürede erişimi sağlanabilir (Can & Ünalir, 2010).

Tüm bu bağlam ışığında, yapılan bu araştırma toplamda dokuz bölümden oluşmaktadır. Birinci bölüm olan bu bölümde çalışmanın gerekçesi üzerinde durularak ön bilgiler sunulmuştur. Devam eden ikinci bölümde ISO 27001 BGYS ve erişim kontrol

politikası ile ilgili alan yazın çalışmalarına yer verilmektedir. Üçüncü bölümde bilgi güvenliği kavramına yönelik tanımlar ve kavramsal çerçeve sunulmaktadır. Dördüncü bölümde ISO 27001 BGYS'nin kurulması ve uygulanması aşamaları anlatılmaktadır. Beşinci bölümde, ISO 27001 BGYS içerisinde yer alan A9 Erişim Kontrol Politikası ve Kontrol Maddeleri açıklanmaktadır. Altıncı bölümde araştırma metodu, yedinci bölümde ISO 27001 BGYS ve erişim protokolü hakkında yapılan metodolojik çalışmaya ilişkin bulgular ele alınmaktadır. Sekizinci ve dokuzuncu bölümde ise araştırma bulgularına yönelik tartışmalar, sonuçlar ve öneriler değerlendirilmektedir.

2. BGYS ve ERİŞİM KONTROL POLİTİKASINA YÖNELİK YAPILAN ALANYAZIN ÇALIŞMALARI

Bu bölümde BGYS ve kapsamında yer alan erişim kontrol politikasına ilişkin yapılan alanyazın çalışmaları yer almaktadır.

Bingöl (2010), yapmış olduğu çalışmada, küçük işletmeler için BGYS sisteminin kurulması, uygulanması, yönetilmesi sürecinin kolaylaştırılması ve danışmanlık hizmeti maliyetlerinin düşürülmesi amacıyla açık kaynak kodlu yazılım ile oluşturulacak bir otomasyon hizmeti önerisinde bulunmuştur.

Haklı (2012), yürütmüş olduğu çalışmada, kamu kurumları için bilgi güvenliği yönetim standardının kurulması, uygulanması ve yönetilmesi amacıyla bir model önerisi sunulmuştur. Önerilen model uygulama yazılım ile desteklenmiştir.

Mete (2010), BGYS'nin bilgi işlem merkezlerinde uygulanması, Kahraman (2006) BGYS'nin Aselsan A.Ş.'de uygulanması, Demirok (2016) BGYS'nin vakıf üniversitesine uygulanması sürecine yer vermiştir.

Kandemirli (2012), Dünyada en yaygın kullanılan sistemlerden ISO 27001, CobIT ve ITIL Güvenlik Yönetimi süreçlerini incelemiş ve kendi içlerinde karşılaştırma yapmıştır. Bu standartların bilgi güvenliği alanında ortak noktalarının fazla olmasına rağmen, kapsam ve derinlik bakımından birbirlerinden farklı olduğu bu sebeple hangisinin seçilmesi konusunda; şirketin stratejileri, politikaları ve gereksinimleri doğrultusunda, kullanılacak standardın kapsamı, uygulanabilirlik ve maliyet parametrelerine göre değişiklik gösterdiği ortaya çıkmıştır.

Ganbat (2013), ISO/IEC 27001 BGYS ve ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi ilişkisini incelemiştir. BGYS sürecinin daha kolay anlaşılabilir ve uygulanabilir olarak tanımlamayı amaçlanmıştır.

Demirtaş (2013), BGYS'nin başarısını etkileyen faktörleri belirlemeye yönelik bir anket çalışması yapılmış ve bilgi güvenliği performansını etkileyen unsurların bulunması hedeflenmiştir. BGYS'nin kurulması, uygulanması ve iyileştirilmesi için model önerisinde bulunulmuştur. Anket sonuçlarında BGYS'nin iş süreçlerine, teknoloji gelişimine, insan kaynakları gelişimine olumlu yönde katkı sağladığı bulguları ortaya çıkmıştır.

Yılmaz (2018), Konya ilinde ISO/IEC 27001 BGYS belgesi almış işletmelerle 25 soruluk bir mülakat yapılarak, bilgi güvenliği sisteminin kurulum aşamasında yaşanan süreci ele alarak işletmelere uygulanabilecek çözüm önerilerinde bulunulmuştur. Mülakat sonucunda karşılaşılan sorunlar; ISO/IEC 27001 sertifikasında yapılması mecburi penetrasyon testinin Konya ilinde yapabilecek konusunda uzman firmaların olmayışı, BGYS'nin kurulum sürecinde yaşanan emek boşa zaman kaybı olarak görülmüş, BGYS'nin kuruma uzun vadeli bir fayda sağlamayacağı farkındalığı ortaya çıkmıştır. Öneri olarak; daha önce aynı sektörde bulunan firmalar ile iletişime geçerek bu süreçte yaşadıkları problemler, edindikleri tecrübeler, yaşadıkları problemlere karşı buldukları çözümler ile ilgili bilgi alışverişinde bulunulması, işleri hızlandıracağı ve sürecin ilerlemesinde faydalı katkılarda bulunarak kolaylık sağlayacağı düşünülmüştür.

Tuygun (2018), ISO 27001 standardına sahip olan bir kamu kurumunun üst yönetimi ve kurum personel açısından ayrı ayrı değerlendirilerek, uygulanabilirliğinin incelenmesi ve ölçülmesi amacıyla 22 soruluk bir anket çalışması yapılmıştır. Kurumun ISO/IEC 27001 hakkındaki fikirleri, farkındalığı ve bu standarda sahip kurumun bilgi güvenliği ile olan etkileşimi üzerine bir inceleme yapılarak sonuçları üzerine durulmuştur. Anket sonuçlarına göre; kurum yönetiminin büyük bir kısmı sertifikaya sahip olan kurumun saygınlık kazandığı ve kurumsal süreçlerin yürütülesinde olumlu yönde etkilediği görüşü ortaya çıkmıştır. Kurum personelinin verilen eğitimler, süresi, verimliliği konusunda olumlu düşündükleri ortaya çıkmış ve genel olarak kurum personelinin BGYS sistemine güven duyduğu görülmektedir.

Gürcan (2014), Finans sektöründe olan firmaların sahip olduğu bilgi güvenliği yapılarının ISO 27001:2013 standardına göre karşılaştırarak değerlendirilmesini sağlayan bir anket çalışması hazırlanmıştır. Anket sonuçlardan kurumun ve çalışanların olgunluk seviyeleri görülmesi amaçlanmıştır. Verilen cevaplara göre erişim kontrol olgunluk seviyesi kısmında katılımcıların erişim kontrol politikasını uyguladığı, belirli aralıklarla değerlendirme ve geliştirme yaptığı gözlemlenmiştir.

Çetinkaya (2008)'nın araştırmasında web tabanlı bir envanter sistemi kullanılarak BGYS kullanan firmaların bilgi güvenliği sistemlerinin uygulanması bireysel ve kurumsal altyapı bilgisi test edilmek istenmiştir. Yapılan anket sonucunda "İş sürekliliği, uyum, bilgi güvenliği ihlal olay yönetimi" ile ilgili eksiklikler bulunmuştur. Bilgi güvenliği alanında çalışma yapan firmalarda daha iyi sonuçlara rastlanmıştır. Erişim

Kontrol Protokolü ile ilgili kısmında uyumluluk skoru 15 üzerinden 10.3, uyumluluk ise 100 üzerinden %68,7 bulunmuştur.

Alsultanny (2014), Eğitim sektöründe yapılan 61 üniversiteden 320 kişinin katıldığı bir anket çalışması yapılmış, üniversite ağının dış saldırılardan korunması düzeyi %62,6 kritik, tanımlanan ayrıcalıkların ihtiyaçları düzeyinde sorusuna verilen yanıtlar %61,6 kritik, periyodik olarak parola değiştirilmesi cevabı ise %43,8 zayıf bulunmuştur. Genel erişim kontrol faktörünün düzeyi ise 100 üzerinden %60,89 kritik düzeyde bulunmuştur.

Bildiğimiz kadarıyla yapılan literatür araştırmalarında Türkiye'deki erişim kontrol politikalarının ISO 27001 BGYS çerçevesinde çok yer verilmediği ve bu alandaki çalışmaların alan yazındaki açığı yeterli seviyede kapatmadığı görülmüştür. Bu nedenle erişim kontrol politikası alanında çalışma yapılması planlanmıştır.

Bu tez çalışmasında ISO 27001 BGYS'nin kurulum süreci, kurulum sürecinin içinde yer alan maddelerden A9 Erişim Kontrol Protokolü maddeleri etkin bir erişim kontrol yönetim oluşturulması ve uygulanması için gerekli kontrol süreçlerini açıklamaktadır. Aynı zamanda ISO 27001 BGYS standardına sahip kurumların erişim kontrol yönetimi ile bu standarda sahip olmayan kurumların erişim kontrol yönetimi arasındaki fark incelenmiştir.

İncelenen alanyazın çalışmalarında; ISO 27001 BGYS'nin kurumlara uygulanması sürecinin nasıl ilerlediği ile ilgili bilgilerden yararlanılmış, tez içinde yer alan BGYS'nin kurulması, uygulanması ve yönetilmesi sürecinin aşamaları başlığı altında ilgili çalışmalardan derlenmiştir. Erişimin kontrolü ile ilgili araştırmalardan faydalanılarak "Bölüm 5 -ISO 27001 ve Erişim Kontrolü Protokolü Politikası ve Kontrol Maddeleri" başlığı oluşturulmuştur.

3. BİLGİ GÜVENLİĞİ

3.1 Bilgi

Bilgi kavramı, uzay, bilgi ya da teknoloji gibi isimlendirmelerle çağrılan günümüzde en çok önem ve değer verilen kavramlardan biri olarak karşımıza çıkmaktadır. Türk Dil Kurumu tarafından bilgi "insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat" veya "insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf" şeklinde tanımlamıştır (TDK, 2019). Dolayısıyla bilgi ister birey, isterse kurum ya da kuruluş olsun değer oluşturması ve kazandırması itibariyle korunması gereken bir varlık olarak ele alınmaktadır.

3.2 Bilgi Güvenliği

Bilgi güvenliği, bir varlık olarak ele alındığında bilginin, oluşabilecek zararlardan korunması, doğru teknolojinin, doğru amaçlarla ve doğru bir şekilde kullanılarak bilgiye yetkisiz kişiler tarafından her ortamda ulaşılmasının önlenmesi olarak tanımlanır (Canberk & Sağıroğlu, 2006).

Bilginin önemi arttıkça bilginin korunma istemi yani bilgi güvenliği de o derece önem kazanmaktadır. Bilgi, teknoloji çağında her tür ortamda bulanabildiği ve paylaşılabildiği için bilginin korunması adına daha çok önlem alınması ihtiyacı doğmuştur. Bilgi kaybının yaratacağı olumsuz riskleri azaltmak ve bilginin değiştirilmeden korunmasını sağlamak kurumların en çok dikkat ettikleri konu haline gelmiştir. Bilgi güvenliğinin temelinde bilgi güvenliğinin üç temel unsuru Şekil 3.1'de gösterilmektedir.

Şekil 3. 1 Bilgi Güvenliğinin Üç Temel Unsuru

- **Gizlilik (Confidentiality):** Sadece erişim yetkisi olan kişilerin bilgiye ulaşmasına izin verilmesi ve önemli bilgilerin yetkisiz kişilerin eline geçmesinin önlenmesidir.
- **Bütünlük (Integrity):** Verinin bir bütün olarak korunmasını sağlamak amacı ile yetkisiz kişilerce verilerin silinmesini veya yeni veri eklenmesini, değiştirilmesini, bozulmasını önlemektir. Verinin eksiksiz olmasını sağlamaktır.
- **Erişilebilirlik (Availability):** Bilginin her an ulaşılabilir ve kullanılabilir olmasıdır. Kişinin kullanım hakkının bulunduğu bilgi kaynağına rahat erişebilmesidir.

Bilginin gizliliğinin sağlanması o bilginin erişilebilirliğini engellememelidir. Ayrıca erişilebilen bilginin bütünlüğünün de sağlanması gerekir. Erişimi sağlanan bir bilginin bütünlüğü sağlanmıyor ise eksik ya da yanlış bilgi söz konusu olacak ve olumsuz sonuçlar doğurabilecektir. Gizli olan bir bilgiye yetki sahibi kullanıcı erişmek istediğinde erişememesi yine kullanılamaz durumda olan bu bilginin bir anlamı olmayacaktır. Dolayısıyla bu üç temel unsur toplamında bilginin güvenliği kavramını oluşturmaktadır (Altun, 2014).

3.3 Bilgi Güvenliğinin Kurumlar Açısından Önemi

Çağımızda politik, ekonomik ve sosyal örgütlerin zamanla karmaşık bir yapı haline gelmesi ile bu durumun idaresi ve denetimi, bilgiye daha çok ihtiyaç duyulmasına neden olmuştur. Günümüz örgütlerinde ihtiyaç duyulan bilgi miktarı gün geçtikçe çoğalmış ve bu nedenle çeşitli ve büyük hacimlere sahip olan bilgi kümelerini anlamak, yorumlamak ve hatırlamak gerek zaman ve gerekse kapasite bakımından zordur. Bu tarz bilgiler ancak sistemli, etkili ve verimli bir şekilde örgütler tarafından çalıştırılabilir. Genel olarak geçmişi anımsamak, günü takip edebilmek ve geleceği planlayabilmek için örgütler bilgiye ihtiyaç duymaktadır (Bensghir, 1996).

Kurumlar açısından bilgi önemli bir faktördür. Günümüzde bilgi artık elektronik ortamlarda daha sık kullanıldığı için, firmalar ve kurumlar açısından değişik güvenlik problemlerinin oluşmasına neden olmuştur. Teknolojinin gün geçtikçe gelişmesi ile bu durum daha da artış göstermiş; şirketlerde bilgi güvenliğinin sağlanması şirketlerin imajı, güvenilirliği ve faaliyetlerinin sürdürülebilmesi açısından çok önemli bir durum olarak karşımıza çıkmaktadır (Şahinaslan, Kantürk, Şahinaslan, & Borandağ, 2009).

Bilgi yönetimi, işletmenin en doğru kararları alarak rekabet üstünlüğü oluşturabilmeleri için bilginin planlı ve sistemli bir şekilde oluşturulması, sürekli güncellenmesi, depolanması, paylaşılması ve kullanılması şeklinde tanımlanabilir (Durna & Uzun, 2008).

Bilgiyi yönetmek zorlu bir süreci kapsamaktadır bu sebeple bilginin korunması önemli bir faktör olarak karşımıza çıkmaktadır. Çünkü güvenli saklayamadığımız bilgilerin yönetimi sağlıklı olmamaktadır. Bilgilerin güvenli saklanması, bilgiye doğru kişilerin erişim sağlaması alınması gereken önlemlerden biri olarak karşımıza çıkmaktadır. Bu açıdan bakıldığında erişim yetkilerinin kontrolü yeterli sağlanmadığı durumda maddi manevi zararlara neden olduğu görülmüştür. Bu bağlamda yapılan araştırmalara aşağıda yer verilmiştir.

2008 yılında yapılan CSI ve FBI kurumlarının Amerika Birleşik Devletleri'nde 522 kuruma (devlet veya özel sektör) yapmış oldukları araştırmanın sonuçlarına göre; %42 sinde mobil cihaz, cep bilgisayarları çalınmış; %49'unda solucan, virüs, truva atı gibi zararlı kod saldırıları gerçekleşmiş; %44 ü şirket çalışanları tarafından internet ve diğer yetkileri ve erişimleri suiistimal etmiştir. Söz konusu 522 kurum yıl içinde 156 Milyon ABD doları kaybetmiştir (Richardson & Director, 2008). Erişim yönetimi kontrol edilmediğinde kurumun itibarını zedeleyen maddi ve manevi kayıplara neden olabilmektedir.

2017'de yapılan başka bir araştırmaya göre 965,6 milyon bilgi sızıntısı olayının 1505'i kişiseldir. %32,2'si dışardan gelen art niyetli saldırılardan ve %65,4'ü ise şirket çalışanlarından oluşmaktadır. Kişisel veriler ve finansal bilgiler %90,8 oranla en çok saldırılan alanlardır. Ağ bağlantıları %45,6 ile bilgi sızıntısının en çok gerçekleştiği kanal olmaktadır. Bilgi sızıntısı en yüksek oranla ticari şirketlerde gerçekleşmektedir ve saldırılar için en cazip olan ekonomi dalları ise yüksek teknoloji, ticaret ve ulaşımdır. Ulaşım, ticaret ve yüksek teknoloji şirketlerinin verileri genelde dışardan gelen saldırılara maruz kalırken; finans, tıp ve eğitim alanındaki şirketler içerden saldırıya uğramaktadır. Bilgisayar korsanlarının kaynakları, koruma sistemleri çalışmayan veya etkili olmayan kontrol edilmeyen kanallardan oluşmaktadır (Marjanovic, 2017).

Yapılan araştırmalar kurumların bilgiyi sadece dış kaynaklardan koruması yeterli olmadığı ve içerden oluşan saldırıların arttığını göstermiştir. Bu sebeple erişim yönetiminin ve erişim kontrolünün şirket içinde önemli bir yeri olmalıdır.

3.4 Türkiye'de Bilgi Güvenliği ile İlgili Yasal Şartlar

Başbakanlık Genelgesi (2016/28) 3.12.2013 tarihinde yayınlanan resmî gazetede KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ de açıklandığı üzere; KamuNet ağına dahil olmak için asgari güvenlik gereksinimlerinden biri "KamuNet'e bağlantı yapacak birimlerini ve sistemlerini kapsayacak BGYS'nin kurması ve işletmesi" maddesi yer almaktadır. Bu sebeple KamuNet ağına bağlı olan tüm kamu kuruluşlarında için BGYS standardı kurulmuş ve uygulanmaktadır.

Elektronik Haberleşme Güvenliği Yönetmeliğinde; İşletmecilerin Yükümlülükleri kapsamında Elektronik haberleşme güvenliğini sağlama yükümlülüğü başlığında elektronik haberleşme şebekesi sağlayan ve altyapısını işleten sermaye şirket veya kurumların 20.07.2010 tarihinden itibaren belge alması zorunlu kılınmıştır. Yönetmelikte "İşletmeci, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğu sağlamakla yükümlüdür." maddesi yer almaktadır.

Gümrük İşlerini Kolaylaştırma Yönetmeliğinde yer alan Yetkili Yükümlü Sertifikası almak isteyen ithalat ve ihracatçıların ISO 27001 belgesi alması şartı istenmiştir. Gümrük ve Ticaret Bakanlığı'na bağlı Risk Yönetimi ve Kontrol Genel Müdürlüğünün Yetkili Yükümlü Sertifikası alacak firmalarda başvurularda aranacak belgeler arasında ISO 27001 BGYS Belgesi alma zorunluluğu vardır. Onuncu maddede "Avrupa Akreditasyon Birliğinin karşılıklı tanıma anlaşmalarına imza atmış akreditasyon kurumları tarafından akredite edilmiş uygunluk değerlendirme kuruluşlarınca düzenlenecek ve akreditasyon kurumunun markasını taşıyan, geçerli ISO 9001 ve ISO 27001 sertifikalarının aslı veya düzenleyen kuruluş tarafından onaylı örneği" yazısı geçmektedir.

Elektrik Piyasası Düzenleme Kurulu Elektrik Piyasası Lisans Yönetmeliği'ne göre TS ISO/IEC 27001 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alınması şartı; Enerji Piyasası Düzenleme Kurumu Lisans Yönetmeliklerinde değişiklik yaparak, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi'ni zorunlu hale getirmiştir. 26.12.2014 tarihli ve 29217 sayılı Resmî 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 gelmiştir

Maliye Bakanlığı Gelir İdaresi Başkanlığı E-fatura Özel Entegratörlük için başvuru yapan firmalara TS ISO/IEC 27001 Belgesi alınması şartı getirmiştir. Maliye Bakanlığı Gelir İdaresi Başkanlığı e-Fatura Uygulaması Kılavuzunda; "Özel entegratör bilgi güvenliği için TS ISO IEC 27001 veya ISO 27001 Belgesine sahip olmalıdır" ifadesi yer almıştır (Özeren & Güngör, 2017).

Yasal şartlara bakıldığında kurumsallaşmaya çalışan şirketler/firmaların Bilgi Güvenliği Yönetim Sistemi belgesi almaları önemlidir.

4. ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

4.1 ISO 27001 Standardı Tarihçesi

ISO/IEC 27000 standartlar serisinin tarihi, İngiltere Sanayi ve Ticaret Bakanlığı'nın Ticari Bilgisayar Güveliği Merkezine (TBGM) dayanmaktadır. Mayıs 1987'de kurulan TBGM'nin iki önemli amacı vardır. Birincisi; bilgi teknolojileri (BT) güvenlik ürünleri satıcılarına, uluslararası geçerliliği olan güvenlik değerlendirme kriterlerini belirlemek ve ilgili değerlendirme ve sertifikasyon planı hazırlamak ve bu sayede güvenlik ürünleri satıcılarına destek olmayı planlamaktadır.

İkinci amacı ise, başarılı güvenlik uygulamaları için kurallar yayınlayarak kullanıcılara yardım etmektir; bu amaçla 1989 yılında "Kullanıcılar için uygulama esasları" yayınlanmıştır. Esaslar Ulusal Bilgisayar kullanıcıları Birliği (UBB) tarafından geliştirilmiş ve daha sonra çoğunluğu İngiliz endüstrisinden gelen kullanıcılarla kurulan kullanıcı birliği konsorsiyum ile belirlenen esasların kullanıcı açısından anlamlı ve uygulanabilir hale gelmesi sağlanmıştır. Metnin son hali ilk defa İngiliz standartları kullanım kılavuzu PD 0003, bilgi güvenliği yönetiminin kullanım esasları olarak yayınlanmış ve son kullanıcı müzakerelerinin etkisi ile daha sonra İngiliz standartları BS7799:1995 olarak yayınlanmaya devam etmiştir. 1998 yılının şubat ayında ikinci kısım BS7799-2:1998 eklenerek daha sonra kapsamlı bir şekilde yeniden gözden geçirilme ve son kullanıcı müzakereleri ile yeni bir sürece geçilerek Kasım 1997 yılında başlayan bu sürecin ilk çıktısı Nisan 1999 yılında BS7799:1999 olarak yayınlanmıştır. Standartların ilk bölümü "Kısa Yol" mekanizması olarak Ekim 1999'da ISO standardı olarak teklif edildi ve küçük çaplı iyileştirmelerle ISO/ IEC 17799:2000 olarak 1 Aralık 2000 tarihinde basılmıştır. BS 7799-2:20002 ise resmi olarak 5 Eylül 2002 tarihinde yayınlanmıştır.

ISO standartlarının güncellenme sürecinin sonunda 15 Haziran 2005 tarihinde ISO/IEC 17799:2005 yeniden yayınlanmıştır. Yapılan en önemli değişiklik bu kontrol kılavuzunda gerçekleşmiştir. Gereklilikler, uygulama rehberi ve diğer bilgilerin farklılıkları gruplayarak net bir şekilde ayırt edilmiştir. Ayrıca yeni kontrollerin eklenmesi ve var olan kontrollerin daha iyi bir şekilde açıklanmasıyla daha kullanışlı hale getirilmiştir.

25 Eylül 2013'te ISO/IEC 27001'in ve ISO/IEC 27002'nin yeni versiyonu yayınlanmıştır. ISO/IEC 27001'in yeni versiyonu 2005 versiyonundan tamamen farklı olmuştur. Bunun sebebi ise bütün yönetim sistemleri standartları için yeni bir standart yapısı geliştirilmiş olmasıdır (GAMMASSL, 2019).

Türkiye'de bu durum, 11 Kasım 2002 tarihinde alınan karar ile Türk Standartları Enstitüsü tarafından TS ISO/IEC 17799 (Kısım-1) standardı tercümesi, İkinci kısım olarak geçen BS 7799 ise tercüme edilerek TS 17799-2 (Kısım-2) ismi ile resmi olarak kabul edilmiştir (Ganbat, 2013). 2 Mart 2006 ISO/IEC 27001:2005'in TSE tarafından kabul edilmiş, 1 Ekim 2013 tarihinde TS ISO/IEC 27001:2006 Bilgi Güvenliği Yönetim Sistemi belgelendirmesi revizyonu son versiyonu olarak son halini almıştır (TÜRKAK, 2019).

4.2 ISO 27001 Bilgi Güvenliği Standardının Dünya'daki Durumu

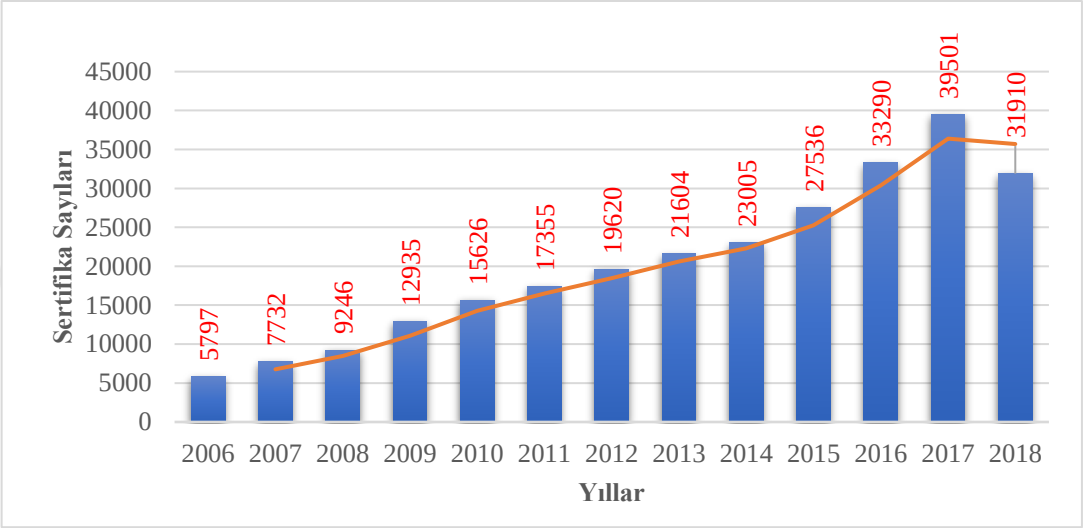
Bilgi güvenliği standardının Dünyada 'ki ve Türkiye'deki durumu başlığı altında hazırlanan grafiklerin oluşturulmasında Uluslararası Standartlar Örgütü tarafından yayınlanan yıllık araştırma raporundaki verilerden yararlanılmıştır (ISO, 2019a).

Oluşturulan grafikler şu sayıltılar çerçevesinde hazırlanmıştır:

- ✓ İlgili sektörlerin karşılaştırılmasında ülkelerin önemli seviyedeki bazı belgelendirme kuruluşları araştırmaya katılmamıştır.
- ✓ Bir ana kuruluş altında faaliyet gösteren alt gruplar tek bir ISO 27001 standardına sahip olduğundan aynı firmanın alt grupları için ankete dahil edilen veriler istatistiksel olarak belirli bir oranda araştırma bulgularından çıkarılmıştır.
- ✓ Grafiklerdeki bu sayısal değerler yalnızca ankete katılmış olan belgelendirme kuruluşlarının doğru kabul edilen görüş ve değerlendirmelerine göre belirlenmiştir.

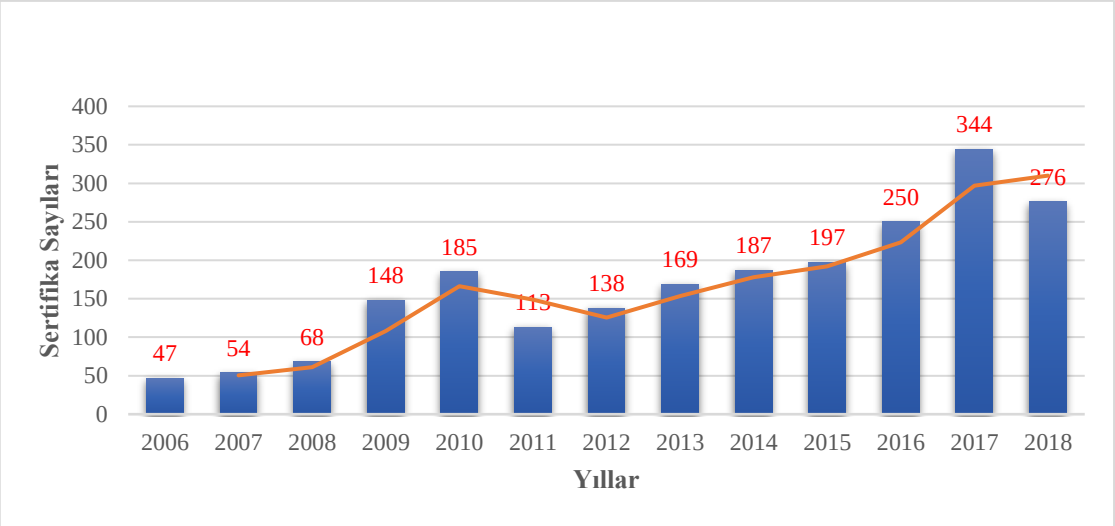
Bu yüzden ISO tarafından yapılan bu anket çalışmasının dünya geneli ISO 27001 belgesine sahip firmaların gerçek sayısını ortaya çıkarmada önemli bir çalışma olduğu, ankete katılan bu belgelendirme kuruluşlarının ankete vermiş oldukları cevapların doğruluğunun yukarıda ifade edilen sayıltılar etrafında değerlendirilmesi gerektiği, dolayısıyla dünya geneli yapılan bu anketin yalnızca bu varsayımlar etrafında doğru kabul edilebileceği göz önünde bulundurulmalıdır (ISO, 2019b).

International Organization for Standardization (2019) verilerine göre sektörlerin ISO 27001 BGYS belgelendirmelerini karşılaştırmak amacı ile Finansal Aracılık ve Emlak, Bilgi Teknolojileri, Eğitim, Sağlık ve Sosyal Hizmetler sektörlerinden oluşan ISO 27001 BGYS sertifika sayılarına ilişkin aşağıdaki grafikler oluşturulmuştur.



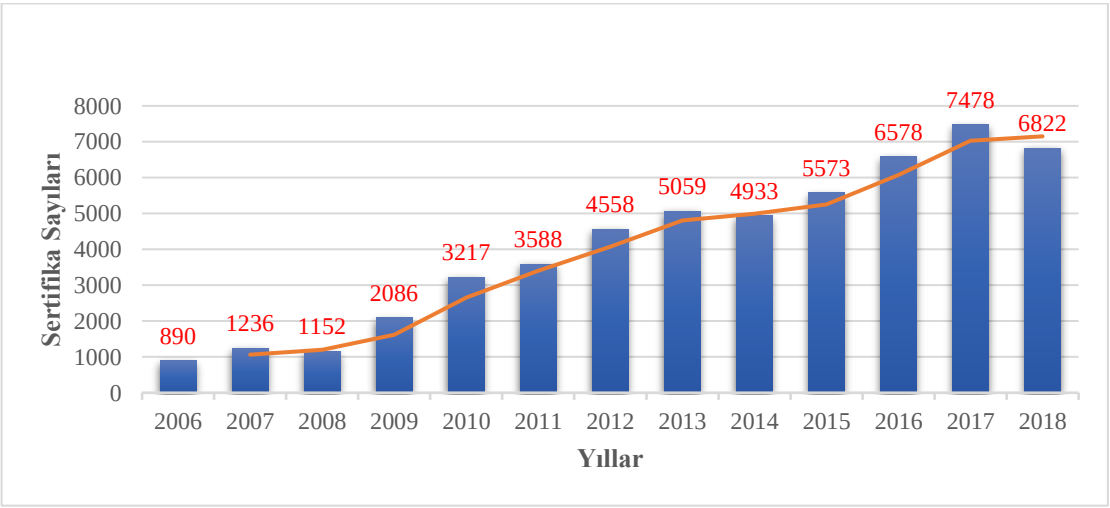
Şekil 4. 1 Yıllara Göre Dünya Genelinde Alınan ISO 27001 Bilgi Güvenliği Yönetim Sistemi Toplam Sertifika Sayısı

2006 ve 2018 yılları arasında yıllara göre dünya genelinde alınan ISO 27001 Bilgi Güvenliği Yönetim Sistemi toplam sertifika sayısı Şekil 4.1'de gösterilmiştir. Dünya'da ISO 27001 BGYS sertifika sayısı 2017 yılında 39501 adet iken, 2018 yılında 31910 dolaylarına azalış göstermiştir. Bu durum, sertifika alımından sonra geçerlik süresi sonunda sertifikaların yenilenmemesi halini veya belgeyi alan şirket ya da kurumların kapanmış olabileceği ihtimallerini düşündürmektedir.



Şekil 4. 2 Yıllara Göre Finansal Aracılık ve Emlak Sektörü Toplam Sertifika Sayıları

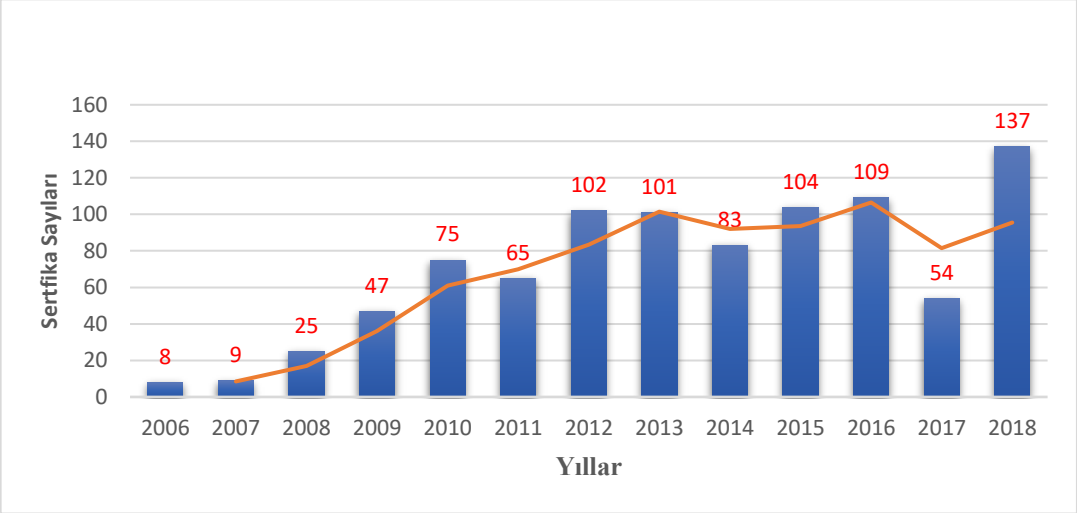
Yıllara göre finansal aracılık ve emlak sektörü toplam sertifika sayıları Şekil 4.2.'de gösterilmiştir. Sektörler arasında önemli bir yere sahip olan Finansal Aracılık ve Emlak sektörü en yüksek sertifika sayısına 344 sertifika ile 2017 yılında ulaşmıştır. Ayrıca 2017 yılı, kendinden önceki yıllara göre incelendiğinde sertifika sayılarındaki artış miktarları yönünden 94 sertifika sayısı ile en çok artış gösteren yıl durumundadır. 2018 yılında bu sayı düşüşe geçerek 276 sertifika sayısına gerilemiştir.



Şekil 4. 3 Yıllara Göre Bilgi Teknolojileri Sektörü Toplam Sertifika Sayıları

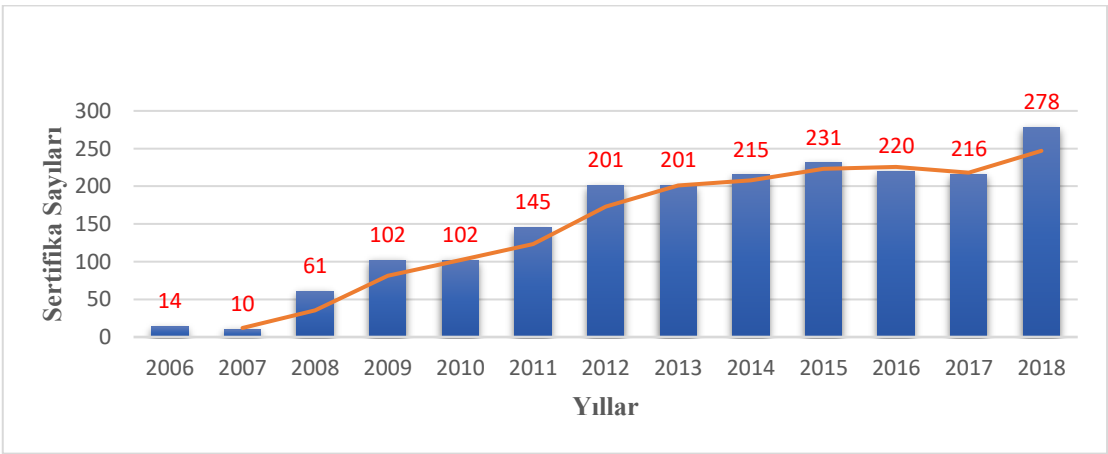
2006 ve 2018 yılları arası bilgi teknolojileri sektörü toplam sertifika sayıları Şekil 4.3'te gösterilmiştir. Bilgi teknolojileri sektöründe sertifika sayıları 2014 ve 2018 yılları

hariç genel olarak bir önceki yıla göre artış göstermiştir. 2017 yılında 7478 sayısı ile en yüksek değerine ulaşmıştır.



Şekil 4. 4 Yıllara Göre Eğitim Sektörü Toplam Sertifika Sayıları

Yıllara Göre Eğitim Sektörü Toplam Sertifika Sayıları Şekil 4.4'te gösterilmiştir. Eğitim sektöründe sertifika sayılarındaki artış en yüksek değeri 2018 yılında yakalayarak 137 sayısına ulaşmıştır. 2017 yılında bir önceki yıla nazaran yarı yarıya düşüşe geçtiği fakat 2018 yılında bu düşüşten meydana gelen açığın iki kat artışla kapatılmış olduğu görülmüştür.



Şekil 4. 5 Yıllara Göre Sağlık ve Sosyal Hizmetler Sektörü Toplam Sertifika Sayıları

2006 ve 2018 Yılları Arasında Sağlık ve Sosyal Hizmetler Sektörü Toplam Sertifika Sayıları Şekil 4.5'te gösterilmiştir. Sağlık ve sosyal hizmetler sektörü sertifika sayıları incelendiğinde; en çok sertifika sayısına 2018'de ulaşıldığı; aynı zamanda bir önceki yıla

göre en çok artışın 62 sertifika sayısı ile yine 2018 yılında gerçekleştiği görülmektedir. 2007, 2016 ve 2017 yıllarında sertifika sayılarının inişte olduğu gözlemlenmiştir.

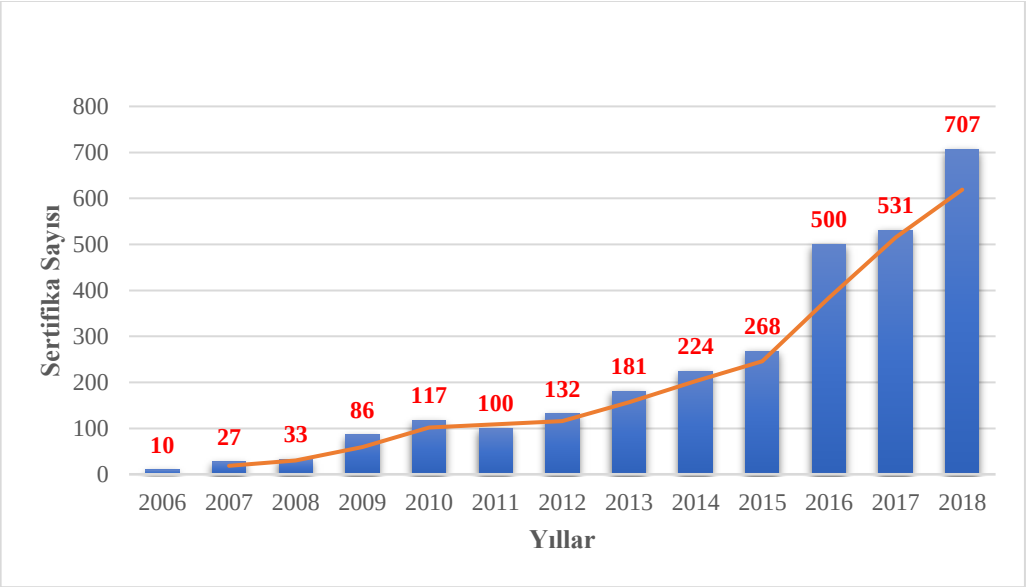
Dünya genelinde, bilgi güvenliği bağlamında sertifika dağılımlarının bölgesel olarak farklı kıtalar arasındaki genel durumu incelendiğinde ISO 27001 BGYS sertifika sayısının fazla olduğu bölgelerde satın alım gücü, ülke ekonomisi, para birimi ve ekonomik performansın Gayrisafi Yurt İçi Hasıla (GSYİH) ile ilişkili olduğu ortaya çıkmıştır. Ayrıca ülkenin refah düzeyi, teknoloji kullanımı, politik ve kültür yapılarının da etkili olduğu gözlemlenmiştir (Shojaie, 2018).

4.3 ISO 27001 Bilgi Güvenliği Standardının Türkiye'deki Durumu

2018 Yılı ISO 27001 BGYS Sertifikalandırma Sayıları ve Ülke Sıralaması Tablo 4.1'te gösterilmiştir. 2006 yılında Türkiye'nin sertifikalandırma sayıları sıralamasının 28 olduğu, 2008 yılında 24. sıraya yükseldiği bilinmektedir. Son on bir yılın (2006-2017) istatistiğine bakıldığında ise 2017 yılında 15 basamak birden yükselerek 13. sıraya geldiği görülmüştür (Yılmaz, 2018). 2018 yılında da bu sayı 11. sıraya yükselerek her geçen yıl ülkemizdeki sertifikalandırma sayılarında artışın olduğu ifade edilmektedir.

Tablo 4. 1 2018 Yılı ISO 27001 BGYS Sertifikalandırma Sayıları ve Ülke Sıralaması

S. No	**Ülke Adı**	**Sertifika Sayısı**
1	Çin	7.199
2	Japonya	5.093
3	Büyük Britanya ve Kuzey İrlanda Birleşik Krallığı	2.444
4	Hindistan	2.161
5	Almanya	1.057
6	İtalya	1.041
7	Amerika Birleşik Devletleri	911
8	Tayvan, Çin'in bölgesi	827
9	Hollanda	788
10	İspanya	726
11	**Türkiye**	**707**
12	Polonya	700
13	Romanya	585
14	Çek Cumhuriyeti	543
15	Macaristan	484



Şekil 4. 6 Yıllara Göre Türkiye'de ISO 27001 Bilgi Güvenliği Yönetim Sistemi Sertifika Sayısı

Yıllara göre Türkiye'de ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifika sayısı Şekil 4.6'da gösterilmiştir. Buna göre, 2006 yılında sahip olunan sertifika sayısı ülke genelinde sadece 10 iken, 2018 yılı sonunda sahip olunan sertifika sayısı 707 rakamına ulaşmıştır. Bu durum kurumların bilgiye verdikleri önemin arttığını ve sahip olunan bilgilerin korunmasının artık eskiye göre daha gerekli ve sistematik bir süreç olduğunu kavradıklarını göstermektedir. Bu sebeple son yıllarda sertifika alım sayısının arttığı söylenebilir. Bu artışın diğer sebebinin ise bölüm 3.4'te bahsedilen "Türkiye'de bilgi güvenliği ile ilgili yasal şartlar" başlığı altında belirtildiği üzere konu ile ilgili gerekli birçok hukuki düzenleme ve iyileştirmelerin yapılması ile birtakım yasal zorunlulukların artmış olması gösterilebilir.

4.4 ISO 27000 Standart Ailesi

- **ISO/IEC 27000 Bilgi güvenliği yönetim sistemleri- Genel bakış ve kelime bilgisi**

  BGYS'ye genel bir bakış sağlar. Ayrıca, BGYS standart ailesinde yaygın olarak kullanılan terimleri ve tanımları açıklar. Bu standartta sahip olmak isteyen büyük veya küçük fark etmeksizin tüm kuruluşlar uygulayabilir (ISO, 2019c).

- **ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi**

  Organizasyon bütününde kuruluşta BGYS oluşturulması, uygulanması, sürdürülmesi ve sürekli olarak daha iyileştirilmesi için gerekenlerin belirlenmesini sağlar. Kuruluş da oluşan ihtiyaçlara göre belirlenen bilgi güvenliği risklerinin değerlendirilmesi ve iyileştirilmesi için gereklilikleri sağlar (ISO, 2019d).

- **ISO/IEC 27002 Bilgi Güvenliği Teknikleri İçin Uygulama Kodu**

  Bilgi güvenliği kontrolleri için uygulama kodu olarak isimlendirilmiştir. ISO 27001 standardı içinde yer alan Ek-A'daki kontroller hakkında daha detaylı bilgi içerir. Bilgi güvenliği kontrol hedeflerinin uygulanması ve seçilmesinde kurumlara rehberlik sağlar.

- **ISO/IEC 27004 Bilgi Güvenliği Yönetimi Ölçüm Teknikleri**

  ISO / IEC 27004, bilgi güvenliği yönetimine ilişkin ölçümlerle ilgilidir: bunlar genellikle meslekte "güvenlik ölçümleri" olarak bilinir. Standart, kuruluşların BGYS'nin etkinliğini ölçmelerine, raporlamalarına ve sistematik olarak iyileştirmelerine yardımcı olmak amacıyla hazırlanmıştır. ISO / IEC 27001'de belirtildiği gibi uygulanan bir BGYS'nin ve kontrollerin veya kontrol gruplarının etkinliğini değerlendirmek için önlemlerin ve ölçümlerin geliştirilmesi ve kullanılması konusunda rehberlik eder (Şereflişan, 2016).

- **ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi**

  Bilgi güvenliği risk yönetimi olarak adlandırılmıştır. Standart, kuruluşun süreç odaklı bilgi güvenliği risk yönetimi için kılavuz bilgi sağlar (Şereflişan, 2016).

  ISO/IEC 27000 Standart ailesinin diğer kısımlarına Ek 2'de yer verilmiştir.

4.5 Bilgi Güvenliği Yönetim Sistemi (TS ISO/IEC 27001)

Çağımızın ekonomisi büyük ölçüde bilgiye dayanmaktadır. Büyük ölçekli iş yerleri ekonomik değişimi yakından takip etmek ve teknolojiye uyum sağlamak için rakiplerine karşı özgün ve daha fazla rekabetçi olmaya çalışmaktadır. Sürekli değişen teknoloji ile mevcut bilgilerin değişmesi ve geçerliliğini kaybetmesi durumu söz konusudur. Bu nedenle rekabeti artırarak öne geçmek isteyen firmalar yeni ve özgün bilgi kaynaklarını

çoğaltmak ve kısa zamanda büyük miktarda veriyi işleyip en etkin şekilde yönetmek durumundadırlar (Aktan & Vural, 2005). Kurumların hedefleri veri kaynaklarını etkin yönetmek ise var olan bilgi kaynaklarını ve oluşturacağı bilgi kaynaklarını güvence altına alması gerekmektedir ki rekabet gücünü artırabilsin; aksi takdirde işletmeler yeni ve özgün bilgi kaynaklarını artırırken var olan verilerin güvenliğini koruyamaz hale gelebilir ve yeni bilgilerin üretilmesine engel olabilir.

BGYS kurum ve kuruluşların önemli bilgilerini yönetmek ve güvence altına almak amacıyla geliştirilen bir sistemdir. Bilgi güvenliği yönetiminin bir sistem olarak ele alınması ve kurumsal ve toplumsal seviyede kurumların güvenliği açısından önem taşımaktadır.

Bilgi güvenliği yönetiminde amaç; olaylar henüz gerçekleşmeden önce öngörebilmek ve önleyici tedbirler almak, önlenemeyen bir durum söz konusu olduğunda ise, en az zarar ve en kısa süre ile normal iş sürecine yeniden dönebilmektir. Bu nedenle uygulamadaki en iyi süreçlerin belirlenerek bu süreçlerin yönetimi için kurumların uygulayabileceği bilgi, kültür ve yetkinliğe sahip olması gerekmektedir (İleri, 2016). BGYS sitemi, bilgi güvenlik yönetim sürecinin en etkin ve verimli şekilde nasıl uygulanması gerektiği ile ilgili kurumlara yol göstermektedir. Bunun yanında oluşabilecek saldırılara reaksiyon gösteren ve kendini yenileyebilen, geliştirebilen bir sistem hedeflenmektedir.

ISO 27001, kurumların kendilerine uygun politikalar, prosedür ve kılavuz oluşturmasına yön veren uluslararası kabul görmüş yapısal bir metodoloji sunar ayrıca ISO 27001 sertifikası kurumların güvenliğe önem verdiğini ve konuyu ciddiye aldığını gösterir (Özbilgin & Özlü, 2019).

Bilgi güvenliğine ilişkin yeterli önlemler alınmadığı takdirde bilgi kaynakları risk altında kalacak ve saldırı girişimlerine açık hale gelecektir. Kurumların faaliyetlerini güvenli bir şekilde sürdürebilmeleri için BGYS'yi uygulamaya geçirmek ve tüm iş süreçlerine entegre etmeleri gerekmektedir. Tüm kurumlar hedefleri düzeyinde güvenlik politikası oluşturmalı, yönetimsel olarak tüm kayıtlar tutulmalı; çalışanlarına, iş ortaklarına ve paydaşlarına aktarmalıdır.

BGYS; kurumların çalıştıkları sisteme kurulumu, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi aşamalarından oluşmaktadır.

4.6 BGYS'nin Kurulması, Uygulanması ve Yönetilmesi Sürecinin Aşamaları

BGYS'nin kurulması, uygulanması ve yönetilmesi sürecinin aşamalarının oluşturulmasında; alanyazında bulunan araştırmalar ve ISO 27001 bilgi güvenliği yönetim sistemi standardında yer alan maddelerden faydalanılmıştır. Bu bağlamda derlenen on bir aşama aşağıda özetlenmiştir.

Aşama 1: Üst Yönetimin Desteği

Üst yönetimin BGYS'nin uygulanmasında yapılması gerekli görev ve sorumlulukları içerir. Sistemin kurulması, işletilmesi, amaçlanan çıktıların gerçekleştirilmesi, sistemin kontrolleri ve onaylayıp yayınlanması için gerekli destekleri sağlar. Üst yönetim kurumun amacına uygun, bilgi güvenliği hedeflerini içeren ve sürekli iyileştirilmesi ile ilgili bilgi güvenliği politikası oluşturmalıdır. Yine üst yönetim BGYS'nin ISO 27001 standardına uygunluğunun kontrolünü sağlamak ve BGYS performanslarının yazılı hale getirilmesi için sorumluluklar yetkiler verebilir (TS ISO/IEC 27001: 2013).

Aşama 2: Bilgi Güvenliği Ekibinin Kurulması

BGYS'nin kurulumu için önemli adımlardan bir tanesi üst yönetimin desteğini alarak bilgi güvenliği komisyonu oluşturmaktır. BGYS'nin düzenlenmesi, uygulanması ve yönetilmesi çalışmalarını takip edecek bir ekip kurulmalıdır. Bu süreç içerisinde kurumun bilgi kaynaklarını kullanan ve görev alacak çalışanların rol ve sorumlulukları belirlenmelidir.

Kurum içindeki tüm birimlerden temsilci seçilerek katılım sağlaması faydalıdır ve başarı şansını arttırır. Aynı zamanda kurum içinde tüm çalışanların uygulamaya dahil edilmesi yönüyle bu yöntem etkili olmaktadır. Her birimden bir temsilcinin olması yönetim ve teknik kadro iletişimi kopukluklarının önüne geçer. BGYS'nin kurulumu, uygulanması işlemi daha çok bilgi teknolojileri birimlerini ilgilendirildiği ve görev tanımlarında olduğu düşünülmektedir fakat sanıldığının aksine pozisyon şartı aranmaksızın alt kademeden üst kademeye kadar tüm çalışanların katılımı ve desteği gereklidir. Kurum içindeki tüm personelin aktif katılımı sağlandığı takdirde istenen hedefe ulaşılması mümkündür (Önel & Dinçkan, 2007).

Aşama 3: Kapsamın Belirlenmesi

Kurumun BGYS'nin amaçlarına ulaşabilmesi için iç ve dış hususlar belirtilmelidir. Yani kapsamı ve sınırlarının belirlenmesi gereklidir. İlgili tarafların beklentileri ve bilgi güvenliği ile ilgili ihtiyaçların belirlenmesi gerekmektedir. Kapsam oluşturulurken kurum tarafından gerçekleştirilen faaliyet ve diğer kurumlar tarafından (müşteri ve tedarikçiler) gerçekleştirilen faaliyetler mutlaka kapsam içinde bulunmalıdır (TS ISO/IEC 27001: 2013). Kapsam belirlendikten sonra yayınlanarak üst yönetim tarafından onaylanmalıdır.

BGYS kurumun tamamını veya bir bölümünü kapsayabilir. Her durumda da kapsam eksiksiz ve doğru tanımlanmalıdır. BGYS dışında kalan varlıkların neden kapsam dışında kaldığı kurum tarafından açıklanabilir durumda olmalıdır (Marttin & Pehlivan, 2010).

Bu standart küçük veya büyük ölçekli tüm kurum tipleri için uygundur. Denetçiler ve belge veren kurum için ISO 27001 süreç maddelerinin 4 ila 10. maddeler arası hepsinin uygulanması gereklidir. Bir tanesinin bile uygulamaya alınmaması kabul edilemez. Kuruluşun bağlamı dahilinde BGYS'nin kurulması, uygulanması, sürdürülmesi ve belirli sürelerle iyileştirilmesini kapsar (TS ISO/IEC 27001: 2013).

Aşama 4: BGYS Yol Planının Oluşturulması

BGYS ekibinin kurulması, kurulumun kapsamı belirlenmesinin ardından BGYS sürecinin adımları belirlenerek bir yol planı oluşturularak kurum içi stratejinin belirlenmesi amaçlanmıştır. Bu süreçte kimlerin hangi görevler alarak ne zaman çalışmalara başlayacağı ve bitirme süreleri belirlenerek uygulama sürecine geçilmesi beklenmektedir. Yapılacak olan tüm çalışmalar dokümante edilerek kayıt altına alınmalı ve üst yönetime belirli aralıklarla bilgilendirme yapılmalıdır.

Aşama 5: Varlıkların Belirlenmesi

Varlık, işletme içinde değerli olan bu sebeple en uygun şekilde korunması gerekli öğelerdir. Varlık envanterinin düzgün hazırlanması, sahip olunan varlıkların değerleri ve önem dereceleri konusunda fikir verir. Tüm varlık envanterlerinin çıkarılması ve sınıflandırılması bilginin güvenli bir şekilde korunması ve risk analizlerinin yapılması hususunda önemli yer tutar (Koç, 2008).

Aşama 6: BGYS'nin Gerçekleştirilmesi ve Uygulama

Hazırlanan bilgi güvenliği süreçlerinin ve yol planlanın, etkin bir işletilmesi ve uygulanması kısmını kapsamaktadır. BGYS'nin sistemin işletimsel planlama ve kontrol, belirli aralıklarla bilgi güvenliği risk değerlendirme, bilgi güvenliği risk işleme planlarının uygulanması şartlarını içerir.

Bilgi sistemlerinde kullanılacak yasal düzenleyici, sözleşmeye bağlı gereksinimler, kurumsal yaklaşımlar net bir şekilde tanımlanmalıdır; bu ihtiyaçları karşılayacak şekilde kontroller, bireysel görevler tanımlanarak belgelendirilmelidir. (Şen & Yerlikaya, 2013). BGYS kurumun belirlenen kapsam dahilinde tüm sistemine uyum sağlayacak şekilde ayarlanmalıdır, doküman ve kayıt yönetimi bu çerçevede tamamlanmalıdır.

Politika ve prosedürlerin yazımı tek bir dosyadan oluşmamaktadır. Bilgi güvenliği, hazırlanırken başka dokümanlar, standartlar ve prosedürlerden destek alınarak hazırlanabilir. Kurumun standartta uygulaması gereken kanun, mevzuat, belirli kurallar ve destekleyici prosedürler referans kısmına eklenerek atıf yapılabilir.

BGYS'de dikkat edilmesi gereken başka bir husus ise bilgi güvenliği olay ihlali ve bu sürecin yönetimidir. Bilgi güvenliği ihlali; normal iş fonksiyonlarının tehlikede olmasıdır. Böyle bir durum ile karşılaşıldığında nasıl yönetilmesi gerektiği ile ilgili bir bilgi güvenliği ihlal yönetim süreci oluşturulmalı, görev ve sorumluluklar belirlenmelidir. Bilgi güvenliğini tehlikeye atacak durumun hızla kaldırılması ve sistemin tekrar güvenli bir ortamda yürütülmesi için gerekli çalışmalar tanımlanmalıdır.

BGYS'nin kaynak planlaması yapması ve ihtiyaç olduğunda planlanan kaynakların sağlanması gereklidir. Bilgi güvenliği kapsamında iş akışını etkileyen çalışan personellerin yeterliliklerinin belirlenerek görev verilen çalışanlar risk değerlendirme, bilgi güvenliği hedeflerinin yerine getirilmesi gibi sürekli iyileştirme çalışmaları yapmalıdır. Bilgi güvenliği farkındalığı oluşturulması için eksikler belirlenerek gerekli planlamaların yapılması gereklidir. Kurumun dahili ve harici iletişim ihtiyaçları tespit edilmelidir. Yazılı bilgilerin oluşturulması, güncelleme, kontrolü, saklanması ve yok edilmesi prosedürlere uygun şekilde yapılarak tüm yapılan işlemler kayıt altına alınmalıdır (Demirok, 2016).

Aşama 6.1: Risklerin Belirlenmesi, Analizi ve Yönetimi

BGYS kurulumu ve uygulanması sürecinde iş yeri bilgi güvenliğini riske atacak durumların nasıl yönetildiğine dair bir çerçeve belirlemelidir. Bir kurumda oluşabilecek veya var olan risklerin kontrolünü sağlamak, planlamak, risk işlemek ve riski değerlendirmek amacıyla planlanan faaliyetler olarak tanımlanır. Önleyici faaliyetler sunarak istenmeyen etkilerin azaltılması ve sürekli iyileştirme sürecinin başlatılmasıdır.

Risk, belirsizliğin yarattığı kurumun amaçları üzerinde oluşabilecek etkilerdir. Bu olasılığı minimuma indirmek için risk kabul kriterleri oluşturulur ve risk tespiti yapılır. Risk olasılıkları, seviyeleri ve sonuçlarının değerlendirilmesini kapsar. Risklerin analiz aşamasında ise riskler tespit edildikten sonra organizasyonlar üzerindeki etkisi gözlemlenerek oluşacak olası zararları önlemek amacı ile kurum yapısı korunarak risk seviyeleri belirlenir yani risklerin önlem alınması gerekli sıralaması oluşturularak öncelikleri değerlendirmeye alınır. Bu değerlendirmeye uygun bir strateji belirlenir. Bir sonraki adımda bilgi güvenliği risk işleme süreci tanımlanarak planlanmalı ve uygulanmalıdır. Son olarak riskler her zaman sabit olmayabilir varlıklar, olaylar ve olayların etkileri hızla değişebilmektedir. Bu sebeple değişen etkilerin doğurabileceği riskleri çabuk gözlemlemek adına süreç sürekli olarak gözden geçirilmelidir (TS ISO/IEC 27001: 2013).

Aşama 7: Uygulanabilirlik Bildirgesi

Standartta seçilmiş kontroller ve bu kontrollerin neden seçildiği, mevcut gerçekleştirilen kontroller ve amaçları, Ek-A'da belirtilen kontrol amaçlarının hangisinin kapsam içinde hangisinin kapsam dışında kaldığı bilgileri, kapsam dışı kalma nedenleri uygulanabilirlik bildirisinde yer alır (Çetinkaya Kılıç & Gökçöl, 2010).

Aşama 8: İç Denetim

İç denetim kurumun içinden veya dışından kurum adına yapılır. Belirli aralıklarla hedeflenen BGYS prosedürlerde tanımlanan gereksinimlere uygunluğunun denetimidir. Objektif ve tarafsız bir şekilde tetkik süreci yürütülmelidir. Aynı zamanda bu iç denetimler iyileştirme çalışmalarına da katkı sağlaması açısından kayıt tutulmasında fayda vardır. Bu durum BGYS standardının kurum içinde uygulanabilirliği ve sürdürülmesi sürecini kapsar.

Aşama 9: Yönetimin Gözden Geçirmesi

Değişen teknolojinin etkisi, kurumun sürecin uygunluğu, yeterliliği ve sistemin verimliliği için sürekli bir iyileştirme sürecinde olmalıdır. Bu aşama BGYS performans etkinliğinin değerlendirildiği bölümdür. BGYS sürecinde bir uygunsuzluk çıktığında, bu durumun düzeltilmesi, uygunsuzluk nedenlerinin belirlenerek çözümü için düzeltici faaliyetlerin yapılması, gerekli kontrollerin sağlanması ve tekrar oluşmaması için önlem alınması gereklidir. BGYS iç denetiminde belirlenen uygunsuzluklar sonucunda düzeltici faaliyet uygulaması yapılır. Düzeltici faaliyet uygulamaları bilgi güvenliği kurulu başkanı tarafından takip edilir ve izlenir. Uygulama etkinlikleri yönetimin BGYS sistemini gözden geçirme toplantılarında değerlendirilir.

Üst yönetim tarafından gözden geçirme süreci belirlenerek düzenli ve planlı aralıklarla mevcut durum, iyileştirmeler ile ilgili kararlar verilmelidir. (TS ISO/IEC 27001: 2013).

Aşama 10: Belgelendirme

Dış denetim, akreditasyon sağlayan bir firma tarafından gelen görevlilerin kurumun BGYS için uygunluğunun denetiminin yapılması işlemidir. Bu aşama belgelendirme kuruluşuna müracaat edilerek başlatılır ve yetkili kişiler tarafından işlemler gerçekleştirilir. Denetim sonrası eksiklikler belirlenir ve tamamlanma sürecine gidilir.

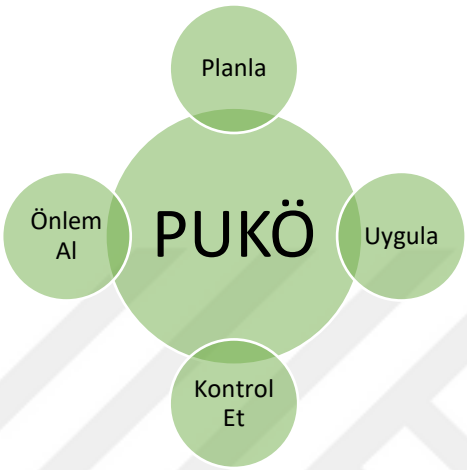
Dış denetimi ve dokümantasyon evrakları tamamlandıktan sonra belgelendirme işlemi yetkili firma tarafından gerçekleştirilir. Denetimin sonucu başarılı olduğunda BGYS tescili yapılarak akreditasyon kuruluşu ve belgelendirme kuruluşunun damgası ile onaylanan bir belge verilir. Belgelendirme işlemi yapan kurum ISO/IEC 27001 standardında belirlenen süreçleri karşıladığı, tamamladığı ve işletildiğini kanıtlamış olacaktır.

Aşama 11: Eğitim ve Farkındalık Çalışmaları

Kurum personelinin çalışma düzeni alışkanlıklarından vazgeçmesi zaman alacaktır. Bu sebeple bu değişimi sağlıklı şekilde yapmanın yolu BGYS'nin kurum kültürüne nüfuz etmesini sağlamaktır. Kurum içi tüm personele yönelik 27001 bilinçlendirme eğitimi alınmasında fayda vardır. Uygulanma sürecinde sistemin öneminin ve faydasının kavranması açısından eğitim farkındalık katacaktır.

4.7 PUKÖ Modeli

BGYS'nin oluşturulmasındaki adımları 4 ana başlıkta inceleyerek PUKÖ modeli oluşturulmuştur. Sistemin başından sonuna kadar olan süreci özet olarak tanımlamaktadır. PUKÖ Modeli Şekil 4.7'de gösterilmiştir.



Şekil 4. 7 PUKÖ Modeli

BGYS'de benimsenen PUKÖ modeli maddeleri:

Planla: BGYS hedefine ulaşmak için gerekli planların hazırlanması, BGYS'nin kurulmasının planını kapsar.

Uygula: Politika ve prosedürlere uygun hazırlanan planın uygulanması ve işletilmesi aşamasıdır.

Kontrol Et: BGYS performans etkinliğinin gözden geçirildiği, denetim işlemlerinin yapıldığı değerlendirme sürecidir.

Önlem Al: BGYS'nin devamlılığı ve iyileştirilmesi sürecinde düzeltme ve önlem alma faaliyetlerinin gerçekleştirilmesidir.

4.8 Bilgi Güvenliği Yönetim Sisteminin Faydaları

BGYS bilgi varlıklarını korumak, bilgilerin güvenli işletilmesi için ilgili taraflara güven vermek ve yeterli güvenlik kontrollerini sağlamak için tasarlanmıştır. Bu çerçevede firmaların veya kurumların tercih ettiği bir sistem olarak karşımıza çıkmaktadır. BGYS'nin kurumlara sağladığı faydalar aşağıda maddeler halinde verilmiştir:

- Bilgi güvenliği çalışmalarını ve hedefleri belirlenerek; BGYS'nin planlanması, uygulanması, kontrol edilmesi ve sistemin devamlı iyileştirilmesini sağlar,
- Devam eden çalışmaların mevzuat, sözleşme, standart ve iş gereksinimlerinin karşılıklarını ifade eder,
- Kişisel Verilerin Korunması Kanunu (KVKK) ihtiyaçlarının karşılıklarını tanımlar,
- Mevcut alınan diğer yönetim sistemleri ile beraber BGYS çalışmalarını tümleşik olarak yürütür,
- BGYS kapsamında ihtiyaç olan kaynakları, görevleri rol ve sorumlulukları tanımlar,
- Gizlilik, bütünlük, erişilebilirlik ölçütlerinin belirlenmesini sağlar ve bilgi varlıklarının listesini çıkarır,
- Bilgi güvenliğini yönetmek için var olan ve oluşabilecek riskleri belirler, değerlendirir ve uygun olan risk işleme prosedürünü yürütür,
- İş devamlılığı planları oluşturur, oluşturulan planların uygulanmasını, sürekliliğini ve iyileştirilmesini sağlar,
- Bilgi güvenliği hususunda değişen teknolojiyi, yenilikleri takip eder ve çözüm bulur,
- Bilgi güvenliği konusunda belirlenen konulara uyulması için bütün paydaşların gerekli tedbirleri almasını sağlar,
- BGYS politikasının duyurulması, erişilir sağlanmasını, bu konuda farkındalık yaratılmasını ve uygulanmasını sağlar,
- BGYS politikasına uyulmaması durumunda gerekli işlemleri başlatarak takibini yapar (TÜBİTAK, 2019).

5. ISO 27001 VE ERİŞİM KONTROLÜ PROTOKOLÜ POLİTİKASI VE KONTROL MADDELERİ

Erişim kontrolü protokolü politikası ve kontrol maddelerinin açıklanmasında (TS ISO/IEC 27002: 2013) bilgi güvenliği teknikleri için uygulama kodu kaynağı temel alınmış ve ilgili alanyazın çalışmaları derlenerek aşağıda özetlenmiştir. Standartta yer alan erişim kontrol politikası kontrol maddelerinin takibi kolaylaştırılması açısından, başlıkların yanında ISO 27002 standart maddesine karşılık gelen ilgili bölüm numarası parantez içinde verilmiştir.

5.1 Erişim Kontrolü Politikası (ISO 27002- Bölüm A.9)

Erişim kontrolü, yetkisi olamayan kullanıcıların bilgiye erişimini engellerken, yetkisi olan kullanıcılara kontrollü ve kayıt altına alınarak hizmet kullanım hakkı verilmesidir.

Yaşanılan problemlerin başında erişim hakkı olmayan yetkisiz kişilerin sisteme izinsiz erişimin sağlanması ve fazla yetkilendirme işlemlerinin dikkatsizliği sonucunda gerçekleşmektedir. Bu sebeple firmaların bilgi güvenliği açısından erişim kontrolü önemli bir faktördür. Nitekim ISO 27001 BGYS içinde yer alan erişim politikası içinde detaylandırılan erişim yönetimine 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) içerisinde de yer verilmiştir. Kanun, kişisel verilere yetkisiz kişilerce erişilmesi, bilgilerin çalınması, verilerin kötüye kullanımı gibi olumsuz vakaları önlemek amacıyla gerekli tedbirleri almıştır.

6698 sayılı Kişisel Verilerin Korunması Kanununda Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) kısmında yer alan, kurum ve kuruluşların veri sorumluları tarafından alınabilecek teknik tedbirler özet bir tabloda gösterilmiştir. Bunlar; Yetki Matrisi, Yetki Kontrol, Erişim Logları, Kullanıcı Hesap Yönetimi olmak üzere ilk dört madde içerisinde yerini almıştır (KVKK, 2019).

Kullanıcıların erişim kontrolünün nasıl gerçekleştireceğini düzenlemek için sistemlere erişim kontrol süreci oluşturulmalıdır. Alt düzeyde çalışan kullanıcıdan üst düzeyde çalışan kullanıcıya kadar tüm sisteme erişim işlemleri planlanmalı, erişim kontrolleri prosedür haline getirilerek dokümante edilmeli ve uygulaması yapılmalıdır. Bu protokolde gerektiği kadar ya da “en az bilme” güvenlik prensibine dayanmalıdır.

Açıkça erişim hakkı tanınmadığı sürece her şey yasak olmalıdır. Firma çalışanları sisteme güvenli bir erişim kontrolü sağladığında saklanan veya işlenen bilginin gizliliği, bütünlüğü ve erişilebilirliği sağlanmış olur.

Erişim politikası 4 tane alt madde ve 14 tane kontrol maddesinden oluşmaktadır. Aşağıda bu alt madde ve kontrol maddeleri kısaca anlatılmıştır.

5.2 Erişim Kontrolünün İş Gereklilikleri (ISO 27002- Bölüm A.9.1)

Bu bölümde bilgi ve bilgiyi işleme sistemlerine erişimlerin sınırlandırılması hedeflenmektedir.

5.2.1 Erişim Kontrol Politikası (ISO 27002- Bölüm A.9.1.1)

Bilgi ve iş güvenliği ihtiyaçları temelinde bir erişim politikası hazırlamak için takip edilebilirliğini sağlamak üzere yazılı hale getirilmeli, düzenli olarak takip edilmeli ve gözden geçirilmelidir. Bir erişim mantıksal ve fiziksel olabilir. Burada her iki durum da önemlidir.

Fiziksel güvenlik açısından erişim kontrolü; şirket binası girişleri ve odaların girişlerine sadece yetkili kişilerin kullanım sağlaması, yetkisiz kişilerin giriş izinlerinin olmamasıdır. Fiziksel erişim insan faktörü olarak erişim kontrolünde güvenlik görevlileri veya kapıcı vb. olabilir. Mekanik erişimlerde kilit, anahtar vb. kullanılabilir. Teknolojik güvenli giriş kontrolleri sağlamak için ise kişisel giriş kartları, parmak izi kullanılabilir. Bilgi ve bilgi sistemlerinin erişim kontrolünde; kimlik doğrulama (authentication) izlenebilirlik (accountability) ve yetkilendirme (authorization) işlemlerini kapsamaktadır (Dinçer, 2007).

Erişim yetkilendirmesi yapılması için erişim kontrol rollerinin belirlenmesi gerekmektedir. Belirlenen erişim yetkilerinin belirli aralıklarla gözden geçirilmelidir. Ayrıca yapılan tüm işlemler yönetim tarafından kayıt altında tutulmalıdır.

5.2.2 Ağlara ve Ağ Hizmetlerine Erişim (ISO 27002- Bölüm A.9.1.2)

Ağ hizmetlerinde oluşabilecek sorunların önüne geçmek için yetkilendirme süreci başlatılarak, şirket çalışanlarının hangi ağa ve ağ servislerine erişim sağlayacağı önceden belirlenmeli ve bir yetkilendirme prosedürü oluşturulmalıdır. Bu sürecin tüm adımları kullanıcılar ve yöneticiler tarafından bilinmelidir. Burada amaç yetkisi olamayan kişilerin

veya kullanıcıların ağ servislerinin kullanımını önleyerek ağ güvenliğinde oluşabilecek riskler için tedbir almaktır.

Güvenli bir ağ ve ağ hizmetlerine erişim oluşturmak için yönetim tarafından ağ ve ağ hizmetlerine erişim için hangi yöntemlerin kullanılacağı oluşturulmalıdır. Ağ hizmetlerine erişimin sağlanması için kimlik doğrulama prosedürleri belirlenmeli ve kullanıcıları sadece kendileri için belirlenmiş olduğu ağ ve ağ hizmetlerine erişimleri sağlanmalıdır. Yetkili kişilerce ağ kullanımının kayıt altına alınması, kontrol edilmesi ve takip edilmesi gereklidir.

5.3 Kullanıcı Erişim Yönetimi (ISO 27002- Bölüm A.9.2)

Yetkili kullanıcılara sistem ve hizmetlerin erişim hakkının tanınması, yetkisiz erişimin engellenmesini sağlar.

5.3.1 Kullanıcı Kaydetme ve Silme (ISO 27002- Bölüm A.9.2.1)

Kullanıcı kimlikleri yönetim tarafından kullanıcıların iş ve görev tanımlarına uygun verilmektedir. Kullanıcıların erişim hakları her zaman sabit kalmayarak iş ve işlemlere göre dönemsel değişiklik gösterebilmektedir. Yönetim tarafından kullanıcı erişim haklarının düzenlenmesi için resmi bir kullanıcı kayıt etme ve silme süreci oluşturmalıdır.

Kullanıcı kimlikleri yalnız bir kişiye özel olmalı ve benzeri olmamalıdır, mutlaka onaylanmalı ve kayıt altına alınmalıdır. Kullanımına yalnızca iş ve işletimsel sebepler gerektiğinde izin verilmelidir. Ayrıca şirketten ayrılması söz konusu kullanıcıların kimliklerinin ivedilikle kaldırılması veya engellenmesi gerekmektedir. Gereksiz kullanıcı kimliklerinin olması durumunda tespit edilerek başka kullanıcılar tarafından kullanılmadığının kontrolü yapılarak, kaldırılması veya engellenmesi süreci oluşturulup, belirli aralıklarla kontrolü sağlanmalıdır.

5.3.2 Kullanıcı Erişimine İzin Verme (ISO 27002- Bölüm A.9.2.2)

Tüm kullanıcı türleri için, sistemlerin ve hizmetlerin tümüne erişim hakkının verilmesi ve iptalinin sağlanması süreci oluşturularak resmi bir kullanıcı erişim izin işlemleri ile yürütülmelidir. Bu süreçte erişim haklarının yönetilmesinde kullanıcının bilgi sistemlerine erişimi; bilgi sistemi ve hizmet sağlayıcı tarafından yetki verilmesi ile beraber yönetimin de ayrıca bir onay vermesi uygun olabilir. Ayrıca servis sağlayıcıları tarafından yetkilendirme süreci henüz tamamlanmadan erişim haklarının aktif olmadığının kontrolü sağlanmalıdır.

Erişim hakları ve taleplerinin kontrolü, verilen özel haklardan daha çok roller çerçevesinde daha kolay yapılmaktadır. Kullanıcının sağladığı erişim seviyesinin kapsamı erişim politikalarına uygun olmalı, erişim hakları ile görevlerinin gereksinimleri ile tutarlı olmalı ve diğer gereksinimlerle örtüşmelidir. Kullanıcı kimliklerine verilen erişim haklarının kaydı merkezi olarak tutulmalı ve erişim hakları düzenli olarak gözden geçirilmelidir.

5.3.3 Ayrıcalıklı Erişim Haklarının Yönetimi (ISO 27002- Bölüm A.9.2.3)

Ayrıcalıklı erişim haklarının amacı, kullanıcılara verilen ayrıcalıklı erişim haklarının kendisine verilen ayrıcalıklı iş için kullanıp kullanmadığının kontrolünü sağlamak ve bu süreçteki yapılan işlerin güvenliği için kayıt altına alınmasıdır. Yapılacak tüm işlem ya da işler ile ilişkili ayrıcalıklı erişim hakkının hangi kullanıcıya sağlanacağı belirlenmelidir ve yetkilendirme süreci bitmeden işlemler devam ettiği süre içerisinde ayrıcalıklı erişim haklarının kullanımına izin verilmemelidir. Sağlanan bu hak sadece kullanımın gerekli olduğu koşullarda kullanıcılara tahsis edilmeli örneğin standart bir kullanıcı için asgari erişim sağlanmalıdır.

Ayrıcalıklı erişim hakları, çalışanların yürütmekte olduğu görevleri için kullandığı kullanıcı kimliğine tanımlanmamalı farklı bir kullanıcı kimliğine tahsis edilmelidir ve sahip olduğu ayrıcalıklı kullanıcı kimliğini düzenli yaptığı işlemler için kullanmamalıdır. Tanımlanan ayrıcalıklı erişim haklarına sahip kullanıcılar, söz konusu kendilerine tanımlanan ayrıcalıklı işler ile doğrudan ilişkili olup olmadığının kontrolü sağlanmalıdır. Ayrıcalıklı erişim haklarının kullanıcılara verilmesi ve kullanımı, sınırlandırılmalı ve kontrol edilmelidir. Tüm yetkilendirme işlemi ve tüm ayrıcalıklı haklara sahip kullanıcılar kayıt altında tutulmalıdır. Ayrıcalıklı erişim haklarının sonlandırılması için gerekçeler belirlenmelidir.

Genel yönetici, kullanıcı kimliklerinin başkası tarafından izinsiz kullanımını önüne geçmek için bir yöntem oluşturmalı ve uygulanmalıdır. Genel yönetici tarafından gizli kimlik doğrulama bilgileri paylaşıldığında bunun önemle saklanması gerekmektedir.

Ayrıcalıklı sistem yöneticisi haklarına sahip olan kullanıcının dikkatsiz kullanımı sistemlere zarar vermesine neden olabilir bu durum büyük bir hataya yol açabilir. Bu sebeple dikkat edilmelidir.

5.3.4 Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi (ISO 27002- Bölüm A.9.2.4)

Gizli kimlik doğrulama bilgilerinin kullanıcılara tahsis edilmesi bir süreç oluşturularak resmi hale getirilmeli ve kontrol edilmelidir.

Yönetim vermiş olduğu gizli kimlik doğrulama bilgilerini kullanıcılara onaylatmalıdır. Kullanıcıların kimliklerini doğrulama işlemleri yapıldıktan sonra geçici gizli kimlik doğrulama bilgileri kullanıcılara güvenli bir şekilde verilmelidir, dış tarafların veya korumasız (açık metin) elektronik posta mesajlarının kullanımından kaçınılmalıdır. Geçici gizli kimlik doğrulama bilgileri tahmin edilmez olmalı, eşi ve benzeri olmamalıdır. Kullanıcılara başlangıçta ilk kullanım için verilen geçici gizli kimlik doğrulama bilgilerini daha sonra değiştirmelidir.

En yaygın kullanılan gizli kimlik doğrulama bilgilerinden olan parola, kullanıcı kimliğini doğrulamasının ortak bir aracıdır. Başka gizli kimlik doğrulama kodları üreten cihazlarda (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) vardır.

Kullanıcıların kendilerine ait gizli kimlik doğrulama bilgilerinin saklanması ve gruba ait gizli kimlik doğrulama bilgisini sadece grup üyelerince bilinmesi hususu bir taahhütte dayandırılmalıdır örneğin bu taahhütname iş akdi şartlarında olabilir.

5.3.5 Kullanıcı Erişim Haklarının Gözden Geçirilmesi (ISO 27002- Bölüm A.9.2.5)

İş sürecinde çalışanların pozisyonları değişebilmekte veya pozisyonları aynı kalarak verilen işlere göre erişim hakları farklılaşabilmektedir. Tüm bunların güvenli olarak yürütülmesi için bir kontrol süreci olmalıdır. Burada amaç varlık sahiplerinin, kullanıcıların bilgiye sağlanan erişim haklarını belirli periyotlarla kontrolünü sağlamasıdır. Yani şirket içinde bir iş rolünden başka bir iş rolüne geçerken, bulunduğu pozisyondan daha alt bir pozisyona veya üst bir pozisyona geçiş veya iş akdinin feshi durumlarında kullanıcı erişim hakları kontrol edilerek yeniden düzenlenmeli ve bu süreç belirli periyotlarla gözden geçirilmelidir.

Ayrıcalıklı erişim hakları için verilen yetkilendirmeler ve ayrıcalıklı hesapların değişimi bir süreç haline getirilerek daha sık aralıklarla gözden geçirilmelidir, yetkisi olamayan ayrıcalıklı haklara sahip kullanıcıların olup olmadığını tespit etmek için kullanıcılara verilen ayrıcalıklı haklar düzenli kontrol edilmelidir.

5.3.6 Erişim Haklarının Kaldırılması veya Düzenlenmesi (ISO 27002- Bölüm A.9.2.6)

Dış kaynak kullanıcılarda dahil olmak üzere tüm kullanıcıların bilgi ve bilgiyi işleme yetkilerine sahip erişim hakları; iş sözleşmesinin veya anlaşmasının sona ermesiyle kaldırılmalı, istihdamın ya da sözleşmenin değişmesi durumunda ise düzenlenmelidir.

İş akdinin sonlanması ile bilgi ve bilgiyi işleme hizmetleri ile ilgili ayrılan kişinin varlıklara erişim hakkı askıya alınmalı veya kaldırılmalı. Askıya alınma durumu erişim haklarını kaldırıp kaldırmamanın gerekliliğini belirler. İstihdamı onaylanmamış tüm erişim hakları kaldırılmalı ve bu durum istihdam değişikliklerini kapsamalıdır. Kaldırılma ya da düzenlenme işlemi; bilgi işleme olanaklarının veya aboneliklerinin kaldırılması, kimlik kartlarının iptal edilmesi ya da değiştirilmesi ile yapılabilir. Erişim haklarının kaldırılmasını ya da ayarlanması bilgileri, çalışanların ve yüklenicilerin erişim haklarının ne olduğunu belirleyen doküman da bulunmalıdır. Düzenlenecek veya kaldırılacak erişim hakları fiziksel ve mantıksal erişim haklarını da kapsamalıdır. Aktif olan kullanıcı kimliklerini işten ayrılan biri veya dış taraf kullanıcısı, kullanıcı kimliklerinin parolası biliyorlarsa; istihdamın, anlaşmanın feshi veya iş sözleşmesinin değişimi söz konusu olduğunda bu parolalar değiştirilmelidir.

Bilgi varlıklarına erişim haklarında oluşabilecek risklerin azaltılması ve kaldırılması, değerlendirilmesi ile ilişkili iş akdinin sonlanması veya iş değişikliklerinde;

- Kullanıcı erişim haklarının değişikliği ve sonlandırılması yönetim, çalışan veya dış taraf kullanıcısı tarafından başlatılıp başlatılmadığı ve sonlandırma nedeni,
- Tüm çalışanların veya dış taraf kullanıcıların var olan sorumlulukları,
- Mevcut erişilebilir varlıkların değeri belirtilmelidir.

Dikkat edilmesi gereken diğer hususlar ise şunlardır:

Grup kimlikleri için kullanılan erişim haklarını işten ayrılan ve dış taraf kullanıcıları ve daha fazla kişiye verilmiş olma durumunda işten ayrılan kişilerin erişim hakları kaldırılarak erişim listesinden silinmelidir. Ayrılan personel ile bu bilgilerin paylaşılmaması için tüm çalışanlara öneride bulunulmalıdır.

Yönetimin işi sonlandırılmasından memnun kalmayan çalışan veya dış taraf kullanıcısı bilgi sistemlerine bilinçli ve kasıtlı olarak bozup zarara yol açmak isteyebilir.

İşten ayrılan veya istifa eden çalışan ilerde kullanmak üzere bilgi toplamaya devam etmek isteyebilir. Bu durumlar göz önünde bulundurularak hareket edilmelidir.

5.4 Kullanıcı Sorumlulukları (ISO 27002- Bölüm A.9.3)

Kullanıcılar sahip olduğu kişisel kimlik doğrulama bilgilerinin emniyetinden sorumlu tutulur.

5.4.1. Gizli Kimlik Doğrulama Bilgisinin Kullanımı (ISO 27002- Bölüm A.9.3.1)

Gizli kimlik doğrulama bilgisinin kullanımında kurumsal kuralları uygulamaları kullanıcılar için zorunlu tutulmalıdır.

Uygulama kılavuzu tüm kullanıcılar için aşağıdaki hususları tavsiye etmelidir; yöneticiler dahil tüm çalışanlar gizli kimlik doğrulama bilgilerini gizli tutulmalıdır ve diğer taraflara bilgileri açıklamamalıdır. Gizli kimlik doğrulama bilgilerinin başkaları tarafından öğrenilmesi, bilinmesi ile ilgili durum söz konusu olduğunda değiştirilmesi gereklidir.

Parolalar gizli kimlik doğrulama bilgisi olarak kullanılması durumunda nitelikli ve güvenli oluşturulmasında şu hususlara dikkat edilmelidir; kolay hatırlanabilir ve kolay tahmin edilebilir olmamalı, parola sahibinin kişisel bilgileri olmamalıdır (adı soyadı, cep telefonu, doğum yılı gibi). Sözlük saldırılarına karşı korumalı olmalı yani sözlüklerde yer alan kelimeleri içermemelidir. Parolanın tamamı alfabetik karakterlerden oluşmamalı veya tamamı sayısal olmamalıdır. Geçici olarak tanımlanan bir parola ise ilk oturum açıldığında değiştirilmelidir.

Bireysel kullanıcılar gizli kimlik doğrulama bilgilerini hiç kimse ile paylaşılmamalıdır. Otomatik olarak ayarlanmış oturum açma işlemlerinde parolalar gizli kimlik doğrulama bilgisi olarak kullanıldığında güvenli bir koruma ile kayıt altına alınmalıdır. İş için kullanılan gizli kimlik doğrulama bilgileri ile iş dışı amaçlar için kullanılan gizli kimlik doğrulama bilgileri aynı olmamalıdır.

5.5 Sistem ve Uygulama Erişim Kontrolü (ISO 27002- Bölüm A.9.4)

Erişim izni olmayan kişilerin sisteme ve uygulamalara erişiminin kısıtlanması ile ilgili ilkeler bu madde de anlatılır.

5.5.1 Bilgiye Erişimin Kısıtlanması (ISO 27002- Bölüm A.9.4.1)

Bilgi, sistem ve uygulamalarına erişim, erişim kontrol politikasına uygun prosedürde sınırlandırılmalıdır.

Erişim kısıtlamaları kullanıcıların iş faaliyetlerini kapsamalı ve tanımlanan erişim kontrol politikasına uyum sağlamalıdır. Erişim sınırlandırmalarını desteklemek amacıyla şu bilgilerin dikkate alınmasında fayda vardır; bilgi sistemlerine belirli kullanıcıların eriştiğinin kontrolünün sağlanmalıdır. Kullanıcıların hangi erişim haklara sahip olduğunun kontrolü sağlanmalıdır (okuma, yazma, silme ve yürütme). Başka programlara erişim haklarının kontrolü sağlanmalı, gerektiğinde kısıtlanmalıdır. Hassas verilerin konurumu için, sistem ve uygulama verilerinin fiziksel ya da mantıksal erişim kontrolleri yapılmalıdır.

5.5.2 Güvenli Oturum Açma Prosedürleri (ISO 27002- Bölüm A.9.4.2)

Erişim kontrol politikasının kullanımının zorunlu tutulduğu yerde; sistem ve uygulamalara erişimin güvenli olması için oturum açma prosedürü oluşturulmalı ve bu süreç tarafından güvenli oturum açılımı kontrol edilmelidir.

Kullanıcının doğru olduğunu ileri sürdüğü kimliğini ispat etmesi için uygun kimlik doğrulama tekniği belirlenmelidir. Parolalara farklı bir seçenek olarak kriptografik araçlar, akıllı kartlar, token ya da biyometrik araçlar, kimlik doğrulama ve daha etkili kimlik doğrulama gerektiğinde kullanılabilir.

Sistem veya uygulamalara giriş için işlemler, yetkisiz erişim ihtimallerini en aza indirecek şekilde ayarlanmalıdır. Güvenli bir oturum açma prosedürü bu bilgileri sağlamalıdır; oturum açma işlemi gerçekleşmeden uygulamalar ve sistemler görüntülenmemelidir. Sistem ve uygulama tanımlayıcılarını görüntülenmesi ancak oturum açma işlemi başarı ile gerçekleştiğinde olmalıdır. Bilgisayarlara yalnız yetkisi olan kişilerin erişimine açık olduğunu belirten bir uyarı bilgisi görüntülemelidir. Yetkisiz bir kullanıcının oturum açma teşebbüsünde, oturumu açmasına yardımcı olacak hiçbir mesaj görüntülenmemelidir. Girilen tüm girdi ve verilerin geçerli olmaması durumunda oturum açma bilgisi tamamlanmalıdır. Eğer bir hata durumu ortaya çıkarsa, sistem verinin hangi kısmının doğru ve yanlış olduğunu belirtmemelidir. Eğer yanlış bir girişim durumu olursa, sistem verisinin hangi bölümünün hatalı hangi kısmının doğru olduğunu belirten bir ifade yer almamalıdır. Kaba kuvvet ile oturum açma girişimlerine karşı korunaklı

olmalıdır. Tüm başarılı giriş işlemleri ve başarısız girişimlerin kaydı olmalıdır. Tüm erişim girişimleri ve oturum açma kontrollerinde başarısız bir girişim belirlendiğinde güvenlik önlemi alınması için olay başlatılmalıdır.

Daha önce girilen başarılı oturumun tarihi ve zamanı, en son kayıtlı başarılı oturum açılışından bu yana girdiği tüm başarısız oturum açma girişimlerinin ayrıntıları başarılı gerçekleşen oturum açma işlemlerinin ardından görüntülenmelidir.

Parolaların girilmesi anında görüntülenmemesine dikkat edilmelidir. Ağ üzerinden parolalar açık bir biçimde metin şeklinde ulaştırılmamalıdır. Ortak kullanıma açık alanlarda veya kuruluşun güvenliği yeteri kadar sağlanmadığı farklı mekanlarda, risk oluşabilecek ortamlarda; aktif oturum, bilgisayar kullanılmadığında ve ekran zaman aşımı belirtilen süre tamamlandığında ekran koruyucu aktifleşerek oturum kapanmalıdır. Risk ihtimali fazla olan uygulamalar da güvenliği ek olarak arttırmak için ve yetkisiz erişim fırsatlarını minimuma indirmek amacıyla bağlantı süreleri sınırlandırılmalıdır.

5.4.3 Parola Yönetim Sistemi (ISO 27002- Bölüm A.9.4.3)

Bilginin taşıdığı değer ve önemini korumak için parola kullanımı günümüzde mecburi hale gelmiştir. Gelişen teknoloji ile parolalara her yerde kullanılmaktadır. Kişisel veya kurumsal bilgilerin güvenliğini korumak için, bilgisayarlara giriş için, dosyalara, programlara vb. yerlere erişim için kullanılmaktadır. Standartlara uygun interaktif bir parola yönetim sistemi kurularak, yeterli güvenlik düzeyene ulaşmış parolaların kullanımı sağlanmalıdır.

Nitelikli ve zor tahmin edilemez bir parola oluşturmak ne kadar önemli ise parolanın yönetimine de önem verilmelidir. Bir sorun olduğunda çözebilmek ve tespit edebilmek adına kullanıcıların kimlik ve parolalarının kullanımının zorunlu olması gerekmektedir. Yeterli güvenlik seviyesinde parola belirlenmesinin zorunlu tutularak uygun durumlarda kullanıcılara kendi parolalarını kendileri seçme ve değiştirme hakkı tanınmalı, yanlış girişler için de doğrulama prosedürü olmalıdır.

Kullanıcılar ilk oturum açışlarında kendi parolalarını değiştirmek zorunda kalmaları gerekir ve belirli sürelerle parola değiştirme gereksinimi mecburi tutulmalıdır. Daha önce kullanılan parolaların aynısının kullanımı engellenmesi için bir kaydı olmalı ve tekrar kullanımına izin verilmemelidir. Parola bilgilerinin tutulduğu veriler, sistem

dosyalarından farklı bir yerde korunmalıdır. Parolalar korumalı bir formatta saklanmalı ve iletilmelidir. Son olarak da giriş anında ekran üzerinde parolalar görünmemelidir.

5.5.4 Ayrıcalıklı Destek Programlarının Kullanımı (ISO 27002- Bölüm A.9.4.4)

Sistemlerin düzenli uyguladıkları kontrolleri devre dışı bırakacak yardımcı programların kullanımı sınırlandırılarak güçlü kontroller sağlanmalıdır.

Destek sistem programları için yetki verme işlemleri, kullanıcı ekleme ve kimlik doğrulama yöntemleri belirlenmelidir. Destek programlarının kullanımını olabildiğince az sayıda tutarak, güvenilir kullanıcılara yetkili kullanıcı hakkı tanınmalı ve geçici kullanımlar için yetkilendirme yapılmalıdır. Destek programları sürekli kullanıma açık olamamalı, belirli bir süre olarak kullanılmalı örneğin; yetki verilmiş değişim döneminde olabilir. Yetkilendirme düzeyleri tanımları oluşturulmalı ve yazılı belge haline getirilmelidir. Gereksiz yardımcı programların tamamı kaldırılmalı veya deve dışı bırakılmalıdır. Kullanıcıların görevden ayrılması durumunda sistemlere uygulamalara erişimlerin ve yardımcı programların erişimine kapatılması veya devre dışı bırakılması gereklidir. Destek programları kullanımı kayıt altına alınmalı ve destek programları uygulama yazılımlarından ayrı tutulmalıdır.

5.5.5 Program Kaynak Koduna Erişim Protokolü (ISO 27002- Bölüm A.9.4.5)

Program kaynak koduna erişim sınırlandırılmalıdır. Program kaynak kodu bilgisi içeren ögelere yetkisiz kişilerin erişimi engellenerek istenmeyen değişikliklerin önüne geçilmelidir. Aynı zamanda kontrollerin sıklaştırılarak mülkiyet hakkındaki gizlilik korunmalıdır.

Bilgisayar sistemlerinin çökme veya kullanılamaz hale gelmesini önlemek amacıyla program kaynak kütüphanelerine erişiminin kontrolünü sağlamak için dikkat edilmesi gereken maddeler; program kaynak kütüphanelerinin yürütülmesi ve kopyalanması sıkı bir kontrol prosedürü içermelidir. Program kaynak kodu ve kütüphanesi önceden oluşturulmuş yöntemler ile yürütülmelidir.

Programcılar, kaynak kodlara erişim yetkisi aldıktan sonra program kaynaklarının yayınlanması, kaynak kütüphanesinin ve benzer öğelerin güncelleme işlemlerini yapmalıdır. Program kaynak kütüphanelerine erişim sağlayanların uygulamaların içerisinde kimin ne yaptığını tüm detayları ile görüntülemek için denetim günlükleri kayıt

altına alınmalıdır. Program listeleri emniyetli bir yerde tutulmalıdır. Program kaynak kütüphanesi içinde yapılan işlemler sistemlerin içinde tutulmaya gayret edilmelidir.

Program kaynak kodunun yayına çıkması durumu söz konusu ise bütünlüğün korunması için kontroller yapılmalıdır (örneğin; e-imza kullanılabilir). Program kaynak kütüphanesine destek sağlayacak personelin erişimi sınırlı olmalıdır.

5.5 Erişim Kontrol Politikasının Firmalar Açısından Faydaları

- Kullanıcı hesaplarının güvenli yönetimi,
- Şifrelerin güvenli bir şekilde yönetilmesi ve korunması,
- Hizmetlere erişimin kontrollü sağlanması,
- Kuruma ait gizli bilgilerin etkin koruma yöntemi sağlanması,
- Etkili bir iş yönetimi sağlamak için çalışanların doğru erişim hakkına sahip olması,
- Çalışanların yanlış birimlere erişerek hata yapma olasılığının düşürülmesi,
- Bilgi varlıklarının kullanımının denetlenmesi,
- Bilgi varlıklarına erişimin kötü amaçlı kullanılması durumunda takip yeteneği,
- İhtiyaç dahilinde erişim haklarının iptalinin kolaylaştırır.

6. ARAŞTIRMANIN YÖNTEMİ

6.1 Araştırmanın Konusu

Şirketlerin sahip oldukları bilgilerin korunması adına, bilgiye erişimin güvenli olması ve sahip olunan bilgilerin korunması hususunda erişim yönetimi önemlidir. Bu kapsamda bilgi güvenliğini sağlamak için BGYS şirketler tarafından tercih edilen bir sistem olmuştur. İstanbul'da yer alan şirket veya kurumların ISO 27001 BGYS belgesine sahip olan ve BGYS belgesine sahip olmayan şirket ve kurumların A9 Erişim Kontrol Politikası bazında erişim düzeyi arasındaki farkı bu çalışma kapsamında incelenmesi hedeflenmiştir. Şirketlerin erişim politikasının ne kadar uygulandığının araştırılması, belgeye sahip olan ve olmayan şirket veya kurumların erişim düzeylerini belirlenmek istenmiştir. Çıkan sonuçlar üzerinden BGYS ve bilgiye erişim ile ilgili yaşanan problemlere çözüm önerileri sunulmaktadır.

6.2 Araştırmanın Amacı

Araştırmanın amacı İstanbul ilinde eğitim, bilişim, sosyal hizmet, finans ve diğer sektörlerinde çalışan çeşitli pozisyonlarda bilgi sistemlerine erişim sağlayan kişilerin "ISO 27001 BGYS Erişim Kontrol Yönetiminin Şirketlerdeki Uygulanabilirliği"nin seviyelerini tespit etmeye çalışmaktır. Bilgi ve bilgi işleme sistemlerine kullanıcı erişimlerinin güvenli bir şekilde sağlanması, yetkisi olmayan kişilerin erişimlerinin kısıtlanması ve yetkili kişilerin sisteme erişimine izin verilmesine dikkat çekmek çalışmanın özgün değerini oluşturmaktadır.

BGYS politikası uygulayan ve uygulamayan kurumlarda erişim kontrolleri düzeyleri arasındaki fark "erişim kontrolünün iş gereklilikleri"; "kullanıcı erişim yönetimi düzeyi"; "kullanıcı sorumlulukları düzeyi"; "sistem ve uygulama erişim kontrolü" eksenlerinde incelenmiş ve aşağıdaki araştırma soruları oluşturulmuştur.

1. BGYS politikası uygulayan ve uygulamayan kurumlarda erişim kontrolünün iş gereklilikleri düzeyi nasıldır?
2. BGYS politikası uygulayan ve uygulamayan kurumlarda kullanıcı erişim yönetimi düzeyi nasıldır?
3. BGYS politikası uygulayan ve uygulamayan kurumlarda kullanıcı sorumlulukları düzeyi nasıldır?

4. BGYS politikası uygulayan ve uygulamayan kurumlarda sistem ve uygulama erişim kontrolü düzeyi nasıldır?

6.3 Araştırmanın Modeli

Araştırmanın modeli şirketlerin BGYS kapsamında erişim kontrol düzeylerini etkileyen faktörlerin belirlenmesi amacıyla betimsel tarama deseninde tasarlanmıştır (Alsultanny, 2014). Bu bağlamda araştırmacı tarafından erişim kontrol düzeylerini etkileyen faktörlerin tespit edilmesi için 41 sorudan oluşan "ISO 27001 BGYS Erişim Kontrol Yönetiminin Şirketlerdeki Uygulanabilirliği" isimli anket çevrimiçi olarak oluşturulmuştur. Anket içerisinde 5 seçenekli (Kesinlikle Katılmıyorum, Katılmıyorum, Kararsızım, Katılıyorum, Kesinlikle Katılıyorum) Likert Tipi ölçme aracı tercih edilmiştir.

Anket içerisinde yer alan 26 adet sektör isimleri, Mesleki Yeterlilik Kurumunun internet sayfasından alınmıştır (MYK, 2019). Araştırma İstanbul ilinde bulunan ISO/IEC 27001 BGYS sertifikasına sahip olan ve olmayan çeşitli sektörlerde şirket çalışanlarının katılımı ile gerçekleştirilmiştir.

Ölçme aracının görünüş geçerliliğini ve kapsam geçerliliğini sağlamak adına, alan uzmanlarından dört kişiye ölçek maddeleri okutulmuş ve gerekli görülen düzenlemeler yapılmıştır. Bu aşamadan sonra anket katılımcılara açılmıştır.

6.4 Araştırmanın Sınırlılıkları

Bu araştırma sadece İstanbul ilinde gerçekleştirilmiştir. İstanbul Valiliğince yayınlanan verilere göre İstanbul Türkiye'nin en kalabalık şehridir (İstanbul Valiliği, 2019). Yerleşik büyük ölçekli firmaların İstanbul'da bulunması sebebiyle İstanbul'daki şirketlerin ISO 27001 BGYS belgesine sahip olması beklenebilir. Ülkenin nüfus sayısı az illerinde bu sonuç değişkenlik gösterebilir. Farklı şehirlerde yapılan araştırmalar ve daha çok sektör analizlerinden oluşan bir değerlendirme anket sonuçlarında değişkenlik gösterebilir.

6.5 Veri Toplama Aracı

Araştırmaya ilişkin katılımcı görüşlerinin belirlenmesi amacıyla oluşturulan anket üç bölümden oluşmaktadır. Birinci bölüm araştırmaya katılan kişilerin demografik özellikleri ile ilgili sorulardan oluşmaktadır. İkinci bölümde şirketin ISO 27001 BGYS belgesi ile ilgili genel sorular (1 ve 4 arasındaki sorular) yer almaktadır. Üçüncü bölümde

ise sorular (5 numara ve 41 numara arasındaki sorular) ISO 27001 BGYS politikası belgesinde yer alan A9 altındaki 4 ana başlık ve alt başlıkları içerecek şekilde A9 erişim kontrol maddeleri tablosu ele alınarak hazırlanmıştır. Bunlar; erişim kontrolü iş gereklilikleri, kullanıcı erişim yönetimi, kullanıcı sorumlulukları, sistem ve uygulama erişim kontrolü başlıklarıdır. ISO 27001 BGYS Erişim Kontrol Yönetiminin Şirketlerdeki Uygulanabilirliğine ilişkin anket soruları ve ilgili kontrol kategorileri Tablo 6.1'de gösterilmiştir. Anket sorularına ise Ek-1 kısmında yer verilmiştir.

Tablo 6. 1 ISO 27001 BGYS Erişim Kontrol Yönetiminin Şirketlerdeki Uygulanabilirliği Anketi Soruları ve İlgili Kontrol Kategorileri Tablosu

Ana Başlık	**Alt Başlık**	**İlgili Kategori**	**Soru Numaraları (Ölçme Aracı)**
		ISO 27001	1, 2, 3, 4
A.9.1 Erişim kontrolü iş gereklilikleri	A.9.1.1	Erişim kontrol politikası	5, 6, 7
	A.9.1.2	Ağlara ve ağ hizmetlerine erişim	8, 9, 10, 11
A.9.2 Kullanıcı erişim yönetimi	A.9.2.1	Kullanıcı kaydetme ve silme	12, 13, 14, 15
	A.9.2.2	Kullanıcı erişimine izin verme	16, 17, 18, 19, 20
	A.9.2.3	Ayrıcalıklı erişim haklarının yönetimi	21, 22, 23
	A.9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi	24
	A.9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi	25,26
	A.9.2.6	Erişim haklarının kaldırılması veya düzenlenmesi	27,28
A.9.3 Kullanıcı sorumlulukları	A.9.3.1	Gizli kimlik doğrulama bilgisinin kullanımı	29
A.9.4 Sistem ve uygulama erişim kontrolü	A.9.4.1	Bilgiye erişimin kısıtlanması	30, 31, 32, 33
	A.9.4.2	Güvenli oturum açma prosedürleri	34, 35, 36
	A.9.4.3	Parola yönetim sistemi	37, 38, 38, 39, 40, 41
	A.9.4.4	Ayrıcalıklı destek programlarının kullanımı	
	A.9.4.5	Program kaynak koduna erişim protokolü	

A.9.4.4 Ayrıcalıklı destek programlarının kullanımı ve A.9.4.5 Program kaynak koduna erişim protokolü maddeleri genel kullanıcıdan çok IT birimlerinde çalışanları

ilgilendirdiği için o maddeler ile ilgili soru hazırlanmamıştır. 3, 4, 5 ve 37 numaralı sorular Çetinkaya (2008)'den uyarlanmıştır.

6.6 İstatiksel Analiz

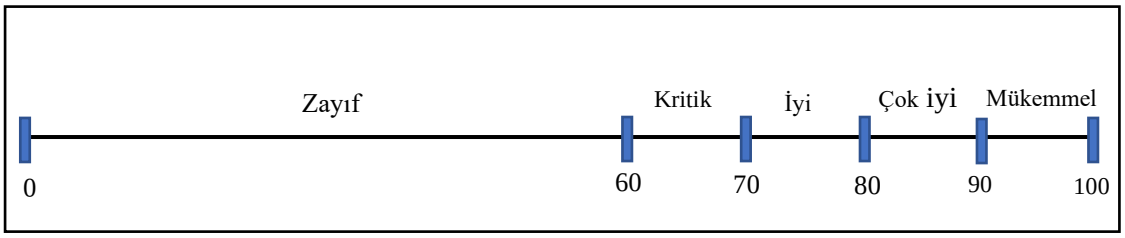
Ankete 344 kişinin katılımı sağlanarak veri toplama süreci tamamlanmıştır. Katılım sağlayan bir kişi cevapları boş bıraktığı için değerlendirmeye alınmamış, 343 kişinin verileri analiz edilmiştir.

Anket verilerinin analizi sürecinde IBM SPSS versiyon 22.0 programı kullanılmıştır. Veri analizi neticesinde Cronbach Alpha ile ölçülen güvenilirlik değeri 0,96 olarak elde edilmiştir. İlgili alanyazında, Cronbach Alfa değerinin 0,7 veya daha yüksek olması durumunda verilerin güvenilir olacağını belirtilmektedir (Pallant, 2005).

Ortalamalar ve standart sapmalar hesaplandıktan sonra bağıl önem Denklem 6.1'de verilen formüle göre hesaplanmıştır (Alsultanny, 2014).

Bağıl Önem= [Ortalama / Üst Ölçek (5)] * 100 (Denklem 6.1)

Bağıl önem hesaplandıktan sonra, seviyesini belirlemek için Şekil 6.1'de gösterilen ölçek kullanılmıştır.



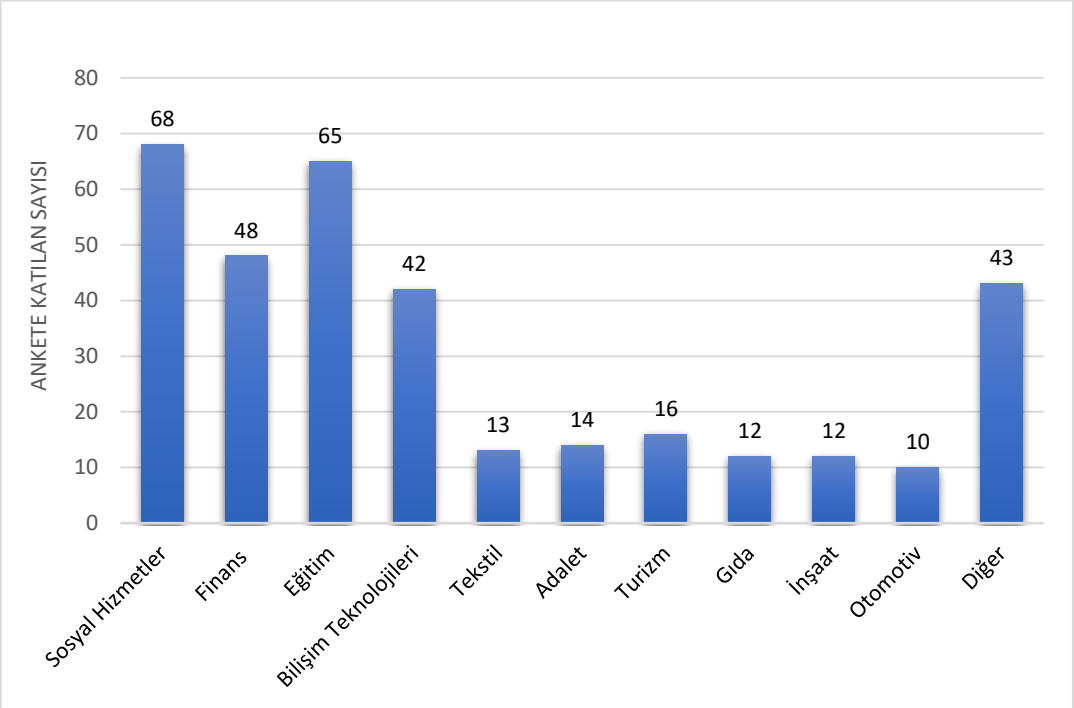
Şekil 6. 1 Sonuç Seviyesini Belirlemek İçin Kullanılan Ölçek

7. BULGULAR

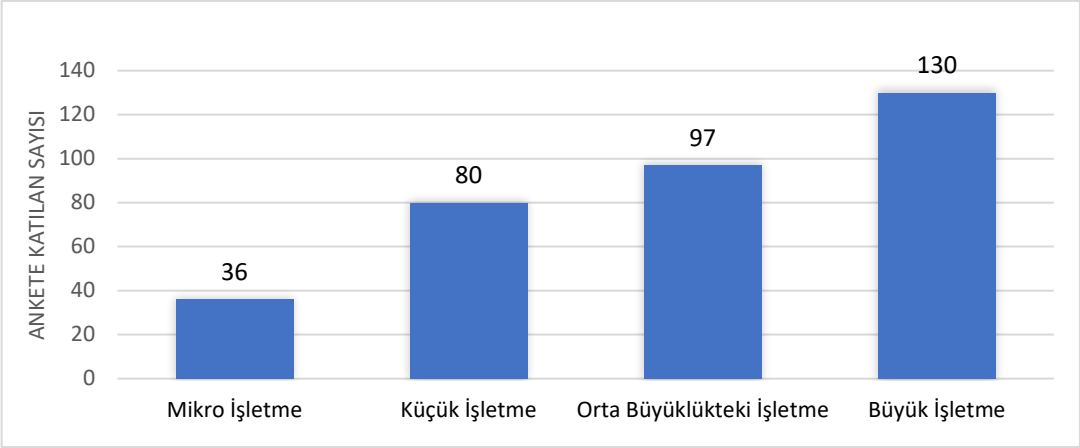
Ankete katılan 343 katılımcıdan, 207 kişi ISO 27001 BGYS belgesine sahip şirket veya kuruluşta çalışmakta, 136 kişi ise ISO 27001 BGYS belgesine sahip olmayan şirket veya kuruluşta çalışmaktadır. Farklı sektörlerde çalışan kişilerin ankete katılımları araştırmanın çeşitliliğini ve zenginliğini arttırmıştır.

Katılımcıların hizmet verdikleri sektörler nicelik fazlalığı yönüyle eğitim, sağlık ve sosyal hizmetler, finans, bilişim teknolojileri, tekstil, adalet, turizm, gıda, inşaat, otomotiv bölümleri olarak belirlenmiş, kalan 12 sektörün dağılım sayıları az olduğu için bu sektörlerin dışında kalan sektörler diğer ismi ile gruplandırılmıştır.

Hizmet verilen sektörlere göre dağılım grafiği, sosyal hizmetler 68 kişi, eğitim 65 kişi, sağlık ve finans 48 kişi, bilişim teknolojileri 42 kişi, tekstil 13 kişi, adalet 14 kişi, turizm 16 kişi, gıda 12 kişi, inşaat 12 kişi, otomotiv 10 kişi, diğer grubu ise 43 kişi olarak Şekil 7.1 gösterilmiştir.

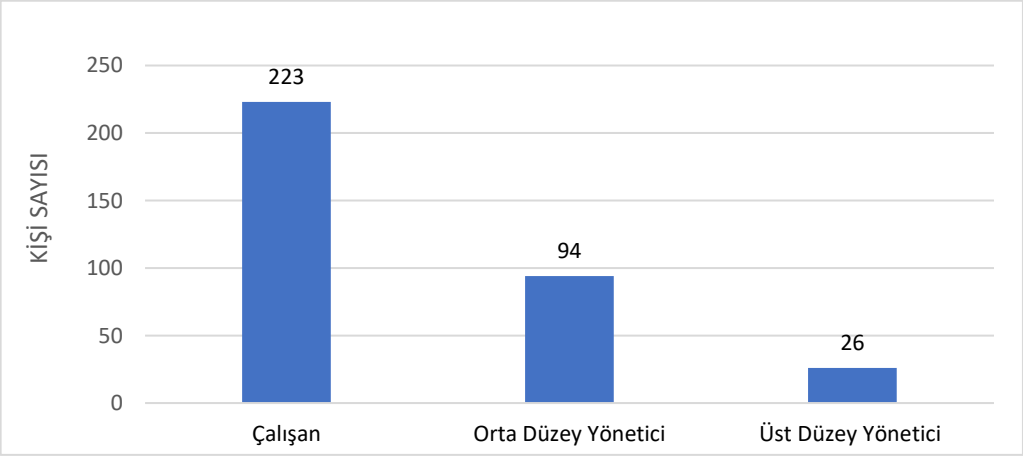


Şekil 7. 1 Hizmet Verilen Sektörlere Göre Dağılım



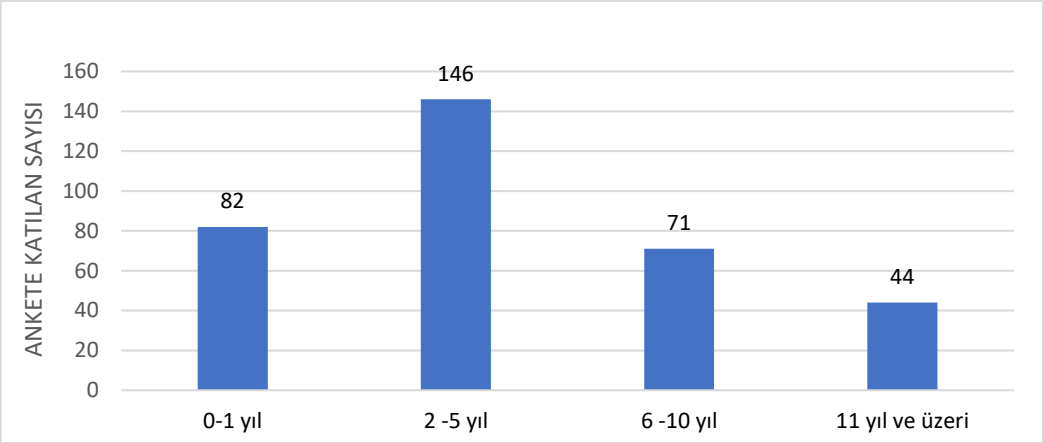
Şekil 7. 2 Büyüklüklerine Göre İşletmelerin Sınıflandırılması

Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik'teki ilgili bölümden alınmıştır; mikro işletme on kişiden az yıllık çalışan istihdam eden, küçük işletme elli kişiden az yıllık çalışan istihdam eden, orta büyüklükteki işletme: iki yüz elli kişiden az yıllık çalışan istihdam eden işletmeler olarak belirtilmiştir (Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik, 2005). Bu çalışmada 251 ve üzeri çalışanlar büyük işletme olarak kabul edilmiştir. Büyüklüklerine göre işletmelerin sınıflandırılmaları ve sayıları Şekil 7.2'de gösterilmiştir. Ankete katılan kişilerin çalıştığı işletme büyüklükleri; 36 kişi mikro işletmede, 80 kişi küçük işletmede, 97 kişi orta büyüklükteki işletme, 130 kişi büyük işletmede çalıştığı görülmektedir.



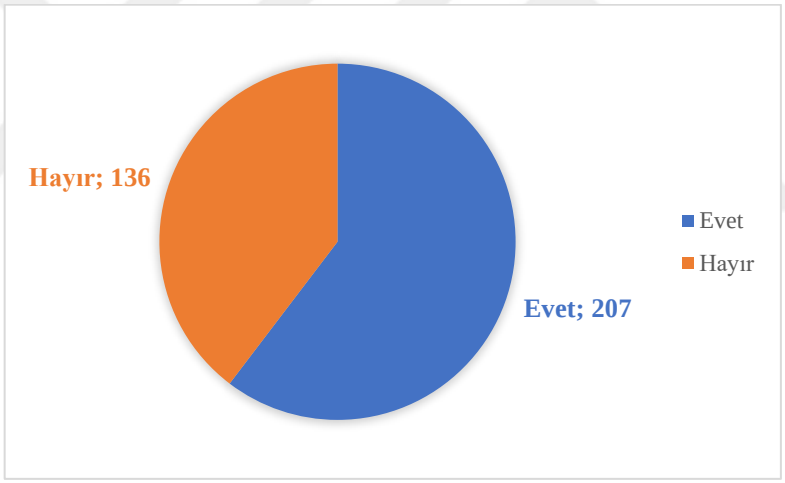
Şekil 7. 3 Ankete Katılan Kişilerin Şirketteki Pozisyonları

Ankete katılan kişilerin şirket içerisindeki pozisyonları sorguladığımızda; Üst Düzey Yönetici 26 kişi, Orta Düzey Yönetici 94 kişi, 223 kişi çalışan pozisyonlarında gösterilmiştir (Şekil 7.3).



Şekil 7. 4 Ankete Katılan Kişilerin Mesleki Kıdemleri

Şirket çalışanlarının çalışma yılları sorgulanmıştır. Ankete katılan kişilerin mesleki kıdemleri Şekil 7.4'te gösterilmiştir. 0-1 yıla arası 82 kişi, 2-5 yıl arası 146 kişi, 6-10 yıl arası 71 kişi, 11 yıl ve üzeri ile 44 kişi olarak gösterilmiştir.



Şekil 7. 5 Ankette BGYS Uygulanma Durumu

Anket içinde yer alan "Şirketinizde ISO 27001 "Bilgi Güvenliği Yönetim Sistemi" politikası uygulanıyor mu?" sorusuna "*Evet*" ve "*Hayır*" cevabı olarak iki farklı cevap seçeneği sunulmuştur. 207 kişi *Evet*, 136 kişi *Hayır* cevabını vermiştir. Şirketlerde BGYS uygulanma durumu Şekil 7.5'te gösterilmiştir.

Katılımcılardan soruya cevap olarak *Evet* seçeneğini işaretleyenlerin çalıştığı şirkette ISO 27001 BGYS politikası uygulanıyor olarak kabul edilmiştir ve tablolar içerisinde "*Evet*" cevabı altında gruplandırılmıştır. Katılımcıların *Hayır* cevabını verenlerin çalıştığı şirkette ISO 27001 BGYS politikası uygulanmıyor olarak kabul

edilmiştir ve "*Hayır*" cevabı altında gruplandırılmıştır. Ankete verilen cevaplar bu iki bağımsız örneklem (*Evet-Hayır*) içerisinde karşılaştırılacaktır.

Tablo 7. 1 Şirket Çalışanlarının Bilgi Güvenliği Yönetim Sistemine İlişkin Bağıl Önem Durumu

No	**İFADELER**	***EVET***				***HAYIR***			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
1	Çalıştığım şirkette ISO 27001 "Bilgi Güvenliği Yönetim Sistemi" belgesi alınmıştır ve uygulanmaktadır.	4,16	1,01	83,29	Çok İyi	1,99	1,10	39,85	Zayıf
2	ISO 27001 politikaları ile ilgili bilgi alabileceğim herksin erişimine açık genel olarak yayınlandığı bir yer vardır / nereden erişim sağlayacağımı biliyorum.	3,57	1,23	71,30	İyi	2,27	1,24	45,44	Zayıf
3	Şirket içerisinde bilgi güvenliği konusunda çalışan vardır.	4,07	1,26	81,35	Çok İyi	2,72	1,37	54,41	Zayıf
4	Bilgi güvenliği politikası yönetim tarafından düzenli olarak gözden geçiriliyor.	4,05	1,14	80,97	Çok İyi	2,75	1,26	55,00	Zayıf
	Final Toplam	**3,96**	**0,94**	**79,23**	**İyi**	**2,43**	**0,97**	**48,68**	**Zayıf**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Bilgi güvenliği yönetim sistemi başlığı altında toplanan dört ifade ve ilgili cevaplar Tablo 7.1'de özetlenmiştir.

ISO 27001 BGYS belgesi alınıp uygulandığının ölçüldüğü birinci soruda; *Evet* grubunun bağıl önemi %83,29 ile çok iyi düzeyde ve *Evet* grubu tablosu içerisinde en yüksek değere sahipken, *Hayır* grubunun bağıl önemi %39,85 ile zayıf düzeydedir.

Çalışanların ISO 27001 politikaları ile ilgili bilgi alabileceği ve nereden erişim sağlayacaklarının ölçüldüğü ikinci soruda; *Evet* grubunun bağıl önemi %71,30 ile iyi düzeyde iken, *Hayır* grubunun bağıl önemi %45,44 ile zayıf düzeydedir.

Şirket içerisinde bilgi güvenliği konusunda çalışanın varlığının sorgulandığı üçüncü soruda; *Evet* grubunun bağıl önemi %81,35 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %54,41 ile zayıf düzeydedir.

Bilgi güvenliği politikası yönetim tarafından düzenli kontrollerinin sağlandığının ölçüldüğü dördüncü soruda; *Evet* grubunun bağıl önemi %80,97 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %55,00 ile zayıf düzeydedir.

BGYS grubu sorularının final toplamı *Evet* grubunun bağıl önemi %79,23 ile iyi düzeyde iken, *Hayır* grubunun bağıl önemi %48,68 ile zayıf düzeydedir.

Tablo 7. 2 Şirket Çalışanlarının Erişim Kontrol Maddelerine İlişkin Bağıl Önem Durumu

No	**Erişim Kontrol Maddeleri**	***EVET***				***HAYIR***			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
1	Erişim kontrol politikası	4,24	0,81	84,77	Çok İyi	3,30	1,15	66,08	Kritik
2	Ağlara ve ağ hizmetlerine erişim	4,20	0,83	84,01	Çok İyi	3,34	1,04	66,80	Kritik
3	Kullanıcı kaydetme ve silme	4,05	0,87	81,06	Çok İyi	3,28	1,03	65,59	Kritik
4	Kullanıcı erişimine izin verme	4,16	0,72	83,28	Çok İyi	3,31	0,92	66,16	Kritik
5	Ayrıcalıklı erişim haklarının yönetimi	3,96	0,99	79,26	İyi	2,90	1,01	57,94	Zayıf
6	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi	3,90	1,28	77,97	İyi	2,80	1,37	56,03	Zayıf
7	Kullanıcı erişim haklarının gözden geçirilmesi	4,02	1,00	80,48	İyi	3,00	1,06	60,07	Zayıf
8	Erişim haklarının kaldırılması veya düzenlenmesi	3,99	1,00	79,76	İyi	3,18	1,06	63,53	Kritik
9	Gizli kimlik doğrulama bilgisinin kullanımı	3,98	1,07	79,61	İyi	2,93	1,20	58,68	Zayıf
10	Bilgiye erişimin kısıtlanması	4,03	0,79	80,53	Çok İyi	3,07	0,96	61,43	Kritik
11	Güvenli oturum açma prosedürleri	4,21	0,91	84,25	Çok İyi	3,08	1,13	61,67	Kritik
12	Parola yönetim sistemi	4,11	0,90	82,28	Çok İyi	3,11	1,08	62,29	Kritik
	Final Toplam	**4,07**	**0,69**	**81,44**	**Çok İyi**	**3,11**	**0,82**	**62,19**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Şirket Çalışanlarının Erişim Kontrol Maddelerine İlişkin Bağıl Önem Durumu Tablo 7.2'de özetlenmiştir.

12 maddeye ayrılmış erişim kontrol maddelerini irdeleyen soruların cevapları incelendiğinde *Evet* grubunun bağıl önemi %81,44 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %62,19 ile kritik düzeyde kalmıştır.

Tablo 7.2 'de yer alan ayrıcalıklı erişim haklarının yönetimi, kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi, kullanıcı erişim haklarının gözden geçirilmesi, erişim haklarının kaldırılması veya düzenlenmesi, gizli kimlik doğrulama bilgisinin kullanımı; ISO 27001 BGYS belgesine sahip olmayan şirket çalışanlarının verdiği cevaplara göre zayıf seviyede çıktığı görülmüştür.

7.1 Birinci Araştırma Sorusuna İlişkin Bulgular

Birinci araştırma sorusu olan "BGYS politikası uygulayan ve uygulamayan kurumlarda erişim kontrolünün iş gereklilikleri düzeyi nasıldır?" sorusuna ilişkin bulgulara aşağıda verilmiştir.

Tablo 7. 3 Şirket Çalışanlarının Erişim Kontrol Politikası Maddelerine İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
5	Şirket çalışanlarının internet kullanımları ve çeşitli uygulamaları kullanımları ağ üzerindeki hareketleri takip etmeye yönelik izleme ve loglama yapılmaktadır.	4,11	1,14	82,22	Çok İyi	3,22	1,39	64,41	Kritik
6	Şirkette erişim yetki ve kontrol matrisi vardır.	4,28	0,96	85,60	Çok İyi	3,21	1,37	64,26	Kritik
7	Şirkette sadece görevimi gerçekleştirmek için gereken bilgilere erişim sağlıyorum.	4,32	0,90	86,47	Çok İyi	3,48	1,34	69,56	Kritik
	Final Toplam	**4,24**	**0,81**	**84,77**	**Çok İyi**	**3,30**	**1,15**	**66,08**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Erişim Kontrol Politikası başlığı altında toplanan üç ifade ve ilgili cevaplar Tablo 7.3'te özetlenmiştir.

Çalışanların internet kullanımlarının takibinin ölçüldüğü beşinci soruda; *Evet* grubunun bağıl önemi %82,22 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %64,41 ile kritik düzeyde gösterilmektedir.

Erişim yetki ve kontrol matrislerinin sorgulandığı altıncı soruda; *Evet* grubunun bağıl önemi %85,60 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %64,26 ile kritik düzeydedir.

Çalışanların görevlerinin tanımları doğrultusundaki bilgilere erişiminin ölçüldüğü yedinci soruda ise; *Evet* grubunun bağıl önemi %86,47 çok iyi düzeyde ve *Evet* grubu tablosu içerisinde en yüksek değere sahipken, *Hayır* grubunun bağıl önemi %69,56 ile kritik düzeydedir.

Erişim Kontrol Politikası grubu sorularının final toplamı *Evet* grubunun %84,77 bağıl önemi ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %66,08 ile kritik düzeydedir.

Tablo 7. 4 Şirket Çalışanlarının Ağlara ve Ağ Hizmetlerine Erişim Maddelerine İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
8	Şirket sistemine uzaktan erişimin sağlanması için yetki onay süreci vardır.	4,30	1,04	86,09	Çok İyi	3,26	1,34	65,15	Kritik
9	Yetkisiz erişimler de dâhil olmak üzere iç ağı, dış tehditlerden korumak için güvenlik önlemleri (güvenlik duvarı vb.) alınıyor.	4,48	0,78	89,57	Çok İyi	3,69	1,20	73,82	İyi
10	Şirket sistemine uzaktan erişim için uyulması gerekli talimatları biliyorum.	3,94	1,19	78,84	İyi	3,18	1,33	63,68	Kritik
11	Şirket sistemine uzaktan erişim için alınan önlemleri güvenli ve yeterli buluyorum.	4,08	1,00	81,55	Çok İyi	3,23	1,22	64,56	Kritik
	Final Toplam	**4,20**	**0,83**	**84,01**	**Çok İyi**	**3,34**	**1,04**	**66,80**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Ağlara ve Ağ Hizmetlerine Erişim başlığı altında toplanan dört ifade ve ilgili cevaplar Tablo 7.4'te özetlenmiştir.

Şirket sistemine uzaktan erişim sağlanması için yetki sürecinin sorulduğu sekizinci soruda; *Evet* grubunun bağıl önemi %86,09 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %65,15 ile kritik düzeye sahiptir.

Şirket içindeki iç ağın koruma düzeyinin ölçüldüğü dokuzuncu soruda; *Evet* grubunun bağıl önemi %89,57 ile çok iyi düzeyde ve *Evet* grubu tablosu içerisinde en yüksek değere sahiptir. *Hayır* grubunun bağıl önemi %73,82 ile iyi düzey sahip ve *Hayır* grubu tablosu içerisinde en yüksek değeri göstermektedir.

Şirket içinde uzaktan erişim için uygulanması gerekli talimatlar bilgisinin ölçüldüğü onuncu soruda; *Evet* grubunun bağıl önemi %78,84 ile iyi düzey sahip iken, *Hayır* grubunun bağıl önemi %63,68 ile kritik düzeydedir.

Şirket sistemine uzaktan erişim için alınan önlemlerin güvenirliğinin ölçüldüğü on birinci soruda; *Evet* grubunun bağıl önemi %81,55 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %64,56 ile kritik düzeydedir.

Ağlara ve Ağ Hizmetlerine Erişim grubu sorularının final toplamı *Evet* grubunun bağıl önemi %84,01 ile çok iyi düzeyde iken, *Hayır* grubunun bağıl önemi %66,80 ile kritik düzeyde gösterilmiştir.

7.2 İkinci Araştırma Sorusuna İlişkin Bulgular

İkinci araştırma sorusu olan "BGYS politikası uygulayan ve uygulamayan kurumlarda kullanıcı erişim yönetimi düzeyi nasıldır?" sorusuna ilişkin bulgulara aşağıda verilmiştir.

Tablo 7. 5 Şirket Çalışanlarının Kullanıcı Kaydetme ve Silme ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
12	Yeni bir çalışan işe başladığında kullanıcı kaydetme işlemleri kontrollü bir şekilde gerçekleştirilir.	4,26	0,96	85,12	Çok İyi	3,47	1,25	69,41	Kritik
13	Şirketten ayrılan kullanıcılar kullanıcı kimliklerinin kaldırılmasına yönelik izlenen bir süreç vardır.	4,11	1,07	82,13	Çok İyi	3,36	1,22	67,21	Kritik
14	Şirketten ayrılan kullanıcıların kullanıcı kimlikleri hemen kaldırılır.	3,93	1,15	78,65	İyi	3,21	1,21	64,26	Kritik
15	Periyodik olarak kullanıcı kimlikleri kontrol edilir.	3,92	1,01	78,36	İyi	3,07	1,15	61,47	Kritik
	Final Toplam	**4,05**	**0,87**	**81,06**	**Çok İyi**	**3,28**	**1,03**	**65,59**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Kullanıcı Kaydetme ve Silme başlığı altında toplanan dört ifade ve ilgili cevaplar Tablo 7.5'te özetlenmiştir.

Yeni bir çalışan işe başladığında kullanıcı kayıt işlemlerinin kontrolü ile ilgili on ikinci soruda; *Evet* grubunun bağıl önemi %85,12 ile çok iyi düzeye sahip ve *Evet* grubu tablosu içerisinde en yüksek değere sahiptir. *Hayır* grubunun bağıl önemi %69,41 ile kritik düzeydedir.

Şirketten ayrılan kullanıcılar kullanıcı kimliklerinin kaldırılmasına yönelik izlenen sürecin varlığının sorgulandığı on üçüncü soruda; *Evet* grubunun bağıl önemi %82,13 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %67,21 ile kritik düzeydedir.

Şirketten ayrılan kullanıcıların kullanıcı kimliklerinin kaldırılmasının ölçüldüğü on dördüncü soruda; *Evet* grubunun bağıl önemi %78,65 ile iyi düzeyde iken, *Hayır* grubunun bağıl önemi %64,26 ile kritik düzeydedir.

Kullanıcı kimliklerinin periyodik olarak kontrolünün ölçüldüğü on beşinci soruda; *Evet* grubunun bağıl önemi %78,36 ile iyi düzeyde iken, *Hayır* grubunun bağıl önemi %61,47 ile kritik düzeydedir.

Kullanıcı Kaydetme ve Silme grubu sorularının final toplamı *Evet* grubunun bağıl önemi %81,06 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %65,59 ile kritik düzeydedir.

Tablo 7. 6 Şirket Çalışanlarının Kullanıcı Erişimine İzin Verme ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
16	Şirket çalışanları rollerinin gerektirdiği işlemler için sisteme erişimi sağlanır.	4,30	0,86	86,09	Çok İyi	3,43	1,11	68,68	Kritik
17	Kullanıcıların bilgi sistemi kullanımı ve erişim hakları yönetim tarafından belirlenir.	4,28	0,90	85,51	Çok İyi	3,58	1,13	71,62	İyi
18	Bilgi sistemlerine ve hizmetlerine erişmek için kullanıcı kimliklerine verilen erişim haklarının kaydı şirket tarafından tutulur.	4,28	0,82	85,51	Çok İyi	3,40	1,16	67,94	Kritik
19	Şirket çalışanlarının sisteme erişimi şirkette yürütmekte oldukları görevleri doğrultusunda önceden belirlenmiş rollere göre tanımlanır.	4,22	0,91	84,35	Çok İyi	3,43	1,21	68,53	Kritik
20	Yetkim dışında bir yere erişmeye çalıştığımda yöneticime uyarı gider.	3,64	1,28	72,75	İyi	2,65	1,24	53,09	Zayıf
	Final Toplam	**4,14**	**0,72**	**82,84**	**Çok İyi**	**3,30**	**0,92**	**65,97**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Kullanıcı Erişimine İzin Verme başlığı altında toplanan beş ifade ve ilgili cevaplar Tablo 7.6 ’da özetlenmiştir.

Şirket çalışanlarının rollerinin gerektirdiği işlemler için sisteme erişimlerinin ölçüldüğü on altıncı soruda; *Evet* grubunun bağıl önemi %86,06 ile çok iyi düzeye sahip ve *Evet* grubu tablosu içerisinde en yüksek değere sahiptir. *Hayır* grubunun bağıl önemi %68,68 ile kritik düzeydedir.

Kullanıcıların bilgi sistemi kullanımı ve erişim hakları yönetimin belirlediğinin sorgulandığı on yedinci soruda; *Evet* grubunun bağıl önemi %85,51 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %71,62 ile iyi düzeyde aynı zamanda *Hayır* grubu tablosu içerisinde en yüksek değeri göstermektedir. ISO 27001 BGYS olsun olmasın, yönetimin kullanıcıların erişim haklarının belirlenmesinde aktif rol oynadığı görülmüştür.

Bilgi sistemlerine erişmek için kullanıcı kimliklerine verilen erişim haklarının kaydının şirket tarafından tutulduğunun ölçüldüğü on sekizinci soruda; *Evet* grubunun bağıl önemi %85,51 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %67,94 ile kritik düzeydedir.

Şirket çalışanlarının sisteme erişimi görevleri doğrultusunda önceden belirlenmiş rollere göre tanımlandığının ölçüldüğü on dokuzuncu soruda; *Evet* grubunun bağıl önemi %84,35 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %68,53 ile kritik düzeydedir.

Çalışanların yetkisi dışında bir yere erişmeye çalıştığında yöneticilerinin haberdar edilmesinin sorgulandığı yirminci soruda; *Evet* grubunun bağıl önemi %72,75 iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %53,09 ile zayıf düzeydedir.

Kullanıcı Erişimine İzin Verme grubu sorularının final toplamı *Evet* grubunun bağıl önemi %82,84 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %65,97 ile kritik düzeydedir.

Tablo 7. 7 Şirket Çalışanlarının Ayrıcalıklı Erişim Haklarının Yönetimi Maddelerine İlişkin Bağıl Önem Durumu

No	**İFADELER**	***EVET***				***HAYIR***			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
21	Şirket bilgi sistemlerine ayrıcalıklı erişim yapacak kullanıcılar erişim yapılacakları bilgisayarlara ait IP/MAC adreslerini bilgi işleme bildirmektedir	4,04	1,01	80,77	İyi	2,90	1,18	57,94	Zayıf
22	Ayrıcalıklı erişim yapacak kullanıcıların ağda kalış süreleri ve erişebilecekleri alanlar tanımlanmıştır ve loglanmaktadır.	3,94	1,16	78,74	İyi	2,89	1,22	57,79	Zayıf
23	Ayrıcalıklı erişim haklarına sahip kullanıcıların yetkinlikleri, söz konusu ayrıcalıklarının görevleri ile ilişkili olup olmadığının doğrulanması için düzenli olarak gözden geçirilir.	3,91	1,08	78,26	İyi	2,90	1,15	58,09	Zayıf
	Final Toplam	**3,96**	**0,99**	**79,26**	**İyi**	**2,90**	**1,01**	**57,94**	**Zayıf**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Ayrıcalıklı Erişim Haklarının Yönetimi başlığı altında toplanan üç ifade ve ilgili cevaplar Tablo 7.7'de özetlenmiştir.

Şirket bilgi sistemlerine ayrıcalıklı erişim yapacak kullanıcıların bilgi işleme bilgisayarlara ait IP/MAC adresleri ile ilgili bilgi verildiğinin ölçüldüğü yirmi birinci soruda; *Evet* grubunun bağıl önemi %80,77 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %57,94 ile zayıf düzeydedir.

Ayrıcalıklı erişim yapacak kullanıcıların ağda kalış süreleri ve erişebilecekleri alanların tanımlanıp kayıtlarının tutulduğunun ölçüldüğü yirmi ikinci soruda; *Evet* grubunun bağıl önemi %78,74 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %57,79 ile zayıf düzeydedir.

Ayrıcalıklı erişim haklarına sahip kullanıcıların yetkinlikleri, söz konusu ayrıcalıklarının görevleri ile ilişkili olup olmadığının kontrolünün ölçüldüğü Yirmi üçüncü soruda; *Evet* grubunun bağıl önemi %78,26 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %58,09 ile zayıf düzeyde gösterilmiştir.

Ayrıcalıklı Erişim Haklarının Yönetimi grubu sorularının final toplamı *Evet* grubunun bağıl önemi %79,26 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %57,94 ile zayıf düzeydedir.

Tablo 7. 8 Şirket Çalışanlarının Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	**İFADELER**	***EVET***				***HAYIR***			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
24	Kullanıcıların kimliklerinin doğrulanması için bazı yöntemler (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılır.	3,90	1,28	77,97	İyi	2,80	1,37	56,03	Zayıf

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Kullanıcıların kimliklerinin doğrulanması için uygulanan yöntemlerin sorgulandığı yirmi dördüncü soruda; *Evet* grubunun bağıl önemi %77,97 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %56,03 ile zayıf düzeydedir. (Tablo 7.8)

Tablo 7. 9 Şirket Çalışanlarının Kullanıcı Erişim Haklarının Gözden Geçirilmesi ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
25	Kullanıcı erişim hakları yönetim ve bilgi güvenliği birimi tarafından belirli periyotlarla kontrol edilmektedir.	4,00	1,05	80,00	İyi	2,94	1,13	58,82	Zayıf
26	Şirket içinde bir iş rolünden diğerine geçiş durumunda kullanıcı erişim hakları gözden geçirilerek yeniden tahsis edilir.	4,05	1,10	80,97	Çok İyi	3,07	1,21	61,32	Kritik
	Final Toplam	**4,02**	**1,00**	**80,48**	**İyi**	**3,00**	**1,06**	**60,07**	**Zayıf**

σ: Standart Sapma Bö: Bağıl önem Ort.: Ortalama

Kullanıcı Erişim Haklarının Gözden Geçirilmesi başlığı altında toplanan iki ifade ve ilgili cevaplar Tablo 7.9 ‘da özetlenmiştir.

Yönetim ve bilgi güvenliği biriminin kullanıcı erişim haklarının periyodik kontrolü ile ilgili yirmi beşinci soruda; *Evet* grubunun bağıl önemi %80,00 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %58,82 ile zayıf düzeydedir.

Şirket içinde iş rolü değişikliğinde kullanıcı erişim haklarının kontrolü ve düzenlemelerinin araştırıldığı yirmi altıncı soruda; *Evet* grubunun bağıl önemi %80,97 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %61,32 ile kritik düzeydedir.

Kullanıcı Erişim Haklarının Gözden Geçirilmesi grubu sorularının final toplamı *Evet* grubunun bağıl önemi %80,48 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %60,07 ile zayıf düzeydedir.

Tablo 7. 10 Şirket Çalışanlarının Erişim Haklarının Kaldırılması veya Düzenlenmesi ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
27	Yetki değişiklik taleplerinin hangi koşullarda ve nasıl yapılacağını biliyorum.	3,87	1,16	77,39	İyi	3,07	1,24	61,32	Kritik
28	Hizmet veya sisteme erişim için nasıl ve kime müracaat edileceği tüm kullanıcılar tarafından bilinir.	4,11	1,04	82,13	Çok İyi	3,29	1,22	65,74	Kritik
	Final Toplam	**3,99**	**1,00**	**79,76**	**İyi**	**3,18**	**1,06**	**63,53**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort: Ortalama

Erişim Haklarının Kaldırılması veya Düzenlenmesi başlığı altında toplanan iki ifade ve ilgili cevaplar Tablo 7.10 ‘da özetlenmiştir.

Yetki değişiklik taleplerinin hangi koşullarda ve nasıl yapılacağını bilinirliğinin ölçüldüğü yirmi yedinci soruda; *Evet* grubunun bağıl önemi %77,39 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %61,32 ile kritik düzeydedir.

Kullanıcıların hizmet veya sisteme erişim için nasıl ve kime müracaat edileceğinin sorgulandığı yirmi sekizinci soruda; *Evet* grubunun bağıl önemi %82,13 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %65,74 ile kritik düzeydedir.

Erişim Haklarının Kaldırılması veya Düzenlenmesi grubu sorularının final toplamı *Evet* grubunun bağıl önemi %79,76 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %63,53 ile kritik düzeydedir.

7.3 Üçüncü Araştırma Sorusuna İlişkin Bulgular

Üçüncü araştırma sorusu olan “BGYS politikası uygulayan ve uygulamayan kurumlarda kullanıcı sorumlulukları düzeyi nasıldır?” sorusuna ilişkin bulgulara aşağıda verilmiştir.

Tablo 7. 11 Şirket Çalışanlarının Gizli Kimlik Doğrulama Bilgisinin Kullanımı ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	**İFADELER**	***EVET***				***HAYIR***			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
29	Şirket prosedürleri gereği kullandığımız kimlik doğrulama bilgileri zor ve tahmin edilemezdir.	3,98	1,07	79,61	İyi	2,93	1,20	58,68	Zayıf

σ: Standart Sapma Bö: Bağıl önem Ort: Ortalama

Kimlik doğrulama bilgilerinin zor ve tahmin edilemez olduğunu ölçtüğümüz yirmi dokuzuncu soruda; *Evet* grubunun bağıl önemi %79,61 iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %58,68 ile zayıf düzeydedir (Tablo 7.11).

7.4 Dördüncü Araştırma Sorusuna İlişkin Bulgular

Dördüncü araştırma sorusu olan “BGYS politikası uygulayan ve uygulamayan kurumlarda sistem ve uygulama erişim kontrolü düzeyi nasıldır?” sorusuna ilişkin bulgulara aşağıda verilmiştir.

Tablo 7. 12 Şirket Çalışanlarının Bilgiye Erişimin Kısıtlanması ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
30	Görevim ile ilgili eriştiğim verilerin tümü kayıt altına alınmaktadır.	4,10	0,93	81,93	Çok İyi	3,24	1,26	64,85	Kritik
31	Erişilen ve kaydı tutulan veriler belirli sürelerle gözden geçirilmektedir.	3,87	1,02	77,49	İyi	2,93	1,11	58,53	Zayıf
32	Kullanıcıların erişim haklarının kontrolü örneğin; okuma, yazma, silme ve yürütme olarak IT departmanı tarafından tanımlanır.	4,12	0,90	82,32	Çok İyi	3,07	1,28	61,32	Kritik
33	Erişim kontrollerini sağlayan IT birimi de yönetim tarafından kontrol edilir.	4,02	0,97	80,39	İyi	3,05	1,36	61,03	Kritik
	Final Toplam	**4,03**	**0,79**	**80,53**	**Çok İyi**	**3,07**	**0,96**	**61,43**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort: Ortalama

Bilgiye Erişimin Kısıtlanması başlığı altında toplanan dört ifade ve ilgili cevaplar Tablo 7.12 ‘de özetlenmiştir.

Çalışanların görevleri doğrultusunda eriştiği verilerle ilgili kayıtların alındığının ölçüldüğü otuzuncu soruda; *Evet* grubunun bağıl önemi %81,93 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %64,85 ile kritik düzeydedir.

Erişilen ve kaydı tutulan verilerin belirli sürelerle kontrollünün ölçüldüğü otuz birinci soruda; *Evet* grubunun bağıl önemi %77,49 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %58,53 ile zayıf düzeydedir ve *Hayır* grubu tablosu içerisinde en düşük değere sahiptir.

Kullanıcıların erişim haklarının kontrolü IT departmanı tarafından tanımlandığının sorgulandığı otuz ikinci soruda; *Evet* grubunun bağıl önemi %82,32 ile çok iyi düzeyde ve *Evet* grubu tablosu içerisinde en yüksek değere sahip iken, *Hayır* grubunun bağıl önemi %61,32 ile kritik düzeydedir.

Yönetimin, erişim kontrollerini sağlayan IT biriminin kontrolünün sorulduğu otuz üçüncü soruda; *Evet* grubunun bağıl önemi %80,39 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %61,03 ile kritik düzeydedir.

Bilgiye Erişimin Kısıtlanması grubu sorularının final toplamı *Evet* grubunun bağıl önemi %80,53 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %61,43 ile kritik düzeydedir.

Tablo 7. 13 Şirket Çalışanlarının Güvenli Oturum Açma Prosedürleri ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
34	Kullanıcı şifrelerinin son kullanma süresi vardır.	4,26	1,11	85,12	Çok İyi	3,16	1,44	63,24	Kritik
35	Kullanıcıların art arda yapılan kimlik doğrulama hatasından sonra erişim kilitlenir.	4,18	1,12	83,57	Çok İyi	2,99	1,29	59,85	Zayıf
36	Çalışanlar bilgisayarların başından kalktıklarında oturumlarını kilitlemekte yâda otomatik olarak bilgisayar oturumları kilitlenmektedir.	4,20	1,10	84,06	Çok İyi	3,10	1,36	61,91	Kritik
	Final Toplam	**4,21**	**0,91**	**84,25**	**Çok İyi**	**3,08**	**1,13**	**61,67**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort: Ortalama

Güvenli Oturum Açma Prosedürleri başlığı altında toplanan üç ifade ve ilgili cevaplar Tablo 7.13'te özetlenmiştir.

Kullanıcı şifrelerinin son kullanma süresinin varlığının ölçüldüğü otuz dördüncü soruda; *Evet* grubunun bağıl önemi %85,12 ile çok iyi düzeyde ve *Evet* grubu tablosu içerisinde en yüksek değere sahip iken, *Hayır* grubunun bağıl önemi %63,24 ile kritik düzeydedir.

Art arda yapılan kimlik doğrulama hatasından sonra erişimin kilitlenmesinin ölçüldüğü otuz beşinci soruda; *Evet* grubunun bağıl önemi %83,57 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %59,85 ile zayıf düzeyde ve *Hayır* grubu tablosu içerisinde en düşük değere sahiptir.

Çalışanlar bilgisayarların başında değilken oturumlarını kilitlemekte ya da otomatik bilgisayar oturumları kilitlenmesinin ölçüldüğü otuz altıncı soruda; *Evet* grubunun bağıl önemi %84,06 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %61,91 ile kritik düzeydedir.

Güvenli Oturum Açma Prosedürleri grubu sorularının final toplamı *Evet* grubunun bağıl önemi %84,25 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %61,67 ile kritik düzeydedir.

Tablo 7. 14 Şirket Çalışanlarının Parola Yönetim Sistemi ile İlgili Maddelere İlişkin Bağıl Önem Durumu

No	İFADELER	*EVET*				*HAYIR*			
		Ort.	**σ**	**Bö%**	**Seviye**	**Ort.**	**σ**	**Bö%**	**Seviye**
37	Şirket sistemi gereği belirli aralıkla parolamı değiştirmem bekleniyor.	4,26	1,11	85,12	Çok İyi	3,17	1,42	63,38	Kritik
38	Şirketim sadece zor olan parolaları kullanmama izin veriyor.	4,02	1,21	80,39	İyi	3,10	1,35	62,06	Kritik
39	Oluşturulan parolaların güvenliğini kontrol edebileceğim sistemi (Kolay -Orta- Zor) görebiliyor ve ona göre değişiklik yapabiliyorum.	3,65	1,29	73,04	İyi	2,66	1,32	53,24	Zayıf
40	Parolamın süresi dolduğunda uyarı geliyor, erişim kısıtlanıyor ve değiştirmek zorunda kalıyorum.	4,25	1,08	84,93	Çok İyi	3,12	1,42	62,35	Kritik
41	Parola oluşturma talimatlarını biliyorum ve uyguluyorum.	4,40	0,91	87,92	Çok İyi	3,52	1,24	70,44	Kritik
	Final Toplam	**4,11**	**0,90**	**82,28**	**Çok İyi**	**3,11**	**1,08**	**62,29**	**Kritik**

σ: Standart Sapma Bö: Bağıl önem Ort: Ortalama

Parola Yönetim Sistemi başlığı altında toplanan beş ifade ve ilgili cevaplar Tablo 7.14 ‘de özetlenmiştir.

Şirket sistemi gereği belirli aralıkla parola değişikliğinin ölçüldüğü otuz yedinci soruda; *Evet* grubunun bağıl önemi %85,12 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %63,38 ile kritik düzeydedir.

Şirket sistemi gereği sadece zor olan parolaların kullanımı izninin ölçüldüğü otuz sekizinci soruda; *Evet* grubunun bağıl önemi %80,39 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %62,06 ile kritik düzeydedir.

Oluşturulan parolaların güvenliğini kontrol eden sistemi (Kolay -Orta- Zor) ile ilgili otuz dokuzuncu soruda; *Evet* grubunun bağıl önemi %73,04 ile iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %53,24 ile zayıf düzeyde ve *Hayır* grubu tablosu içerisinde en düşük değere sahiptir.

Parolaların süresi dolduğunda değiştirme zorunluluğunun sorgulandığı kırkıncı soruda; *Evet* grubunun bağıl önemi %84,93 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %62,35 ile kritik düzeydedir.

Parola oluşturma talimatları bilgisinin ölçüldüğü kırk birinci soruda; *Evet* grubunun bağıl önemi %87,92 ile çok düzeyde ve *Evet* grubu tablosu içerisinde en yüksek değere sahip iken, *Hayır* grubunun bağıl önemi %70,44 ile kritik düzeydedir.

Parola Yönetim Sistemi grubu sorularının final toplamı *Evet* grubunun bağıl önemi %82,28 ile çok iyi düzeye sahip iken, *Hayır* grubunun bağıl önemi %62,29 ile kritik düzeydedir.

8. TARTIŞMA

Deloitte GFSI (Global Financial Service Industry- Global Finansal Hizmet Sektörü) firmasının 2007 yılında yaptığı güvenlik anketi çalışmasına 32 ülkeden 170'in üzerinde finans kuruluşu katılım sağlamıştır. Ankete katılan kurumların %50'si birinci operasyonel önceliklerinin "erişim ve kimlik yönetimi" olduğunu söylemiştir. Çalışmada gösterilen en yaygın 15 iç denetim bulgusundan 5 tanesi erişim ve kimlik yönetimi ile ilgili olduğu ortaya çıkmıştır. Bunlar; gereğinden fazla verilmiş erişim yetkileri, görev değişimi ve sonlanması ardından erişim yetkilerinin silinmemesi, erişim kontrollerinin prosedürlerle uyumsuzluğu, yazılım geliştirme personelinin üretim ortamında gereğinden fazla yetkisinin olması, zayıf şifre parametrelerinin kullanılması olarak gösterilmiştir (Özgirgin, 2007). Yapılan çalışmada erişim ve kimlik yönetiminin dikkat edilmesi gereken en öncelikli faaliyetlerden biri olduğuna dikkat çekmiştir. Çıkan sonuçlar üzerinden erişim güvenliğinin tüm dünyada alınması gereken önlemler arasında olduğu görülmektedir.

Marjanovic (2017)'e göre orta ölçekli firmalar kişisel veri sızmasında büyük ölçekli firmalara göre daha çok saldırıya uğramaktadır. Bu açıdan orta ölçekli firmaların bilgi sızmasına karşı, erişim kontrollerinin daha dikkatli olması gerektiği söylenebilir. Bununla beraber yapmış olduğumuz bu tez çalışmasında, ISO 27001 BGYS içerisinde yer alan erişim kontrol politikalarının uygulanması ile şirket büyüklüğü arasında herhangi anlamlı bir ilişki bulunamamıştır. Bu iki çalışma arasındaki fark, örneklemlerin farklı olmasından kaynaklanıyor olabilir.

Javorović & Bilandžić (2007)'e göre kurumların bilgi sistemlerinin yetkisiz erişime karşı korunmasının bilgi güvenliği için önemli dört alan içerdiğine dikkat çekmektedir: güvenlik doğrulaması, fiziksel güvenlik, veri güvenliği ve bilgi sistemi güvenliğinden oluşmaktadır. Bunlara ek olarak bu araştırmada ISO 27001 BGYS içerisinde yer alan erişim kontrol politikasının uygulanması ISO 27001 BGYS sistemine sahip şirketlerin erişim politikasının çok iyi seviyede olduğunu göstermiştir. Bu sonuç yetkisiz erişimlere karşı güvenli bir koruma sağladığını göstermektedir.

Eğitim, Teknoloji, Sağlık ve Sosyal Hizmetler, Finans sektörleri BGYS politikalarının tartışılması:

Çalışmaya katılan şirketlerin ayrıcalıklı erişim haklarının yönetimi politikalarına yönelik inceleme neticesinde şirket bilgi işlem sistemlerine ayrıcalıklı erişim yapacak kullanıcıların erişim için kullanacakları kişisel ya da kurumsal bilgisayarlara ait IP/MAC adreslerini bilgi işlem sorumlularına bildirmede kabul edilebilir (X=4,04) iyi seviyede oldukları dolayısıyla ayrıcalıklı erişim haklarına sahip kullanıcıların ayrıcalıklarının görev alanları ile ilişkili olup olmadığının doğrulanması için önemli bir tedbir olduğu düşünülmektedir. Buna ilişkin olarak eğitim sektörünün bilgi güvenliği politikaları incelendiğinde de benzer şekilde bir IP/MAC adresi kayıt ve takip sisteminin varlığı görülmektedir. Finans sektörünün BGYS politikalarında ayrıcalıklı erişim haklarının yönetimi ile ilgili maddelerin olmadığı görülmektedir. Sağlık sektörünün BGYS politikalarında ayrıcalıklı hesapların erişim haklarının tahsisi 3 aylık süreyi geçmeyecek şekilde kontrolü sağlanır. Ayrıcalıklı erişim hakkı verilen çalışan sayısı asgari düzeyde tutulmaktadır. Ayrıcalıklı erişim hakkı düzenli yürüttüğü görevin dışında tanımlanan bir kimliği kapsamaktadır. Ayrıcalıklı erişim hakkı yer değişikliği veya görev değişikliği söz konusu olduğunda erişim haklarını düzenleyen birime bilgi verilmesi gerektiği ile ilgili maddeler yer almaktadır. Teknoloji sektörünün BGYS politikalarında ayrıcalıklı erişim haklarının yönetimine yönelik bir maddeye rastlanmamıştır.

Şirket çalışanlarının fiziksel bazlı kimlik doğrulama bilgilerine ilişkin seviyelerinin (X=3,90) iyi düzeyde olduğu tespit edilmiş; şirketlerin kullanıcıların fiziksel kimliklerinin doğrulanmasına da önem verdiği düşünülmektedir. İlgili eğitim sektörü BGYS politikaları içerisinde kullanıcı güvenliği politikası gereği bu bulguyu destekler nitelikte fiziksel kimlik doğrulama yöntemlerine (akıllı kart ve token) başvurulduğu görülmektedir. Finans sektörünün BGYS politikalarında akıllı kart, biyometrik bilgi içeren verilerin kullanıldığı maddeler arasında yer almıştır. Sağlık sektörünün BGYS politikalarında kullanıcıların kimliklerinin doğrulanması için bazı yöntemler (akıllı kart, tek kullanımlık parola, parmak izi, token vb.) kullanıldığı maddelerin varlığı görülmektedir. Teknoloji sektörünün BGYS politikalarında fiziksel bazlı kimlik doğrulama ile ilgili bir yazıya rastlanmamıştır.

Şirketlerin kullanıcı erişim haklarının gözden geçirilmesine yönelik politika maddeleri değerlendirildiğinde, kullanıcıların sahip oldukları erişim haklarının belirli

aralıklarla bilgi güvenliği vb. birimler aracılığıyla yeterli düzeyde (X=4,00) kontrol edildiği ve şirket içinde gerçekleştirilen rol değişikliklerinin hemen ardında kullanıcıların erişim haklarının çok iyi düzeyde (X=4,05) yeniden gözden geçirildiği tespit edilmiştir. Bununla birlikte incelenen eğitim sektörü BGYS belgesinde de benzer şekilde kullanıcı erişim haklarının düzenli aralıklarla yetkililer tarafından kontrol edilmesine ve rol değişikliklerinde kullanıcı erişim haklarının yeniden gözden geçirilip gerekli güncellemelerin yapılması gerekliliğine ilişkin maddelerin olduğu görülmektedir. Finans sektörünün BGYS politikaları bilgiye erişimi kontrol etmek ve yetkisiz erişimleri önlemek için gerekli güvenlik önemlerini maddelerine yer verilmiştir. Sağlık sektörünün BGYS politikalarında erişim hakları iş değişikliği, görev yeri değişikliği terfi vb. nedenlerle kontrolü sağlanarak belirli periyotlarla gözden geçirilmektedir. Teknoloji sektörünün BGYS politikalarında genel olarak politikanın genel olarak gözden geçirme prosedüründen bahsetmiştir ancak erişim haklarının gözden geçirilmesine yönelik politika maddelerine yer vermediği görülmüştür.

Çalışmaya katılan yönetici ve çalışanların, erişim haklarının kaldırılmasına ilişkin yetki değişikliklerinde taleplerin hangi şartlar altında ve nasıl yapılacağına dair bilgilerinin kabul edilebilir (X=3,87) iyi düzeyde olduğu tespit edilmiş olup sistemlere erişim için ise nasıl ve kimlere müracaat edileceğinin tüm çalışanlar tarafından bilindiğine ilişkin yaygın görüşün ise çok iyi (X=4,11) düzeyde olduğu görülmüştür. Dolayısıyla şirketin tüm çalışanlarının BGYS içerisinde erişim haklarının kaldırılmasına ilişkin olarak yetki değişikliklerinin nasıl yapılacağına dair bilgilerinin tam olmaması şirket bilgi güvenliği açısından güçlü görülmektedir. Benzer şekilde ele alınan eğitim sektörü BGYS politikaları gereği yetki değişiklik taleplerinde çalışanların kime başvuru yapılacağına ilişkin maddeler varken hangi şartlar altında bu başvurunun yapılabileceğine ilişkin kesin maddelerin olmadığı tespit edilmiştir. Finans sektöründe BGYS politikaları ile ilgili erişim haklarının kaldırılmasına ilişkin bir madde görülmemektedir. Sağlık sektöründeki BGYS politikaları periyodik olarak kontrol edilmekte ve kontrol sürecinde gereğinden fazla verilmiş erişim hakları kaldırılmaktadır. Teknoloji sektörünün BGYS politikalarında erişim haklarının yetkili kişi tarafından yapıldığı ve değiştirildiği maddesine yer verilmiştir ancak erişim haklarının kaldırılmasına yönelik bir maddeye rastlanmamıştır.

Çalışmaya katılan firma yetkilisi ve çalışanlarının kullanılan sistemler üzerindeki kimlik doğrulama bilgilerinin zor ve tahmin edilemezlik boyutunun kabul edilebilir iyi seviyede (X=3,98) olduğu ve buna ilişkin olarak kullanıcı sorumluluklarının farkında oldukları söylenebilir. Bilgi güvenliği sistemine ilişkin eğitim sektöründe yer alan gizli kimlik doğrulama bilgisinin kullanımına yönelik olarak ele aldığı politikalar değerlendirildiğinde ise, kullanıcıların kullanmış olduğu kimlik doğrulama bilgilerinin zor ve tahmin edilemez olması talimatı gereğinin parola politikası altında uygulama geliştirme standartları içerisinde bireylerin ve grupların kimlik doğrulaması işleminin desteklendiğine yönelik bir madde ile kimlik doğrulama bilgisinin önemine ilişkin bir politikanın varlığı görülmektedir. Bu durum farklı sektörlerde yer alan firma ya da kurumların kimlik doğrulama bilgisinin kullanımına ilişkin olarak kullanıcı sorumluluklarını önemsediği ifade edilebilir. Finans sektörünün BGYS politikaları kimlik doğrulama bilgilerinin kullanımından bahsetmektedir. Sağlık sektörünün BGYS politikalarında kimlik doğrulama bilgilerinin kullanımından bahsetmekte fakat kimlik doğrulama bilgilerinin zorluk derecesinden, tahmin edilmez bir kimlik doğrulama prosedürü ile ilgili bir madde yer almamaktadır. Teknoloji sektörünün BGYS politikalarında kimlik doğrulama bilgilerinin kullanımı ile ilgili bir bilgi yer almamaktadır.

Araştırma Sonuçlarına İlişkin Öneriler

Çalışanların ISO 27001 politikaları ile ilgili bilgi alabileceği ve nereden erişim sağlayacaklarının ölçüldüğü ikinci soruda *Evet* grubunda iyi düzeyde gösterilmektedir. Araştırma sonuçlarına göre ISO 27001 BGYS standardına sahip olan şirketlerde politika ile ilgili bilgiyi nereden erişim sağlayacağı tüm çalışanlar tarafından bilinmediği ortaya çıkmıştır. Bu durumda herhangi bir sorun olduğunda veya çalışanların politika ile ilgili merak ettikleri bir konuda, nasıl bir yol izlenmesi gerektiğini öğrenmek istediklerinde standardın kolay erişilebilir durumda olması önemlidir. Bu durumun çok iyi düzeyde olması beklenmektedir.

ISO 27001 BGYS standardına sahip olan şirketlerde daha yüksek düzey de olması için;

- Politika personelin istediğinde kolay ulaşabileceği bir ortamda bulundurulmalı ve sergilenmelidir. Bunun için en uygun ortam kurumun intranet sitesidir. (Eskiyörük, 2008)

- Yöneticiler çalışanlarına bu konu kapsamında belirli sürelerle hatırlatma yapılarak elektronik posta ile okunurluğunu sağlayabilir.
- BGYS adı ile masa üstüne kısa yol oluşturularak çalışanlara kolaylık sağlanabilir.
- Yeni bir çalışan işe başladığında oryantasyon sürecinde BGYS sistemi ile ilgili eğitim verilebilir.

Ayrıcalıklı erişim yapacak kullanıcıların ağda kalış süreleri ve erişebilecekleri alanların tanımlanıp kayıtlarının tutulduğunun ölçüldüğü yirmi ikinci soruda *Evet* grubunda iyi düzeyde gösterilmektedir. ISO 27001 BGYS standardına sahip olan şirketlerde bu daha yüksek düzey de olması için; şirket çalışanlarının internet kullanımları ve çeşitli uygulamaları kullanımları ağ üzerindeki hareketleri takip etmeye yönelik izleme ve loglama yapılmalıdır fakat logların sadece kayıt altına alınması tek başına yeterli olmayabilir. Bu sebeple bu verileri anlamlı hale getiren bir sisteme ihtiyaç duyulmaktadır. Sunucu tarafından tutulan erişim kayıtları bir metin editörü ile açıldığında hiçbir anlam ifade etmeyeceği gibi karışık ve düzensiz bir yapıda gözükecektir. Web kullanım madenciliği ile analiz edilerek buradaki veriler anlamlı hale gelebilmektedir. (Özseven & Düğenci, 2011). Bu yöntemle kişilerin işyerindeki çalışma işleyişinin takibi kontrollü bir şekilde gerçekleşmesi beklenmektedir.

Şirketten ayrılan kullanıcıların kullanıcı kimliklerinin kaldırılmasının ölçüldüğü on dördüncü soruda *Evet* grubu iyi düzeyde ve kullanıcı kimliklerinin periyodik olarak kontrolünün ölçüldüğü on beşinci soruda da evet grubu iyi düzeyde çıkmıştır. Kullanıcı kimliklerinin kaldırılması ve kontrolü konusunda eksikliklerin olduğu görülmüştür. Bu seviyenin çok iyi düzeyde olması için; sistem yöneticilerinin manuel olarak yaptıkları kullanıcı kaydetme ve silme, kullanıcı erişimine izin verme, erişim haklarının kaldırılması veya düzenlenmesi işlemleri zaman alabilmekte ve hataya sebep olma ihtimalini artırabilmektedir. Bu sistemlerin kontrolü için LDAP (Lightweight Directory Access Protocol- Hafif Dizin Erişim Protokolü) kullanılabilir. LDAP bir dizin servisi standardıdır.

LDAP ile geliştirilen sistem kullanıcıların ve sistemin yönetimini kolaylaştırmıştır. LDAP desteği ile servisler LDAP sunucusu üzerinden bir tane kullanıcı girişi ile kullanıcı bilgilerine erişim ve doğrulama yapma imkânı sağlar. Bu sistem ile LDAP kullanıcıları kontrol etmek için veri tabanından istekte bulunan istemcilerin yönetiminin güvenli sağlanması için kurallar oluşturulmuştur. SSO (Single Sign On) için kullanılan LDAP

kullanıcı yetki ve kontrolleri için ihtiyaç olan tanımları en esnek şekilde yapılmıştır. LDAP üç grup içinde tanımlı 9 adet görev aşağıda verilmiştir:

- Sorgulama işlemleri: arama ve karşılaştırma
- Güncelleme işlemleri: ekleme, silme, güncelleme, yeniden isimlendirme
- Kimlik doğrulama ve kontrol işlemleri: bağlanma, bağlantıyı kesme ve bağlantı iptali (Kavak & Türker, 2014).

Şirket çalışanlarının ayrıcalıklı erişim haklarının yönetimi tablosu sorularının sonuçlarında seviyeleri iyi düzeyde olduğu görülmüştür fakat BGYS belgesine sahip şirketlerde çok iyi düzeyde olması beklenmektedir. Ayrıcalıklı erişim hakkı, bir kuruluşu ayrıcalıklı erişimin yanlışlıkla veya kasıtlı olarak kötüye kullanılmasından korur (Purba & Soetomo 2018). Bu bağlamda Ayrıcalıklı erişim haklarına ilişkin yaşanan problemlerin çözümü için; ayrıcalıklı kullanıcı kimliklerine yetki geçerlilik süresi verilebilir. Yetki süresi bitmesine yakın bir zamanda, yetki veren ve yetki alan kişilere iletilmek üzere otomatik e-posta sistemi oluşturulabilir. Yetki almaya devam etmek isteyen kullanıcıların almak istediği erişim hakkı form doldurarak devam etmesi gerektiği, yetki veren kişilere de bilgi maili ile hatırlatılabilir. Alternatif olarak talep halinde (PAM) “Privileged User Management” Ayrıcalıklı Hesap Güvenliği ürünleri satın alınabilir.

Yönetim ve bilgi güvenliği biriminin kullanıcı erişim haklarının periyodik kontrolünün ölçüldüğü yirmi beşinci soruda; Evet grubun iyi düzeye olduğu görülmüştür. fakat BGYS belgesine sahip şirketlerde bu seviyenin çok iyi düzeyde olması beklenmektedir. Düzenli periyotlarla kontrollerin yapılmaması unutulduğu veya gerekli önemin verilmediği durumunu düşündürmüştür. Bu sistemin unutulması halinde kontrol eden birime hatırlatma e-postaları hazırlanabilir. Üst yönetim tarafından sistemi kontrol eden kişilerin kullanıcı erişim haklarının gözden geçirilmesi işlemlerinin düzenli gerçekleştirip gerçekleştirmediği izlenebilir. Bazı kritik sistemlerde ise Excel tablolarına verilen kişi bilgileri ve görevleri kayıt altına alınabilir, belirli periyotlarda o birimde çalışan kişinin yöneticisine yetkinin devamlılığı konusu sorgulanarak gerekli izinlerle devam edilmesi konusunda imza istenebilir. Düzenli kontroller oluşabilecek sorunların çoğunlukla önüne geçilmesi sağlar.

Şirketler hassas bilgi varlıklarını korumak için veri sızıntılarına ve siber saldırılara karşı önlem alarak kaynakların korunumunu sağlamalıdır. Kritik bilgilere ayrıcalıklı

erişimin güvenli bir şekilde sağlanması ve bu erişimin güvenli yönetilmesi, denetlenmesi önemlidir.

Bilgi güvenliğinin iyi seviyede korunmasında sızma testleri de önemli bir faktördür. Sızma testleri, saldırı olmadan önce onu engelleyecek ve ona karşı savunmak için ihtiyaçların ve gerekli önlemlerin alınmasında kullanılan önemli erken bir ikaz sistemidir. Sızma testleri belirli aralıklarla (yıl içerisinde iki ya da üç kez tekrarlanabilir) veya sistemlerin yenilenme sürecinde yapılmalıdır. Bu durumun kurumsal bilgi güvenliğini yüksek seviyede koruduğuna her zaman dikkat çekilmelidir. İç ve dış ortamların denetimi için belirli sürelerle bağımsız uzman kuruluşlarca takibi sağlanarak, kurumsal bilgi güvenliği seviyesinin güncel durumu belirlenmelidir. Bilgi güvenliği yalnızca teknoloji ile sağlanır düşüncesinden uzaklaşarak insan eğitim ve teknoloji üçgeni için yeni bir bakış açısı getirilmelidir (Vural & Sağıroğlu, 2008).

9. SONUÇ

Erişim kontrolü, bilgiyi tutarlılık ve bütünlük içinde depolayabilen ve işleyebilen sistemler oluşturmak için önemli bir güvenlik hizmetidir. Güçlü erişim kontrolü, kullanıcıların sistemdeki hareketlerinin takip edilmesine yardımcı olur ve iyi bir denetim sağlar. Bilgi güvenliği söz konusu olduğunda erişim kontrolü, kimlik doğrulama ve denetim bir arada düşünülmelidir. Bu üç yöntem arasındaki bağlılığı bilgi güvenliği araştırmacıları ve uygulayıcıları görmezden gelmiştir. Bu disiplinleri ayrı ayrı ele almak yerine, her bir yöntemin güçlü noktasını bir ara getirerek koordineli bir yaklaşıma ihtiyacımız vardır (Sandhu & Samarati, 1994). ISO 27001 BGYS erişim politikaları ile beraber bu üç faktörün etkisi artacaktır. Ayrıca insan ve eğitim faktörleri de unutulmamalıdır; şirket bilgilerinin korunmasında bilgi sistemlerini bilinçli kullanan çalışanların olumlu etkisi yadsınamaz.

Araştırma sorularımızda BGYS politikası uygulayan ve uygulamayan kurumlarda erişim kontrolünün iş gereklilikleri düzeyi, kullanıcı erişim yönetimi düzeyi, kullanıcı sorumlulukları düzeyi, sistem ve uygulama erişim kontrolü düzeyi sorgulanmıştır. Anket sonuçları ISO 27001 BGYS belgesine sahip olan şirketlerin erişim kontrol seviyelerinin çok iyi düzeyde olduğunu, ISO 27001 BGYS belgesine sahip olmayan kuruluşların şirketlerin erişim kontrol seviyelerinin kritik düzeyde olduğunu göstermiştir. BGYS'nin şirket veya kurumlarda uygulanması erişim güvenliğine ve kontrolüne olumlu yönde fayda sağladığı görülmüştür.

Şirketlerin sahip olduğu bilgi varlıklarını korunması adına ISO 27001 BGYS belgesinin alınarak uygulanması önerilmektedir. Sadece ISO 27001 BGYS belgesine sahip olmak yeterli olmadığını şirketlerin veya kurumların belirli sürelerle denetimleri gerçekleştirmeleri gerektiği unutulmamalıdır.

Araştırma İstanbul ilinde yapılmış olup, Türkiye genelinde farklı illerde benzer bir çalışmanın yapılması faydalı olabileceği düşünülmektedir. Bu çalışmada ISO 27001 BGYS içerisindeki politikalardan erişim politikası ele alınarak incelenmiştir, BGYS içerisinde yer alan diğer politika başlıklarının da uygulanabilirliği incelenebilir. Bu tarz çalışmaların bilgi güvenliği araştırmalarına katkı sağlayacağı düşünülmektedir. Bunun yanında çalışanların siber IQ'larını artırmalarını amaçlayan eğitim, veri ve siber güvenlik kavramları incelenerek bu doğrultuda bir bilinç oluşturulabilir.

KAYNAKÇA

Aktan, C. C., & Vural, İ. Y. (2005). *Bilgi çağında bilginin yönetimi*. Konya: Çizgi Kitap Evi. Erişim adresi: http://www.canaktan.org/can-aktan-kitaplar/bilgi-yonetimi.pdf

Alsultanny, Y. A. (2014). Evaluating Protesttin of Computer Network in Education Sector. In *Proceedings of the World Congress on Engineering and Computer Science* (Vol. 1).

Altun, R. (2014). *Belirli kısıtlara göre bilgi güvenliği ihlallerinin tespiti.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Bensghir, T. K. (1996). *Bilgi Teknolojileri Ve Örgütsel Değişim.* (No. 274). TODAİE.

Bingöl, U. (2010). *ISO 27001 Bilgi güvenliği yönetim sistemi otomasyonu.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Can, Ö., & Ünalir, M. O. (2010). Ontoloji Tabanlı Erişim Denetimi. *Pamukkale University Journal of Engineering Sciences*, *16*(2).

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, *9*(3), 165-174.

Çetinkaya Kılıç, M., & Gökçöl, O. (2010). Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi. 3. *Ağ ve Bilgi Güvenliği Sempozyumu*.

Çetinkaya, M. (2008). *Bilgi güvenliği yönetim sistemi alt yapısının değerlendirilmesi için bir test aracı geliştirilmesi.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Demirok, E. (2016). *Kurumsal bilgi güvenliği yönetim sistemi uygulaması; Vakıf üniversitesi örneği.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Demirtaş, H. (2013). *Bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları: Bir uygulama örneği*. (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Dinçer, Ö. (2007). Erişim Kontrol Politikası Oluşturma Kılavuzu. *TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)*.

Durna, H. U. U. (2008). İşletmelerde Rekabet Unsuru Olarak Bilgi Yönetimi. *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *1*(1), 33-40.

Ekşi, B. (2019a). Erişim Adresi: https://www.burakeksi.com/ISO-27000-ailesi-hangi-standartlardan-olusur/ Erişim tarihi: 01 Aralık 2019

Ekşi, B. (2019b). Erişim Adresi: https://www.burakeksi.com/ISO-27000-ailesi-hangi-standartlardan-olusur/ Erişim tarihi: 01 Aralık 2019

Eskiyörük, D. (2008). Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Kılavuzu. *TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)*.

GAMMASSL (2019). Erişim Adresi: http://www.gammassl.co.uk/27001/history.php Erişim tarihi: 09 Kasım 2019

Ganbat, O. (2013). *Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Gürcan, İ. A. (2014). *Assessing information security management requirements for finance sector using an Iso27001 based approach.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Haklı, T. (2012). *Bilgi güvenliği standartları ve kamu kurumları bilgi güvenliği için bir model önerisi.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

ISO (2019a). International Standart Organization. Erişim Adresi: https://ISOtc.ISO.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 Erişim tarihi: 03 Aralık 2019

ISO (2019b). International Standart Organization. The Iso Survey of Management System Standard Certifications 2018 Explanatory Note. Erişim Adresi: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 Erişim Tarihi: 01 Aralık 2019

ISO (2019c). International Standart Organization. Erişim Adresi: https://www.ISO.org/standard/73906.html Erişim tarihi: 27 Kasım 2019

ISO (2019d). International Standart Organization. Erişim Adresi: https://www.ISO.org/standard/54534.html Erişim tarihi: 30 Kasım 2019

Ivandić Vidović D., Karlović L., Ostojić A. (2011). Korporativna sigurnost, Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb

İleri, Y. Y. (2016). Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, *17*(4), 55-72.

İstanbul Valiliği (2019). Erişim Adresi: http://www.istanbul.gov.tr/nufus-bakimindan-turkiyenin-en-buyuk-kenti-istanbul Erişim tarihi: 20 Aralık 2019

Kahraman, S. (2006). *Yönetimde bilgi güvenlik sisteminin yapısı, işleyişi ve Aselsan AŞ'de uygulaması.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Kandemirli, B. M. (2012*). Bilgi teknolojileri güvenliği ve sigorta şirketinde ISO/IEC 27001 standartları çerçevesinde bilgi güvenlik yönetim sistemi uygulaması.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Kavak, İ., & Türker, G. F. (2014). LDAP ile Güvenli Kullanıcı Kontrol Sistemi. *Akademik Bilişim Konferansı*.

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

Küçük Ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri Ve Sınıflandırılması Hakkında Yönetmelik (2005, 18 Aralık). Resmî Gazete (No:25997). Erişim adresi: https://www.kosgeb.gov.tr/Content/Upload/Dosya/Mevzuat/KOBI%CC%87%E

2%80%99lerin_Tan%C4%B1m%C4%B1,_Nitelikleri_ve_S%C4%B1n%C4%B1fland%C4%B1r%C4%B1lmas%C4%B1_Hakk%C4%B1nda_Yo%CC%88netmelik.pdf Erişim tarihi: 25 Kasım 2019

KVKK (2019). Erişim Adresi: https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf Erişim tarihi: 25 Aralık 2019)

Marjanovic, M. (2017). Leaking of Confidential Personal Information. *No. 21 Int'l J. Econ. & L., 7*, 133.

Marttin, V., & Pehlivan, İ. (2010). ISO 270012005 Bilgi Güvenliği Yönetimi Standardı Ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, *1*(1), 49-56.

Mete, H. (2010). *ISO/IEC 27001 Bilgi güvenliği yönetim sistemi'nin bilgi işlem merkezlerinde uygulanması.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

MYK (2019). Erişim Adresi: https://www.myk.gov.tr/index.php/tr/ulusal-meslek-standard-ana/182 Erişim tarihi: 11 Eylül 2019

Önel, D., & Dinçkan, A. (2007). Bilgi güvenliği yönetim sistemi kurulumu. *TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü)*.

Özbilgin, İ. G., & Özlü, M. (2019) ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve Ağ Yönetimi Politikası. Erişim adresi: https://www.academia.edu/31607289/ISO_27001_Bilgi_G%C3%BCvenli%C4%9Fi_Y%C3%B6netim_Sistemi_ve_A%C4%9F_Y%C3%B6netimi_Politikas%C4%B1

Özeren, Ö., & Güngör, F. M. (2017). Ülkemizde Bilgi Güvenliği Yönetim Sistem Uygulamaları ve Yasal Şartlar. *Standart Ekonomik ve Teknik* Dergi. (1300-8366), ss.14-17 Erişim adresi: https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/7843/25072017102956-2.pdf Erişim tarihi: 25 Kasım 2019

Özgirgin, K. B., (2007), Rol Tabanlı Erişim Kontrolü, Deloitte firması. Erişim adresi: http://www.denetimnet.net/UserFiles/Documents/Makaleler/Rol-

Tabanl%C4%B1-Eri%C5%9Fim-Kontrol%C3%BC_Burak%20%C3%96zgirgin.pdf Erişim tarihi: 28 Kasım 2019

Özseven, T., & Düğenci, M. (2011). LOG Analiz: Erişim Kayıt Dosyaları Analiz Yazılımı ve GOP Üniversitesi Uygulaması. *Bilişim Teknolojileri Dergisi*, *4*(2).

Pallant, J. (2005). SPSS Survival Manual, 2nd Edn Buckingham.

Purba, A., & Soetomo, M. (2018). Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control. *ACMIT Proceedings*, *5*(1), 65-76.

Richardson, R., & Director, C. S. I. (2008). CSI computer crime and security survey. *Computer security institute*, *1*, 1-30.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE communications magazine*, *32*(9), 40-48.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *Akademik Bilişim*, *9*, 11-13.

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

Şereflişan, O. (2016). *Quantitive management of information security in organizations.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

TS ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi

TS ISO/IEC 27002:2013 Bilgi Güvenliği Teknikleri İçin Uygulama Kodu

Tuygun, M. (2018, Ocak). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Kamu Kurumlarına Uygulanabilirliğinin İncelenmesi. *5th International Management Information Systems Conference*, Gazi University, Ankara. Erişim adresi : https://imisc.figshare.com/articles/ISO_IEC_27001_Bilgi_G_venli_i_Y_netim_Sistemi nin_Kamu_Kurumlar_na_Uygulanabilirli_inin_ncelenmesi/7379612/1 Erişim tarihi: 21 Ekim 2019

TÜBİTAK (2019). Erişim Adresi: https://bilgem.tubitak.gov.tr/tr/kurumsal/bilgem-bilgi-guvenligi-politikasi Erişim tarihi: 01 Aralık 2019).

TÜRKAK (2019). Erişim Adresi: http://www.turkak.org.tr/TURKAKSITE/DuyuruDetay.aspx?ID=93 Erişim tarihi: 05 Eylül 2019).

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

Yılmaz, M. (2018). *İşletmelerde bilgi güvenliği uygulama sorunları ve çözüm önerileri; Konya örneği.* (Yüksek Lisans Tezi). Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

EKLER

Ek 1: Bilgi Sistemlerine Erişim Kontrol Anketi

BİLGİ SİSTEMLERİNE ERİŞİM KONTROL ANKETİ

Bu anket formundan elde edilecek olan bilgiler Doğuş Üniversitesi Bilgisayar Mühendisliği Bölümünde yürütülmekte olan bir Yüksek Lisans Tez çalışmasında bilimsel amaçla kullanılacaktır. Söz konusu çalışma "ISO 27001 Bilgi Güvenliği Yönetim Sistemi- Erişim Kontrol Yönetiminin Şirketlerdeki Uygulanabilirliğini" ölçmek amacı ile gerçekleştirilmektedir. Bu etkiyi ölçebilmemiz için siz değerli katılımcının yaklaşık 9-10 dakikasını alacaktır.

Vereceğiniz cevaplar doğru sonuçların elde edilebilmesi açısından oldukça önemlidir. Çalışma tamamen akademik amaç için gerçekleştirilmektedir. Katılımcıların verdikleri hiçbir bilgi bireysel veya firma nezdinde açıklanmayacaktır. Katkılarınız için teşekkür ederim.

Şirketinizin hizmet verdiği sektör nedir?

☐Adalet ve Güvenlik

☐Ağaç İşleri, Kâğıt ve Kâğıt Ürünleri

☐Bilişim Teknolojileri

☐Cam, Çimento ve Toprak

☐Çevre

☐Eğitim

☐Elektrik ve Elektronik

☐Enerji

☐Finans

☐Gıda

☐İnşaat

☐İş ve Yönetim

☐Kimya, Petrol, Lastik ve Plastik

☐Kültür, Sanat ve Tasarım

☐Maden

☐Medya, İletişim ve Yayıncılık

☐Metal

☐Otomotiv

☐Sağlık ve Sosyal Hizmetler

☐Spor ve Rekreasyon

☐Tarım, Avcılık ve Balıkçılık

☐Tekstil, Hazır Giyim, Deri

☐Ticaret (Satış ve Pazarlama)

☐Toplumsal ve Kişisel Hizmetler

☐Turizm, Konaklama, Yiyecek-İçecek Hizmetleri

☐Ulaştırma, Lojistik ve Haberleşme

Şirketinizin kuruluş yılı nedir? …….

Şirketinizdeki çalışan sayısı kaçtır?

☐ 1 – 9 kişi ☐ 10 – 49 kişi ☐ 50 - 250 kişi ☐ 251 kişi ve üzeri

Şirketinizdeki pozisyonunuz nedir?

☐Üst düzey yönetici ☐Orta düzey yönetici ☐ Çalışan

Kaç yıldır bu şirkette çalışıyorsunuz?

☐0 -1 yıl ☐2 -5 yıl ☐6 -10 yıl ☐11 yıl ve üzeri

Şirketinizde ISO 27001 "Bilgi Güvenliği Yönetim Sistemi" politikası uygulanıyor mu?

☐Evet ☐Hayır

Ek 1 (Devamı) Bilgi Sistemlerine Erişim Kontrol Anketi

		Kesinlikle	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle
1	Çalıştığım şirkette ISO 27001 "Bilgi Güvenliği Yönetim Sistemi" belgesi alınmıştır ve uygulanmaktadır	☐	☐	☐	☐	☐
2	ISO 27001 politikaları ile ilgili bilgi alabileceğim herksin erişimine açık genel olarak yayınlandığı bir yer vardır / nereden erişim sağlayacağımı biliyorum	☐	☐	☐	☐	☐
3	Şirket içerisinde bilgi güvenliği konusunda çalışan vardır	☐	☐	☐	☐	☐
4	Bilgi güvenliği politikası yönetim tarafından düzenli olarak gözden geçiriliyor	☐	☐	☐	☐	☐
5	Şirket çalışanlarının internet kullanımları ve çeşitli uygulamaları kullanımları ağ üzerindeki hareketleri takip etmeye yönelik izleme ve loglama yapılmaktadır	☐	☐	☐	☐	☐
6	Şirkette erişim yetki ve kontrol matrisi vardır	☐	☐	☐	☐	☐
7	Şirkette sadece görevimi gerçekleştirmek için gereken bilgilere erişim sağlıyorum	☐	☐	☐	☐	☐
8	Şirket sistemine uzaktan erişimin sağlanması için yetki onay süreci vardır	☐	☐	☐	☐	☐
9	Yetkisiz erişimler de dahil olmak üzere iç ağı, dış tehditlerden korumak için güvenlik önlemleri (güvenlik duvarı vb.) alınıyor	☐	☐	☐	☐	☐
10	Şirket sistemine uzaktan erişim için uyulması gerekli talimatları biliyorum	☐	☐	☐	☐	☐
11	Şirket sistemine uzaktan erişim için alınan önlemleri güvenli ve yeterli buluyorum	☐	☐	☐	☐	☐
12	Yeni bir çalışan işe başladığında kullanıcı kayıt etme işlemleri kontrollü bir şekilde gerçekleştirilir	☐	☐	☐	☐	☐
13	Şirketten ayrılan kişilerin kullanıcı kimliklerinin kaldırılmasına yönelik izlenen bir süreç vardır	☐	☐	☐	☐	☐
14	Şirketten ayrılan kullanıcıların kullanıcı kimlikleri hemen kaldırılır	☐	☐	☐	☐	☐
15	Periyodik olarak kullanıcı kimlikleri kontrol edilir	☐	☐	☐	☐	☐
16	Şirket çalışanları rollerinin gerektirdiği işlemler için sisteme erişimi sağlanır	☐	☐	☐	☐	☐
17	Kullanıcıların bilgi sistemi kullanımı ve erişim hakları yönetim tarafından belirlenir	☐	☐	☐	☐	☐
18	Bilgi sistemlerine ve hizmetlerine erişmek için kullanıcı kimliklerine verilen erişim haklarının kaydı şirket tarafından tutulur	☐	☐	☐	☐	☐
19	Şirket çalışanlarının sisteme erişimi şirkette yürütmekte oldukları görevleri doğrultusunda önceden belirlenmiş rollere göre tanımlanır	☐	☐	☐	☐	☐
20	Yetkim dışında bir yere erişmeye çalıştığımda yöneticime uyarı gider	☐	☐	☐	☐	☐

Ek 1 (Devamı) Bilgi Sistemlerine Erişim Kontrol Anketi

21	Şirket bilgi sistemlerine ayrıcalıklı erişim yapacak kullanıcılar erişim yapılacakları bilgisayarlara ait IP/MAC adreslerini bilgi işleme bildirmektedir	☐	☐	☐	☐	☐
22	Ayrıcalıklı erişim yapacak kullanıcıların ağda kalış süreleri ve erişebilecekleri alanlar tanımlanmıştır ve loglanmaktadır	☐	☐	☐	☐	☐
23	Ayrıcalıklı erişim haklarına sahip kullanıcıların yetkinlikleri, söz konusu ayrıcalıklarının görevleri ile ilişkili olup olmadığının doğrulanması için düzenli olarak gözden geçirilir	☐	☐	☐	☐	☐
24	Soru 24: Kullanıcıların kimliklerinin doğrulanması için bazı yöntemler (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılır	☐	☐	☐	☐	☐
25	Kullanıcı erişim hakları yönetim ve bilgi güvenliği birimi tarafından belirli periyotlarla kontrol edilmektedir	☐	☐	☐	☐	☐
26	Şirket içinde bir iş rolünden diğerine geçiş durumunda kullanıcı erişim hakları gözden geçirilerek yeniden tahsis edilir	☐	☐	☐	☐	☐
27	Yetki değişiklik taleplerinin hangi koşullarda ve nasıl yapılacağını biliyorum	☐	☐	☐	☐	☐
28	Hizmet veya sisteme erişim için nasıl ve kime müracaat edileceği tüm kullanıcılar tarafından bilinir	☐	☐	☐	☐	☐
29	Şirket prosedürleri gereği kullandığımız kimlik doğrulama bilgileri zor ve tahmin edilemezdir	☐	☐	☐	☐	☐
30	Görevim ile ilgili eriştiğim verilerin tümü kayıt altına alınmaktadır	☐	☐	☐	☐	☐
31	Erişilen ve kaydı tutulan veriler belirli sürelerle gözden geçirilmektedir	☐	☐	☐	☐	☐
32	Kullanıcıların erişim haklarının kontrolü örneğin; okuma, yazma, silme ve yürütme olarak IT departmanı tarafından tanımlanır	☐	☐	☐	☐	☐
33	Erişim işlemlerinin kontrollerini sağlayan IT birimi de yönetim tarafından kontrol edilir	☐	☐	☐	☐	☐
34	Kullanıcı şifrelerinin son kullanma süresi vardır	☐	☐	☐	☐	☐
35	Kullanıcıların art arda yapılan kimlik doğrulama hatasından sonra erişim kilitlenir	☐	☐	☐	☐	☐
36	Çalışanlar bilgisayarların başından kalktıklarında oturumlarını kilitlemekte ya da otomatik olarak bilgisayar oturumları kilitlenmektedir	☐	☐	☐	☐	☐
37	Şirket sistemi gereği belirli aralıkla parolamı değiştirmem bekleniyor	☐	☐	☐	☐	☐
38	Oluşturulan parolaların güvenliğini kontrol edebileceğim sistemi (Kolay -Orta- Zor) görebiliyor ve ona göre değişiklik yapabiliyorum	☐	☐	☐	☐	☐
39	Şirketim sadece zor olan parolaları kullanmama izin veriyor	☐	☐	☐	☐	☐
40	Parolamın süresi dolduğunda uyarı geliyor, erişim kısıtlanıyor ve değiştirmek zorunda kalıyorum	☐	☐	☐	☐	☐
41	Parola oluşturma talimatlarını biliyorum ve uyguluyorum	☐	☐	☐	☐	☐

Ek 2: 27000 Standart Ailesi

27000 STANDART AİLESİ

- **ISO/IEC 27006 Bilgi Güvenliği Yönetim Sistemlerinin Denetim ve Belgelendirmesini Sağlayan Kuruluşlar İçin Gereklilikler**

  Akredite olarak BGYS bağımsız denetim ve belgelendirme hizmeti sağlayan firmalar için kılavuz bilgi sağlar (Ekşi, 2019a).

- **ISO/IEC 27007 Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Rehber**

  BGYS denetimi için yönergelerdir. Denetim amaçları şunlardır: BGYS denetim programını yönetmek, Bir BGYS denetiminin yapılması, BGYS denetçilerinin yönetimidir (Şereflişan, 2016).

- **ISO/IEC 27008 Bilgi Güvenliği Kontrollerine İlişkin Denetçiler İçin Talimatlar**

  ISO / IEC 27007'nin teknik tamamlayıcısı bu kılavuz tarafından sağlanmıştır. Amacı bilgi güvenliği kontrollerini denetlemektir. Bu, risk odaklı bir yaklaşımla seçilen BGYS kontrolleri ile ilgili tüm denetçiler için bir rehberdir. Gerekli "BGYS kontrollerinin" ne kadarının uygulandığı ve nasıl doğrulanacağına dair rehberlik eder (Şereflişan, 2016).

- **ISO/IEC 27010 Sektörler ve Kurumlar Arası İletişim İçin Bilgi Güvenliği Yönetimi**

  Sektörler arası ve kurumlar arası iletişim için bilgi güvenliği olayları riskleri, kontrolleri ile ilgili bir rehberdir. Bu rehber endüstriler veya uluslar arasında özellikle de kritik alt yapıya sahip olanlar arasında sınırları belirler (Şereflişan, 2016).

- **ISO/IEC 27011 ISO / IEC 27002 Dayalı Telekomünikasyon Kuruluşlar İçin Bilgi Güvenliği Yönetim Kuralları**

  Bu uygulama rehberi telekom endüstrisi içindir. ITU-T ve ISO / IEC JTC1 / SC27 tarafından geliştirilmiştir (Şereflişan, 2016). Telekomünikasyon organizasyonlarında bilgi güvenliği kontrollerinin uygulanmasını destekleyen kılavuzlar tanımlamaktadır.

- **ISO/IEC 27013 ISO O/IEC 27001 ve ISO/IEC 20000-1 Entegre Uygulanması Konusunda Rehberlik**

  Bu standart, hem ISO / IEC 27001 (BGYS) hem de ISO / IEC 20000-1: 2011'in birlikte uygulanması için rehberlik eder. Birbirlerinin amaçlarını tamamlayan ve destekleyen iki yönetim sistemidir (Şereflişan, 2016).

- **ISO/IEC 27014 Bilgi Güvenliğinin Yönetişimi**

  Bu standart, bilgi güvenliğinin yönetilmesi ile ilgili kavram ve ilkeler için bir rehberdir ve her tür ve boyuttaki kuruluşa uygulanabilir. İyi bir bilgi güvenliği sürecinin yönetimi, iş stratejileri ve amaçları ile bilgi güvenliğinin kuruma uyumunu sağlar. Açık verimli ve en iyi şekilde uygulanmasını sağlar (Şereflişan, 2016).

- **ISO/IEC 27015 Finansal Hizmetler İçin Bilgi Güvenliği Yönetimi Kılavuzu**

  Bu rehber sektöre özgü bir rehberdir ve finansal hizmet kuruluşlarına (bankalar, kredi kartı şirketleri vb.) ISO / IEC 27000 standartlarını kullanarak BGYS uygulamalarında yardımcı olmaktadır (Şereflişan, 2016).

- **ISO/IEC 27031 İş Sürekliliği İçin Bilgi ve İletişim Teknolojisi Hazırlığı İçin Yönergeler**

  ISO / IEC 27031, iş sürekliliğini sağlamada bilgi ve iletişim teknolojisinin arkasındaki kavram ve ilkelere rehberlik eder. Herhangi bir organizasyon için bir yapı veya çerçeve önerir. Kuruluşun BGYS 'sinin bir parçası olarak bilgi iletişim teknolojileri hazırlığının iyileştirilmesine yönelik tüm ilgili yönergeleri belirler (Şereflişan, 2016).

- **ISO/IEC 27032 Siber Güvenlik Kuralları**

  Siber güvenlik durumunun iyileştirilmesi konusunda rehberdir. Diğer güvenlik alanlarındaki faaliyetlerin; bilgi güvenliği, ağ güvenliği, internet güvenliği ve kritik bilgi altyapısının korunmasını amaçlar.

- **ISO/IEC 27033 Ağ Güvenliği**

  ISO / IEC 18028 ağ güvenlik standardından türetilen çok parçalı bir standarttır. ISO / IEC 27002'de sunulan ağ güvenliği kontrollerinin uygulanması hakkında ayrıntılı rehberlik eder. Ağa bağlı cihazların güvenliği için geçerlidir ve iletişim

bağlantıları yoluyla aktarılan bilgilerin güvenliğinin yanı sıra, güvenlik, ağ uygulamaları ve ağ kullanıcılarının yönetimini kapsar (Şereflişan, 2016).

- **ISO/IEC 27034 Uygulama Güvenliği**

  Uygulama güvenliğini belirleyen, tasarlayan, tedarik eden, uygulayan ve kullananlara bilgi güvenliğinin nasıl uygulanacağına rehberlik sağlar. Gerekli güvenlik düzeyi, organizasyonu BGYS'nin amacıdır.

- **ISO/IEC 27035 Bilgi Güvenliği Olay Yönetimi**

  Olayları etkin bir şekilde yönetmek, olayları tanımlamak ve müdahale etmek, olumsuz etkileri en aza indirmek, adli delil toplamak (uygun olan yerlerde) ve zaman zaman, iyileştirerek BGYS' de iyileştirmelere yol açma konusunda düzenleyici kontrolleri içerir (Şereflişan, 2016).

- **ISO/IEC 27036 Tedarikçi İlişkileri İçin Bilgi Güvenliği**

  Tedarikçilerden hizmet ve mal teminindeki bilgi risklerinin değerlendirilmesi ve sağlanması konusunda kılavuzluk sağlar. Burada kastedilen perakendecilikten ya da bilgiye dayalı ürünlerden ziyade firmadan firmaya ilişkilerdir (Şereflişan, 2016).

- **ISO/IEC 27037 Dijital Kanıtların Tespiti, Toplanması ve Edinilmesi ve Saklanması**

  Dijital delillerin ele alınmasında delil değeri olabilecek potansiyel dijital delillerin tanımlanması, toplanması ve saklanması gibi belirli faaliyetler için kılavuz sağlar. Dijital kanıt işleme sürecinde karşılaşılan genel durumlarla ilgili bireylere rehberlik eder ve kuruluşlara disiplin prosedürlerinde ve yetki alanları arasındaki potansiyel dijital kanıtların alışverişinde yardımcı olur (Şereflişan, 2016).

- **ISO/IEC 27038 Dijital Redaksiyon İçin Şartname**

  Dijital belgeler üzerinde dijital redaksiyon gerçekleştirmek için tekniklerin özelliklerini belirtir. Ayrıca yazılımın yeniden düzenlenmesi için gereklilikleri de belirtir (Şereflişan, 2016).

- **ISO/IEC 27040 Depolama Güvenliği**

  Veri depolama güvenliğinin planlanması, tasarlanması, belgelendirilmesi ve uygulanması için kanıtlanmış ve tutarlı bir yaklaşım kullanarak kuruluşların uygun bir risk azaltma düzeyini nasıl tanımlayabilecekleri hakkında ayrıntılı teknik rehberlik sunar. Depolama güvenliği, depolandığı bilgilerin korunması (güvenliği) ve depolama ile ilişkili iletişim bağlantılarında aktarılan bilgilerin güvenliği için geçerlidir. Depolama güvenliği, cihazların ve medyanın güvenliğini, cihazlarla ve medyayla ilgili yönetim faaliyetlerinin güvenliğini, uygulamaların ve hizmetlerin güvenliğini ve cihazların ve medyanın kullanım ömrü boyunca ve kullanımdan sonra son kullanıcılarla ilgili güvenliği içerir (Şereflişan, 2016).

- **ISO 27790 Sağlık Bilişimi- Belge Kayıt Çerçevesi**

  Sağlıkta Bilgi Güvenliği Yönetimi ile ilgili kılavuzluk eder, 27002 kullanılarak sağlık sektöründe bilgi güvenliğinin sağlanması ile ilgili rehber sunar (Ekşi, 2019b).

ÖZGEÇMİŞ

Adı Soyadı	: Kübra AKTAŞ
Doğum Yeri ve Yılı	: Ankara, 1989
E-posta	: kubra06@gmail.com

Eğitim:

Yüksek Lisans	: Doğuş Üniversitesi – Bilgisayar Mühendisliği – Yüksek Lisans (2016 -2020)
Lisans	: Ahmet Yesevi Üniversitesi – Bilgisayar ve Öğretim Teknolojileri Öğretmenliği (2010 – 2015)
Ön lisans	: Hacettepe Üniversitesi MYO – Bilgisayar Teknolojileri ve Programlama (2007 – 2009)
Lise	: Yunus Emre Anadolu Kız Meslek Lisesi – Bilgisayar Bölümü (2003 – 2007)

İş Tecrübeleri:

Türkiye Teknoloji Takımı Vakfı / Eğitim Uzmanı

Ataşehir Metin Sabancı Spastik Çocuklar Merkezi / Bilgisayar Öğretmeni

Hekimzade Sağlıklı Yaşam Merkezi Bilgi İşlem / Bilgi Teknolojileri Uzm. Yardımcısı

Keops Yapı Mimarlık Bilgi İşlem / Bilgi Teknolojileri Uzm. Yardımcısı

Ümraniye Hüseyin Tolgacan Sipahi İÖO / Bilgisayar Öğretmeni

Sertifikalar: ISO 27001:2013 Bilinçlendirme ve İç Tetkikçi