
GAZİ ÜNİVERSİTESİ
Gazi
1926

ISO27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ STANDARDININ KAMU KURUMLARINA UYGULANABİLİRLİĞİNİN ARAŞTIRILMASI: ANKARA İLİ ÖRNEĞİ

MEHMET TUYGUN

YÜKSEK LİSANS TEZİ
BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2019

Mehmet TUYGUN tarafından hazırlanan "ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Dr. Öğr. Üyesi Hüseyin ÇAKIR

Gazi Eğitim Fakültesi Bil. ve Öğr. Tek. Eğitimi, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.....

Başkan: Prof. Dr. Şeref SAĞIROĞLU

Bilgisayar Mühendisliği, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.....

Üye: Doç. Dr. Olgun DEĞİRMENCİ

Hukuk, TOOB ETU Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.....

Tez Savunma Tarihi: 20/06/2019

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

.....

Doç. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

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

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

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

Mehmet TUYGUN

20/06/2019

ISO27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ STANDARDININ KAMU KURUMLARINA UYGULANABİLİRLİĞİNİN ARAŞTIRILMASI: ANKARA İLİ ÖRNEĞİ

(Yüksek Lisans Tezi)

Mehmet TUYGUN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2019

ÖZET

Bu araştırma ISO27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyon sürecinin tamamlamış kamu kurumlarında kurum personelinin sistem hakkındaki düşüncelerinin incelenmesi amaçlanmıştır. Bu sebeple araştırma kapsamında, "Yönetim Kadrosu", "BGYS Ekip Üyeleri", "Kurum Teknik Personeli" ve "Kurum Personeli" gibi dört farklı odak grup üzerinde ilgili gruplar için hazırlanmış farklı anketler uygulanmıştır. Hazırlanan anketlerde 5'li likert ölçeği kullanılmıştır. Likert tipi ölçek sorularında güvenilirlik analizi uygulanmıştır. Yapılan ön çalışmanın analizleri sonucunda anketin güvenilirlik katsayısının kabul edilebilir düzeyde olduğu görülmüştür. Elde edilen verilerde odak gruplarının görüşlerinin belirlenmesi amacıyla frekans ve yüzdelik dağılımları belirlenerek yorumlanmıştır. Elde edilen veriler ışığında, yönetim kadrosunun ISO27001 sertifikasyon sürecini olumlu karşıladığı, kurumsal süreçlerin ve bilgi güvenliğinin sağlanması açısından olumlu katkı sağladığı yönünde görüş birliği olduğu görülmüştür. Diğer taraftan BGYS ekip üyelerinin, ISO27001 süreçlerinin etkin bir şekilde yönetilebilmesi için gereken teknik yeterlilik, eğitim ve sayısal çokluk noktasında takviye ihtiyaçları olduğu yönünde görüş bildirdikleri görülmüştür. Teknik ekip üyelerinin ise ISO27001 süreçlerinin işlerini kolaylaştırdığı ve etkin çalışma yürütülmesine katkı sağladığı yönünde olumlu görüş bildirdikleri fakat teknik yeterlilikler ve sayısal yeterlilik konusunda görüş birliği olmadığı görülmüştür. Kurum personelinin ise ISO27001 kapsamında alınan farkındalık eğitimlerini faydalı olduğu ve BGYS süreçlerinin kurumsal bilgi güvenliği açısından gerekli olduğu yönünde olumlu görüş bildirdikleri görülmüştür.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	ISO27001, BGYS, bilgi güvenliği, bilgi güvenliği yönetim sistemi, bilgi güvenliği yönetim sistemi standardı
Sayfa Adedi	:	100
Danışman	:	Dr. Öğr. Üyesi Hüseyin ÇAKIR

INVESTIGATION OF THE IMPLEMENTATION OF ISO27001 INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD ON PUBLIC INSTITUTIONS: CASE OF ANKARA PROVINCE, TURKEY

(M. Sc. Thesis)

Mehmet TUYGUN

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

June 2019

ABSTRACT

The aim of this research is to examine the opinions of the personnel of the institution in the public institutions that have completed the ISO27001 Information Security Management System certification process. For this reason, in the scope of the research, different questionnaires were prepared for the related groups on four different focus groups such as “Management Staff”, “ISMS Team Members”, ”Institution Technical Staff”, ”Institution Staff”. The 5-point Likert scale was used in the surveys. Reliability analysis was applied in Likert type scale questions. As a result of the analysis of the preliminary study, it was found that the reliability coefficient of the questionnaire was acceptable. In order to determine the opinions of the focus groups, frequency and percentage distributions were determined and interpreted. In light of the data obtained, it is seen that the management team has a positive attitude towards the ISO27001 certification process and in terms of ensuring institutional processes and information security. On the other hand, it has been observed that ISMS team members have expressed their opinion on the need for technical qualification, training and numerical multiplicity in order to manage the ISO27001 processes effectively. It was observed that the technical team members gave a positive opinion that the ISO27001 processes facilitated their work and contributed to the effective execution of the work, but there was no consensus on technical qualifications and numerical competence. It has been observed that the staff of the institution have been positive about the awareness trainings taken within the scope of ISO27001 and that ISMS processes are required for enterprise information security.

Science Code	:	92403
Key Words	:	ISO27001, ISMS, information security, information security management, information security management system
Page Number	:	100
Supervisor	:	Dr. Hüseyin ÇAKIR

TEŞEKKÜR

Öncelikle benimle çalışmayı kabul ederek çalışmalarım boyunca değerli katkılarını, yardımlarını esirgemeyen, tecrübesini ve ilmini sabırla ve cömertçe aktarmaya çalışan, en yoğun zamanlarında bile vakit ayırmak için elinden geleni esirgemeyen değerli tez danışmanım Dr. Öğr. Üyesi Hüseyin ÇAKIR'a; benim bu günlere gelmeme vesile olan, hiçbir zaman benden hem maddi hem de manevi desteklerini esirgemeyen, annem Meryem TUYGUN ve babam Ahmet TUYGUN'a teşekkür ederim.

Son olarak; başarılarımda mutlaka önemli ölçüde katkısı olan, desteğini hiçbir zaman esirgemeyen, çalışmalarım sırasında büyük fedakârlıklar gösteren, hayat arkadaşım, ilham kaynağım, canım eşim Şermin TUYGUN ile kuzularım Cansel Berrin TUYGUN, Ahsen Berra TUYGUN'a da sevgilerimi ve şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı kısaltmalar, açıklamaları ile birlikte sunulmuştur.

Kısaltmalar	Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
COBIT	Bilgi ve İlgili Teknoloji Kontrol Hedefleri
DSS	Veri Güvenliği Standardı
HIPAA	Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
ISO	Uluslararası Standart Organizasyonu
ISO27001	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
ISO27005	ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi Standardı
ITIL	Bilgi Teknolojileri Altyapı Kütüphanesi
PCI	Ödeme Kartı Endüstrisi
TÜRKAK	Türk Akreditasyon Kurumu

1. GİRİŞ

Son yıllarda elektronik sistemlerin günlük yaşantının ve iş hayatının vazgeçilmez bir parçası haline gelmiştir. Sunulan kurumsal hizmetlerin ve kişisel bilgilerin bu sistemler üzerinde paylaşımı, bilgiye erişim yöntemlerinde gelişmeler, bu sistemler üzerinde bulunan zafiyetlerin kötü niyetli saldırıların odağı haline gelmesine sebep olmuştur. Kötü niyetli saldırılar sonucunda kişisel ve kurumsal veri kayıplarının her geçen gün artıyor olması bilgi güvenliğinin öneminin artmasındaki en büyük etkenler arasında yer almaktadır.

Kurumsal veya kişisel bilgi varlıklarına yapılan saldırılar ile birlikte gerek kişisel gerekse kurumsal bilgi güvenliğine verilen önem artmıştır ve yeni yaklaşımların ve bilgi güvenliği standartlarının kurumlar bünyesinde benimsenmesine ve uygulanmasına sebep olmuştur.

Kurumsal bilgi güvenliği, bilginin üretilmesi, işlenmesi, erişimi ve saklanması aşamalarının her birinde sağlanmak zorundadır. Bunun için kurumlar bünyesinde kullanılan veya geliştirilen yazılımlar, donanımsal sistemler ve bilgi güvenliğinin vazgeçilmez bir parçası olan insan kaynakları dikkate alınmalıdır. Kurumsal bilgi varlıklarının korunmaya çalışıldığı bilgi güvenliği yaklaşımlarında güvenlik zincirinin en zayıf halkasının her zaman insanlar olduğu kabul edilmiştir [1]. Bunun sebebi, kurumsal sistemlerde uygulanan birçok teknik veya teknik olmayan güvenlik önlemleri saldırganlar tarafından insanlar kullanılarak çeşitli yöntemlerle aşılabilmektedir [2].

Bilgi güvenliğinin sağlanabilmesi amacıyla, kurumların kendi ihtiyaçları ve süreçleri doğrultusunda bir dizi güvenlik politikalarını ve prosedürlerini belirlemesi ve uygulanması gerekmektedir [3]. Bu politikalar, kurumsal faaliyetlerin gözden geçirilmesi, sistemlere erişimlerin izlenmesi, değişiklik kayıtlarının tutularak gerekli değerlendirmelerin yapılması, silme yetkisinin kısıtlanması gibi bazı kullanıcı işlemlerine indirgenebilmektedir [4].

En temel ifadesiyle bilgi güvenliği, kurumsal bilgi güvenliği risklerini tanımlamak ve bu risklerin etkilerinin kabul edilebilir seviyelere indirgenebilmesi amacıyla yürütülen süreçlerdir. Bu bağlamda, bir BGYS'nin benimsenmesi bir kurum için stratejik bir karar olmalıdır, çünkü BGYS'nin tasarımı ve uygulanması, kurumsal ihtiyaçlar ve amaçlar,

güvenlik gereksinimleri, kullanılan süreçler kurumun büyüklüğü ve yapısı ile doğrudan ilgilidir [3].

Bilgi güvenliği kurumun faaliyetlerini desteklemede çok önemli bir rol oynadığından, bilgi güvenliği konusundaki yönetişimi düzenleyen bir standart veya ölçüte sahip olmak gerekmektedir. Bilgi güvenliği uygulamalarını standartlaştırmak ve düzene koymak için, Dünya üzerinde gerek devlet eliyle enstitüler kurularak gerekse özel sektörde organizasyonlar eliyle bilgi güvenliği uygulamalarını, süreçlerini ve prosedürlerini "bilgi teknolojisi sistemlerini ve bilgilerini korumak için" çeşitli standartlar geliştirilmiştir [5].

Bu standartlardan birisi olan ISO27001 standardı dünya üzerinde bilgi güvenliği alanından oluşturulmuş birçok standart içerisinde geçerliliği olması ve sektör bağımsız yapısıyla her türlü kurum veya kuruluş üzerinde uygulanabilir esnek yapıda olması sebebiyle her geçen gün birçok alanda zorunlu hale getirilmeye başlanan bir standarttır. ISO27001, kurum süreçlerine uygun bir şekilde belirlenmiş bir takım kontroller yardımıyla, bilgi güvenliğinin etkin bir şekilde yönetebileceği ve etkinliğinin ölçebileceği bir yaklaşım sunmaktadır [6].

Türkiye'de ise siber güvenlik ve bilgi güvenliği alanlarında yapılan çalışmalar kapsamında yayınlanan "2016 – 2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile hız kazanmıştır. Bu çalışmalar kapsamında özellikle kamu kurumların bilgi güvenliği yönetim sistemlerinin kurulması ve kurulan bilgi güvenliği yönetim sistemlerinin ISO27001 sertifikası ile sürdürülebilir ve sürekli geliştirilebilir dinamik bir yapıya kavuşturulması istenmiştir. Özellikle kamu kurumları arasında iletişimin sağlandığı, güvenli hat olarak tabir edilen KamuNet ağının kurulması çalışmalarında tüm kamu kurumlarına ISO27001 kurulması zorunlu hale getirilmiştir [7].

1.1. Araştırmanın Amacı

Kamu kurumlarına getirilen BGYS kurma ve bunu ISO27001 standardı ile belgelendirme zorunluluğunun getirilmesi ile Türkiye'de bulunan kamu kurumlarının ISO27001 sertifikasının alınması ve işletilmesi sürecinde ISO27001 Bilgi Güvenliği Yönetim Sisteminin kamu kurumlarına uygulanabilirliğinin araştırılması amaçlanmıştır. Bu amaç kapsamında belirlenmiş olan alt amaçlar ise şunlardır.

ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğine ilişkin;

1. ISO/IEC sertifikasyon sürecinin tamamlamış ve aktif BGYS'ye sahip olan kamu kurumlarında görevli yönetim kademesinde olan kişilerin görüşleri nelerdir?

2. Kurumsal bilgi güvenliği yönetim sisteminin kurulumu ve etkin bir şekilde yönetiminden sorumlu olan ve üst yönetim tarafından görevlendirilmiş kamu kurumlarında görevli BGYS ekip üyelerinin görüşleri nelerdir?

3. ISO27001 sahibi kamu kurumlarında görevli BGYS ekip üyeliği dışında, bilgi güvenliğinden dolaylı olarak sorumlu olan diğer teknik personelin görüşleri nelerdir?

4. ISO27001 sertifikasyon sürecini tamamlamış ve etkin bir şekilde BGYS yürütülen kamu kurumlarında görevli ve teknik olmayan personelin görüşleri nelerdir?

1.2. Araştırmanın Önemi

Kurumsal bir BGYS kurmak, kurulan sitemin sürekliliğini sağlamak, sürekli izlemek ve aksayan yönlerini tespit ederek iyileştirmeler yapmak, bilgi güvenliği farkındalığı oluşturmak, kısacası canlı bir BGYS kurmak ISO27001 belgesi sahibi olmanın olmazsa olmaz şartlarındandır. Bu çalışmanın, kamu kurumlarının kurmuş oldukları BGYS'lerin etkinlik seviyelerine, sahiplenme durumlarına ve teknik yeterliliklerine ışık tutması açısından önemli olduğu düşünülmektedir.

1.3. Araştırmadaki Varsayımlar

Araştırmaya katılım sağlayan kamu kurumlarında görevli personellerin, kurumlarında ISO27001 süreçlerinin gerekliliklerini yerine getirdikleri varsayılır. Örneğin; Üst yönetim ve yönetim kademesinin kendisinden beklenen sahiplenme ve göstermesi gereken iradeyi ortaya koyduğu, BGYS ekip üyelerinin ISO27001 uyum süreçlerinde etkin olarak rol aldıkları ve kurum personeli ve teknik ekiplerin ISO27001 farkındalık eğitimlerine katılım sağlayarak belirli bir olgunluk seviyesine ulaştıkları varsayılır.

1.4. Araştırmanın Kapsam ve Sınırlılıkları

Araştırmanın kapsamı olarak Ankara'da yer alan merkez teşkilatı ve merkez teşkilatına bağlı olan kamu kurumları belirlenmiştir. Araştırma konusunun kurumsal bilgi güvenliği yönetim sistemleri ve çeşitli açılardan kurum personellerine yöneltilen sorulardan oluşması sebebiyle, kamu kurumlarının birçoğundan anket uygulanması talebine olumsuz geri dönüşler alınmıştır. Bu sebeple uygulanan anket çalışması izin alınan 6 adet kamu kurumu ile isimlerinin gizili tutulması şartıyla sınırlıdır. Bahse konu kamu kurumlarında görevli personellerin anket uygulamasına tam anlamıyla katılım sağlamadıkları görülmüştür.

2. KURAMSAL ÇERÇEVE

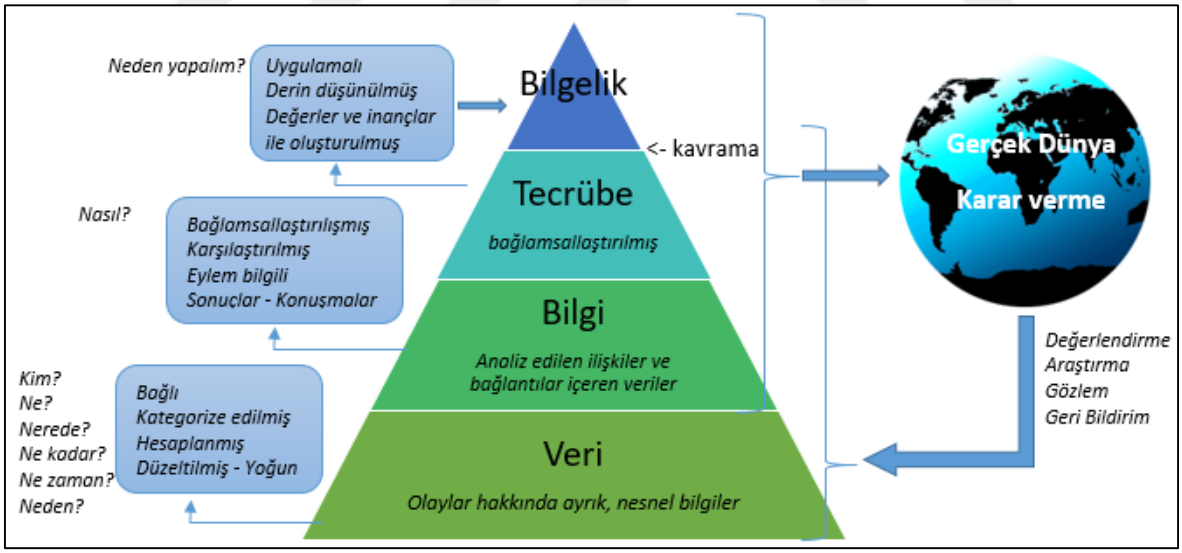
Bu bölümde araştırma konusu olan bilgi güvenliği, BGYS ve ISO27001 hakkında bilinmesi gereken temel kavramlara ve ilgili süreçlere yer verilmiştir.

2.1. Bilgi Güvenliği Kavramları

Bu bölümde bilgi güvenliği ve bileşenleri konusunda temel seviyede bilgi sahibi olmak için gerekli olan tanımlara yer verilmiştir. Bilgi güvenliğinin sağlanabilmesi için öncelikle bilgi kavramı ve bu bilginin güvenliğinin sağlanabilmesi ile doğrudan ilişkili olan temel unsurları göz önünde bulundurmak gerekmektedir.

2.1.1. Bilgi

Bilgi, sözcük anlamı incelendiğinde; İnsan aklının erebileceği olgu seviyesi, zekâ çalışması sonucu ortaya çıkan düşünce, zihnin kavradığı düşünceler bütünü ve verilerden elde edilen anlam şeklinde tanımlandığı görülmektedir [8].



Şekil 2.1. Veriden bilgeliğe geçiş [9]

Bilgi, Dünyada algının temel yapı taşlarından biridir. Zamanın başlangıcından beri insan, çevresini etkili bir şekilde yorumlamıştır ve bilgiyi anlama ve kullanma yeteneği, insanın en büyük başarısı olarak görülebilir [10]. Bilgi, zamanın başlangıcından bu yana kullanılmaya çeşitli yöntemlere aktarılmaya devam etmektedir. İlk başlarda sözlü aktarımlar, hikâyeler,

masallar kullanılmıştır. Sonraki süreçte eğitim kurumları ve kitaplar bilginin aktarılmasında önemli rol üstlenmişlerdir. Son dönemde ise bilgi teknolojilerindeki gelişmelerle birlikte bilginin üretilmesi, yönetilmesi ve paylaşımı oldukça kolaylaşmıştır. Elektronik ortamlarda bilginin işlenmesi, taşınması ve saklanması istenilen zamanda istenilen yerden bilgiye erişimine imkân tanımaktadır.

Bilgi(Information), gelecekte alınması muhtemel kararların şekillenmesinde ve güncel kararların alınmasında kullanılan, belli bir düzende işlenmiş veri(data) olarak da tanımlanabilir. Eğer veri davranışları etkiliyorsa bilgi olarak ifade edilebilir. Bilgi her zaman anlamlı olmayabilir. Belli bir kararın alınmasında önemli bir rol oynayan bilgi, başka bir kararın alınması noktasında sadece bir veri(data) olabilir. Bu noktada bilginin güvenilirliği, konu ile ne kadar ilgili olduğu, eksiksiz olması, erişim kolaylığı, ihtiyaçları karşılaması gibi ölçütler o bilgisinin kalitesini belirlemektedir [11].

Sahip olunan bilginin önemi her geçen gün artmaya devam etmektedir. Sahibi olunan daha fazla bilgi, etrafınızdaki dünyaya daha iyi uyum sağlamanız açısından önemli bir araçtır. Kurum veya kuruluşlarda, bilgi genellikle bir şirketin sahip olduğu en önemli varlıklardan biridir. Bilgiyi aynı zamanda şirketleri birbirinden ayıran ve birinin diğerinden daha başarılı olmasına yardımcı olan kaldıraç gibi de düşünebiliriz [6].

2.1.2. Bilgi güvenliği

Bilgi, Çizelge 2.1'deki gibi herkesin görebileceği sınıflandırılmamış bilgiden, yalnızca en güvenilir kişilerin erişebildiği gizli bilgiye doğru ilerleyecek şekilde farklı kategorilere ayrılabilir. Bilginin önemine, hassasiyetine ve çalınmaya veya kötüye kullanıma karşı savunmasızlığına bağlı olarak, farklı yollarla erişimi kontrol etmek amacıyla korunmaya ihtiyaç duyulur.

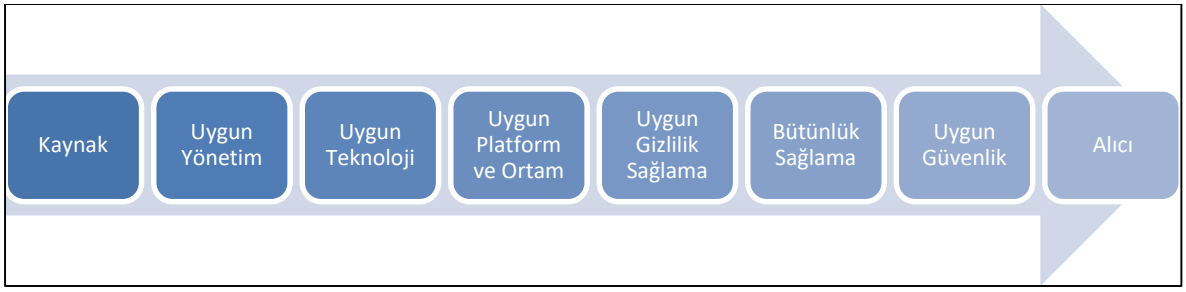
Bilgi varlıklarının nasıl güvence altına alacağınızı anlamak için önce bunun gerçekten ne anlama geldiğini bilmeniz gerekir. En kaba tabirle, kötü niyetlilerin erişilmemesi gereken bilgilere erişimini engellemek olarak ifade edilebilir. Fakat bilgi yalnızca yararlı olduğunu biliyorsanız ve ona erişebiliyorsanız kullanışlıdır. Sadece gizliliği korumak güvenliliğin temin edildiği anlamı taşımamaktadır. Bir kurumun bilgilerini güvenceye alması için soruna insan, süreç ve teknoloji perspektifinden yaklaşması gerekir.

Çizelge 2.1 Bilgi gizlilik sınıfları [12]

Sınıf	**Açıklama**
Çok Gizli	Elde edildiğinde, itibar, yasal durum, stratejik planlar veya ticari durum üzerinde ciddi bir etki yaratabilecek gizli bilgilerdir. Sadece bilmesi gereken kişilerin erişimine açıktır.
Gizli	Gelecekteki ürünler, planlar ve süreçler hakkında gizli bilgiler ve yeni düşünceleri içeren bilgilerdir. Yeni planları geliştiren tüm işbirliği ekibinin bu belgelere erişimi hakkı vardır.
Tescilli	Mevcut ürünler, planlar, süreçler ve diğer özel konular hakkında bilgileri ifade eder. Tüm profesyonel personelin erişimi hakkı vardır.
Kontrollü	Genişletilmiş şirket içinde kontrollü kullanım için hafif duyarlı bilgileri ifade eder. Ancak halka açık bilgi değildir.
Halka Açık	Şirket içerisinde ve dışında serbestçe paylaşılmak istenen bilgileri ifade eder.

En basit anlamda, bir teknoloji onu yönetmesi ve sürdürmesi için bir kişiye ihtiyaç duyar ve bu kişinin bunu yaparken tanımlanmış süreçleri izlemesi gerekir. Bu, bilgi güvenliğinin sistematik hale getirilmesinin bir parçasıdır [12].

Bilgi güvenliği, sınıflandırılmış kurumsal bilgi varlıklarının, izinsiz kullanımı, erişimi, açığa çıkarılması, zarar verilmesi, değiştirilmesi veya yok edilmesi gibi durumlara karşı korunmasıdır.



Şekil 2.2. Bilgi güvenliği altyapı gereksinimleri

Bilgi güvenliği, kurumsal bilgi güvenliği risklerini tanımlamak ve bu risklerin etkilerinin kabul edilebilir seviyelere indirgenebilmesi amacıyla yürütülen süreçlerdir [3].

2.1.3. Bilgi güvenliğinin temel unsurları

Bilgi güvenliğinin her ne kadar "gizlilik", "bütünlük" ve "erişilebilirlik" gibi üç temel kavram üzerine kurulu olduğu söyleniyor olsa da bu üç unsurun yanı sıra birçok unsur olduğu da görülmüştür. Bu unsurlar Şekil 2.3'de görülmektedir.

Şekil 2.3. Bilgi güvenliği unsurları[13]

Gizlilik

Bilgi varlığına yetkili olanların dışında erişimin engellenmesini ifade etmektedir. Bilgi hem bilgisayar sistemleri üzerinde iken, hem sistemler arasında iletilirken hem de saklandıkları yerde yetkili olmayan kişilerin erişimlerine kapalı olmalıdır.

Bütünlük

Veri bütünlüğü olarak ta ifade edilebilir. Bilgi varlığının içeriğinin olması gerektiği gibi korunması ya da değiştirilmemiş olarak muhafaza edilmesinin sağlanması anlamına

gelmektedir. Bu amaçla verilerin erişim kontrollerinin ve yedekleme işlemlerinin belirli aralıklarla gerçekleştirilmesi gerekmektedir.

Erişilebilirlik

Bilgi varlığına ihtiyaç duyulduğu anda, yetkisi olan kişilerin ulaşabilmesinin sağlanması anlamına gelmektedir. Diğer bir deyişle bilgi sistemlerinin kendilerinden beklenen işi sürekli ve tam olarak yerine getirmelerinin sağlanmasıdır [14].

Bilgi güvenliği yönetimi ise, bilginin korunması ile güvenli erişimi arasında kurulan bir denge hali olarak nitelendirilebilir. Bunu sağlamak için işletmeler üst yönetim tarafından desteklenen bir çerçeve dâhilinde, çeşitli politikalarla sınırları çizilen bir güvenlik yönetimi yaparlar.

2.2. Bilgi Güvenliği Yönetim Sistemi

Kurumlarda bilgi güvenliğinin sağlanması sadece teknoloji ile mümkün değildir. Teknolojik çözümlerin yeterli olacağı algısı tamamen yanlış bir algıdır. Bilgi güvenliği teknoloji, süreç ve insan faktörlerinin beraber değerlendirilmesi gereken ve bu üç faktöre göre oluşturulması gereken bir kavramdır. Bilgi güvenliği yönetim sistemi bu noktada teknoloji süreç insan faktörlerine göre oluşturulmuş bir sistemdir.

Bilgi Güvenliği Yönetim Sistemi; bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkelerini sağlamak üzere sistemli, kuralları konulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetimce kabul edilmiş ve desteklenmiş, uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününe denmektedir. Başka bir değişle Bilgi Güvenliği Yönetim Sistemi (BGYS), kuruluşların güvenlik olaylarını bütüncül ve sistematik bir biçimde yönetmelerini sağlayan bir çerçevedir de diyebiliriz.

Aynı zamanda BGYS, kuruluşun bilgi güvenliğini yönetmeye, izlemeye, denetlemeye ve geliştirmeye yardımcı olan süreçler, teknoloji ve insanlar sistemidir. BGYS bünyesinde, insan kaynaklarını, kurumsal politikaları, prosedürleri ve aynı zamanda teknolojinin bir parçası olarak yazılımsal ve donanımsal varlıkları içerir. BGYS'yi uygulayan bir kurum, bilgi varlıklarını çeşitli bilgi güvenliği tehditlerine karşı korunması sağlanabilir. Diğer taraftan BGYS'nin önemli bir parçası risk yönetimidir. Risk yönetimi, riskin belirlenmesi, değerlendirilmesi ve sonrasında işlenerek kabul edilebilir bir düzeye düşürmek veya tamamen ortadan kaldırmak için adımlar atılması sürecidir. Risk değerlendirmesi yapılırken, gizlilik, bütünlük ve erişilebilirlik temel ilkeler doğrultusunda ilgili potansiyel riskler

belirlenmeli ve zayıf yönleri tanımlanmalıdır. BGYS'nin doğru bir şekilde yönetilmesi kurumun, riskleri doğru bir şekilde azaltmasına ve yönetmek için uygun kontrolü tanımasına yardımcı olacaktır. Aynı zamanda felaket / olay sırasında maddi kayıpları ve etkileri en aza indirecektir. Ayrıca, kurumun bilgi güvenliği yönetimine bakış açısını da önemli ölçüde geliştirebilir. Kuruluşun tüm bileşenlerinde bilgi güvenliği bilincini artırabilir [15].

2.2.1. Bilgi güvenliği yönetim sistemi çeşitleri

Dünyada ve Türkiye'de genel kabul görmüş, gerek genel seviyede gerekse spesifik alanlarda bilgi güvenliğinin sağlanması amacıyla çeşitli bilgi güvenliği yönetim sistemleri bulunmaktadır. Bunlardan en çok kabul görmüş ve yaygın bir şekilde uygulananlar şunlardır:

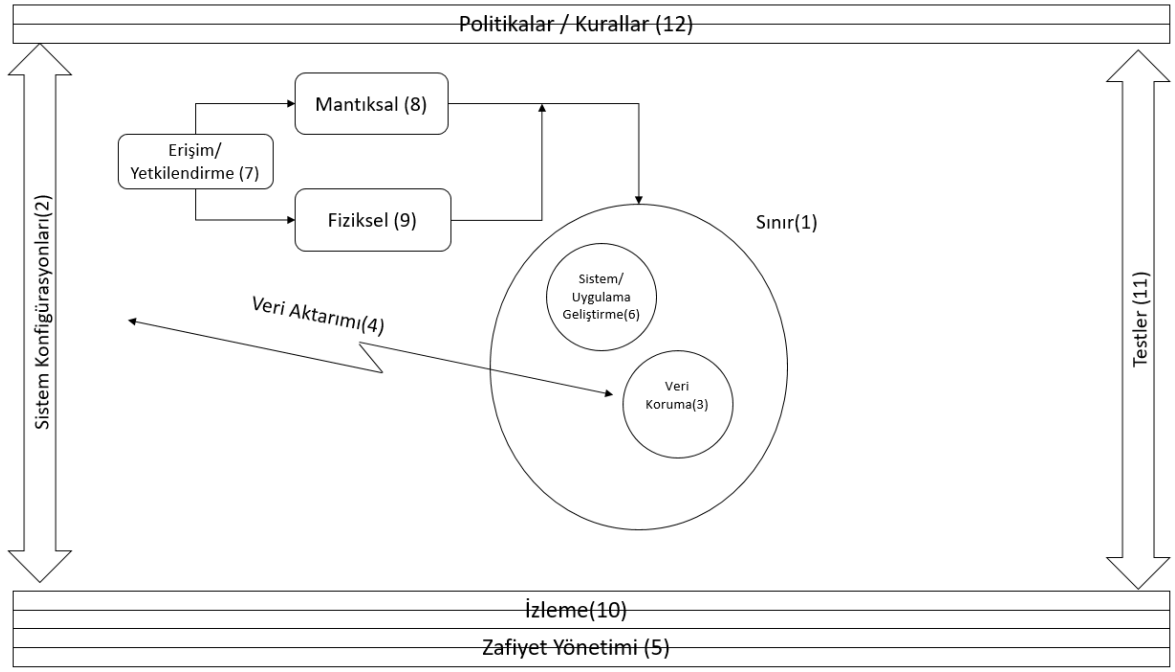
- PCI-DSS
- COBIT
- ITIL
- HIPAA
- ISO27001

Türkiye'de en çok kullanılan ve bu tezin ana konusuna temel teşkil eden ISO27001 standardına ise daha geniş bir şekilde yer verilecektir.

PCI-DSS

Kart ile yapılan ödemelerin güvenliğinin sağlanması, sahtecilik ve dolandırıcılık işlemlerine karşı etkin bir koruma geliştirmek amacıyla geliştirilmiştir. Dünya genelinde kabul görmüş standartlar arasında yer almaktadır. Payment Card Data Security Standard ifadesinin kısaltması PCI DSS'in Türkçe karşılığı Ödeme Kartları Endüstrisi Veri Güvenliğidir.

PCI-DSS 6 ana kriterden oluşmaktadır. Bu ana kriterler altında yer alan 12 adet alt kritere bağlı 200 den fazla kontrol bulunmaktadır. PCI-DSS standardı kapsamına kart üreten tüm bankalar, kartlarla ödeme kabul eden tüm satış noktaları ve alışveriş esnasında verilerin iletilmesini sağlayan ve saklayan tüm hizmet sağlayıcılar girmektedir [16]. PCI-DSS uyumluluğu sayesinde ilgili taraflar gerekli önlemlerini alarak güvenlik ihlali risklerini en aza indireceklerdir. Tüm tarafların güvenli bir şekilde işlem yapmasını sağlar, Müşteri ilişkilerinin gelişmesine katkı sağlar, kar oranlarını olumlu yönde etkiler, Yüksek para cezalarının alınmasını engellemeye yardımcı olur. Kuruluşun imajını olumlu yönde etkiler.



Şekil 2.4. PCI-DSS'ye sistemik bir bakış [17]

COBIT

COBIT, bilgi ve ilgili bilgi teknolojisinin (BT) yönetimi ve kontrolü ihtiyacını ele almaktadır. Control Objectives for Information and related Technology kelimelerinin kısaltmasından oluşmaktadır. ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından bilgi teknolojileri yönetiminde ulaşılması gereken hedefleri ortaya koymak amacıyla geliştirilmiş ve ilk sürümü 1996 yılında yayınlanmıştır [18].

Tüm işletmeye yönelik kurumsal bilgi ve teknolojinin yönetimi için bir çerçevedir. COBIT, en uygun yönetim sistemini oluşturmak ve sürdürmek için bileşenleri ve tasarım faktörlerini tanımlar. Bilginin ve bilgi teknolojilerinin etkin bir şekilde yönetilmesinin, organizasyonların başarısı ve hayatta kalması için kritik öneme sahip olduğunu kabul eder [19].

ITIL

Dünya çapındaki kuruluşlar tarafından kullanılan en iyi uygulamalardan derlenerek oluşturulmuş bir kütüphane olarak ifade edilmektedir. İsmini Bilgi Teknolojileri Altyapısı Kütüphanesi anlamına gelen Information Technology Infrastructure Library kelimelerinin

ilk harflerinden almaktadır. Kurumsal yapılar için mükemmel BT hizmetleri sunmak üzere süreçlere ve süreçlerin birlikte nasıl çalıştığına odaklandı. Bu nedenle, BT Hizmetlerini planlama, izleme ve kontrol etmeyi destekleyen en iyi uygulamalar olarak da adlandırılır.

ITIL, BT yönetimi ve olay yönetimi, problem yönetimi, değişiklik yönetimi, konfigürasyon yönetimi ve kullanılabilirlik yönetimi gibi BT operasyonlarının net bir görüntüsünü sunmaktadır [20].

1980'li yıllarda, İngiltere Ticaret Bakanlığı tarafından BT altyapı ve hizmet süreçlerinin standartlaştırılması çalışmaları sonucu ortaya çıkmıştır. ITIL'in en son sürümü, 2007'de yayınlanan ITIL 3.0'dır. ITIL günümüzde tüm dünyada kabul gören standart haline gelmiştir.

ITIL yaşam döngüsünün aşamaları şunlardır:

1) Hizmet stratejisi
2) Hizmet tasarımı
3) Hizmet geçişi
4) Servis işlemi
5) Sürekli hizmet geliştirme

ITIL yaşam döngüsünün her bir aşaması, Şekil 3.2'de de görüldüğü gibi, kendi içinde farklı süreçler barındırmaktadır. Bu süreçler içerisinde, verilmesi planlanan hizmetlerin hangi şartlar altında oluşması gerektiği, verilmesi planlanan hizmetin proje yönetimi açısından nasıl değerlendirilerek tüm aşamalarının nasıl planlanacağı gibi çalışmalara yer verilmektedir. Aynı zamanda fikir aşamasında olan bir hizmetin canlı hayata nasıl aktarılabileceği, hizmetin yönetim aşamaları ve gözden geçirme sıklıklarının belirlenmesi bu süreçlerin kapsamında yer alan çalışmalar arasında yer almaktadır.

HIPAA

HIPAA, hastanın tıbbi gizliliğini korumak amacıyla elektronik tıbbi kayıtların güvenliğini sağlamak için kurallar ve düzenlemeler sağlayan bir Amerika Birleşik Devletleri mevzuatıdır. Mevzuat birden fazla başlıktan oluşmaktadır. Bununla birlikte, kanunun II. Başlığı, sağlık kayıtlarının işlemlerinin korunmasına ve yayılmasına ilişkin düzenlemelerle ilgilidir. II. Başlık altında, HIPAA'nın Gizlilik Kuralı, hastaların mahremiyetini korumak için ulusal standartları tanımlamaktadır. Aslında, kural sağlık uzmanlarının, hastanın tıbbi

verilerini, ilgili hastadan açıkça yazılı izin alınmaksızın üçüncü şahıslara vermesini yasaklar.

Şekil 2.5. HIPAA uyumluluk süreçleri [21]

Ayrıca, hastanın tıbbi kayıtlarına meşru bir sebep olmaksızın erişilmesine, hastanın mahremiyetini ihlal ettiğinden izin verilmemelidir. Bununla birlikte, mevcut tıbbi tedaviyi daha da ilerletmek için hastanın depolanan tıbbi verilerine erişimin gerekli olduğu durumlarda, HIPAA, tıp uzmanlarının bu kayıtlara erişmesine izin verir. Son olarak, yasada belirtilen gizlilik kurallarını ihlal eden cezalar ve para cezaları açıklanmaktadır [21]. HIPAA uyum süreçleri ilgili görsel Şekil 2.5'de verilmiştir.

2.2.2. ISO/IEC 27001:2013 bilgi güvenliği yönetim sistemi

Bu bölümde bilgi güvenliğinin ve bununla birlikte iş sürekliliğinin sağlanması aşamasında, insanları süreçleri ve bilgi varlıklarını içeren yönetim sistemi olan ISO27001 hakkında detaylı bilgilere yer verilmiştir.

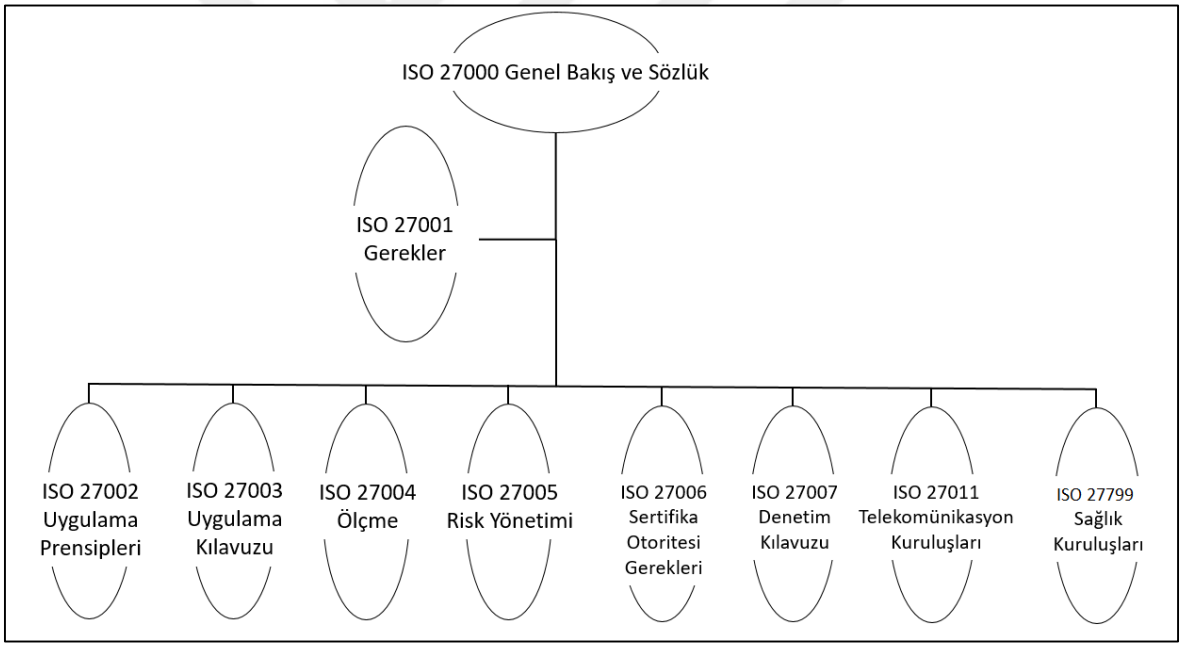
ISO hakkında

ISO (International Organization for Standardization), 25 ülkeden delegeler, 1946 yılında Londra'daki İnşaat Mühendisleri Enstitüsünde buluşması ile başladı ve endüstriyel koordinasyonu ve endüstriyel standartların birleştirilmesini kolaylaştırmak için yeni bir uluslararası organizasyon oluşturulmasına karar verildi. 23 Şubat 1947'de ISO yeni organizasyonu resmen faaliyete geçti.

Kuruluşundan bu yana, teknoloji ve imalatın neredeyse tüm yönlerini kapsayan 21616'dan fazla Uluslararası Standart yayımlandı. Günümüzde ise, standartların geliştirilmesi amacıyla 163 ülkeden ve 779 teknik makamdan üyeleri bulunmaktadır [22].

ISO/IEC 27000 ailesi

ISO / IEC 27000 ailesi standartları, kuruluşların bilgi varlıklarını güvence altına almalarına amacıyla oluşturulmuştur. Bu standartlar ailesini kullanmak, kuruluşların mali bilgiler, fikri mülkiyet hakları, çalışan bilgileri veya üçüncü kişilere ait bilgiler gibi varlıkların güvenliğinin yönetilmesine yardımcı olmaktadır. ISO27001 bilgi güvenliği yönetim sistemi bu ailenin en iyi bilinen standardıdır. ISO / IEC 27000 standart ailesi arasındaki ilişki Şekil 2.6'da gösterilmiştir.



Şekil 2.6. TS ISO/IEC 27000 BGYS ailesi standartları arasındaki ilişkiler.

Bu standart ailesinin bileşenleri kısaca;

- ISO/IEC 27001: Bir bilgi güvenliği yönetim sisteminin dokümantasyonunun yapılarak, tüm süreçlerin planlanması, uygulanması kontrol edilmesi ve önlem alınması süreçlerini kapsar.
- ISO/IEC 27002: Bilgi güvenliği kontrollerinin uygulanması esnasında kılavuz olarak kullanılır.
- ISO/IEC 27003: ISO / IEC 27001'de belirtilen bilgi güvenliği yönetim sistemi gereklilikleri hakkında rehberlik etmekte ve bunlarla ilgili öneriler, olasılıklar ve izinler sunmaktadır. Bilgi güvenliğinin tüm yönleriyle ilgili genel rehberlik sağlamak

bu belgenin amacı değildir [23].

- ISO/IEC 27004: İzleme, ölçüm, analiz ve değerlendirme gerekliliklerini yerine getirmek için bilgi güvenliği performansını ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmelerine yardımcı olmak amacıyla hazırlanmıştır [24].
- ISO/IEC 27005: Bu belge ISO / IEC 27001'de belirtilen genel kavramları desteklemektedir ve bir risk yönetimi yaklaşımına dayalı bilgi güvenliğinin tatmin edici bir şekilde uygulanmasına yardımcı olmak için tasarlanmıştır [22].
- ISO/IEC 27006: Bu Uluslararası Standart, ISO / IEC 17021-1 ve ISO / IEC 27001 içerisinde yer alan gereksinimlere ek olarak, bir bilgi güvenliği yönetim sisteminin (BGYS) denetim ve belgelendirmesini sağlayan kuruluşlar için gereksinimleri belirler ve rehberlik sağlar [25].
- ISO/IEC 27007: Bu belge, ISO 19011: 2011'deki kılavuza ek olarak, bilgi güvenliği yönetim sistemi (BGYS) denetim programının yönetilmesi, denetimlerin yapılması ve BGYS denetçilerinin yeterliliği hakkında rehberlik sağlar [26].
- ISO/IEC 27011: Bu standardın amacı, telekomünikasyon alanında faaliyet gösteren organizasyonlarda bilgi güvenliği kontrollerinin uygulanmasını destekleyen kılavuzlar tanımlamaktır.
- ISO/IEC 27799: Bu standardın amacı, sağlık alanında faaliyet gösteren organizasyonlarda bilgi güvenliği kontrollerinin uygulanmasını destekleyen kılavuzlar tanımlamaktır.

Şeklinde ifade edilebilir.

ISO/IEC 27001:2013

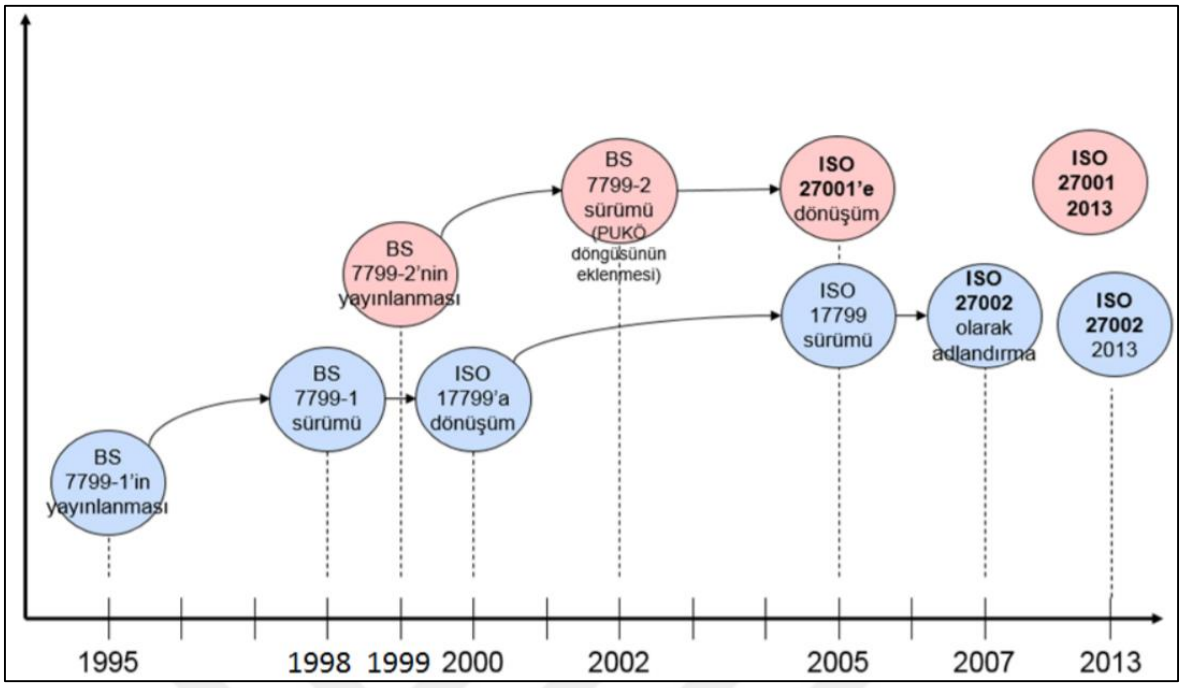
İlk olarak 1993 yılında Uygulama Kuralları (CoP), adı altında İngiltere'de faaliyet gösteren bir grup önde gelen uluslararası şirket ve kuruluşun desteğiyle Ticaret ve Sanayi Bakanlığı tarafından geliştirilmiştir. Daha sonra CoP uygulamalarının İngiliz Standartları Enstitüsü (BSI) tarafından derlenmesi ile birlikte 1995 yılında, BS779 adı altında Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı yayınlanmıştır. Uygulama Kurallarının (CoP) iki temel amacı vardır:

• Kuruluşların güvenlik yönetimi etkili bir şekilde uygulaması, geliştirmesi ve ölçmesi için ortak bir temel sağlamak ve

• Şirketler arasında güvenli ticareti sağlamak.

Bu iki temel amaç güvenlik olaylarının etkilerini mümkün olan en aza indirmek ve iş sürekliliğini sağlamaktır [27].

Standardın ikinci kısmı BS7799–2, 1999 yılında yayınlanmıştır. Daha sonra 2000, BS7799-1 adı altında küçük düzeltmelerden sonra ISO tarafından ISO/IEC–17799 adıyla yayınlanmış ve Dünya genelinde kabul edilen bir standart haline gelmiştir.



Şekil 2.7. ISO27001 tarihçesi [28]

BSI ise 2002 yılında BS–7799–2 adı altında ilk sürüm üzerinde düzenleme ve eklemeler yaparak İngiliz standardı olarak yayınlamıştır. 2005 yılında ise ISO ISO/IEC– 17799 standardının üzerinde düzenlemeler yapılmış ISO/IEC–17799:2005 adıyla yeniden yayınlamıştır [28]. Aynı zamanda BS7792-2 standardının Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) komiteleri tarafından revize edilmesinin ardından ISO / IEC 27001:2005 adını almıştır. Standardın en son sürümü olan ISO / IEC 27001:2013 ise 2013 yılının Eylül ayında yayınlanmış ve hala günümüzde kullanılmaya devam edilmektedir.

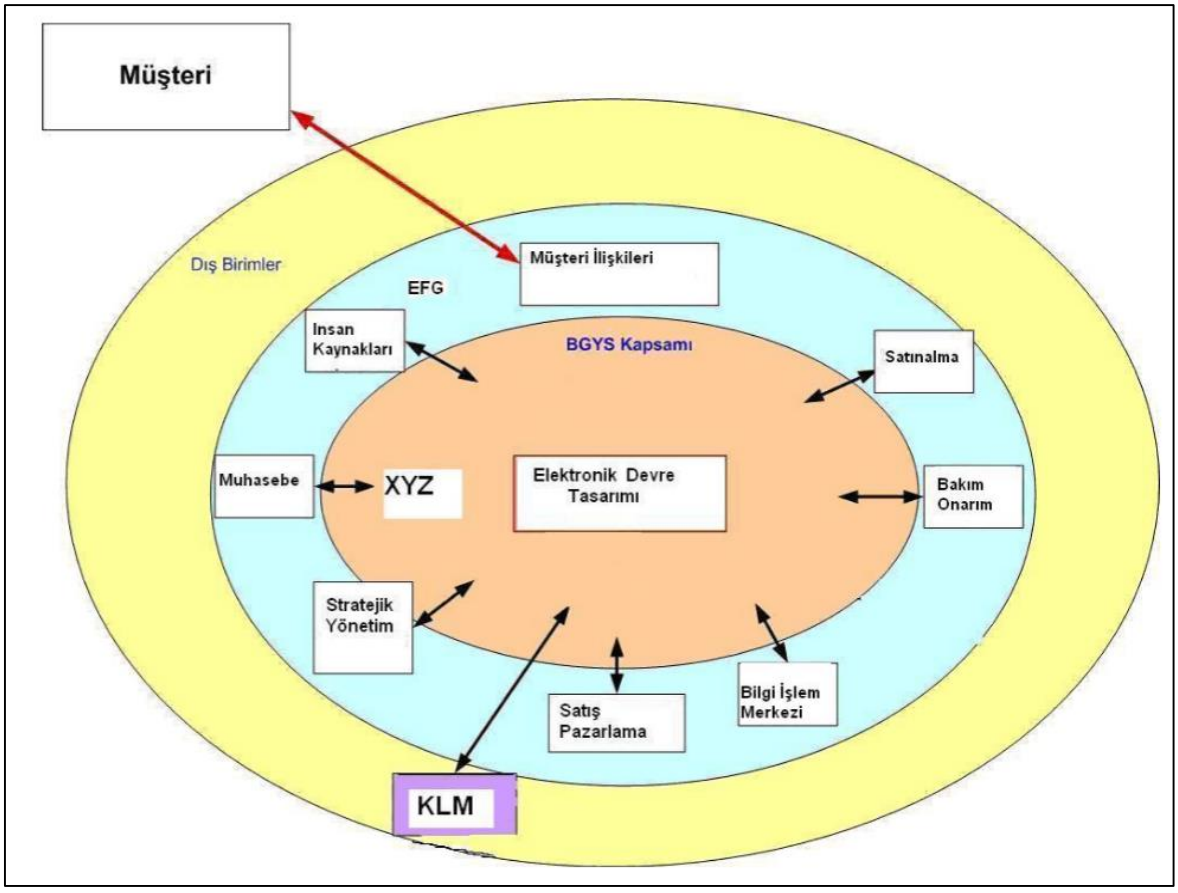
ISO27001 kavramları

Bu bölümde ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardı, uyum süreçlerinde anlaşılması gereken veya kullanılan temel kavramlara yer verilmiştir.

Kapsam

BGYS kurulumunda ilk olarak kapsam ve uygulanacak sınırlar belirlenmelidir. Şekil 2.8'de gösterildiği gibi, BGYS'nin kapsamı, kurumun tamamı olabileceği gibi, sadece bir bölümü de olabilir. BGYS kurulumu için bu kapsamın eksiksiz ve doğru bir biçimde tanımlaması çok önemlidir. Kapsam, idarecilerin niyeti ve kurumun bilgi güvenliği hedefleri dikkate

alınarak hazırlanır. Bu konuda standardın kendisinin doğrudan bir yönlendirmesi söz konusu değildir. Kapsam kurumsal anlamda farklılıklar gösterebileceğinden dışarda bırakılanların hususların hangi sebeplerle dışarıda bırakıldıklarını kurumun sağlam gerekçelerle açıklayabiliyor olması beklenir. Kapsam belirlendikten sonra mutlaka dokümante edilerek yayınlanmalı ve mutlaka üst yönetim tarafından onaylanmalıdır.

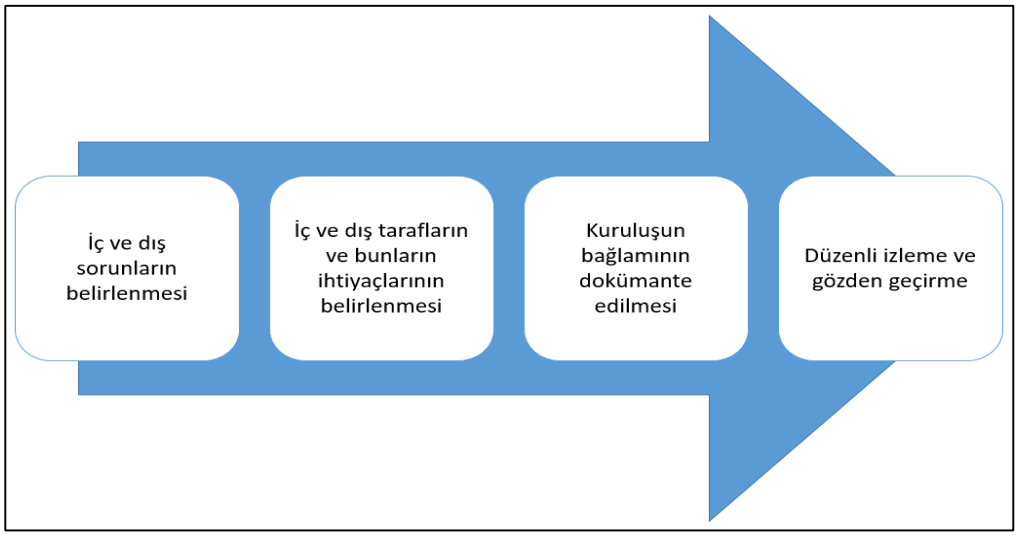


Şekil 2.8. XYZ firmasının EFG yerleşkesi KLM süreçleri BGYS kapsamı örneği [29]

Bağlam

Kurumun, amaçlarına uygun bir bilgi güvenliği yönetim sisteminin, amaçlanan sonuçlarına ulaşmasını etkileyen iç ve dış hususları eksiksiz bir şekilde belirlemesi gerekmektedir. Aynı zamanda bu hususların yasal, düzenleyici gereksinimler ve sözleşmeden doğan yükümlülüklerini içeren bilgi güvenliği açısından gereksinimleri de tanımlanmalıdır.

İç ve dış hususlar belirlenirken kurumun etkileyebileceği veya etkilenebileceği çevresel faktörlerin göz önünde bulundurulması gerekmektedir. Bağlam belirlenirken Şekil 2.9'daki adımların izlenmesi gerekmektedir.



Şekil 2.9. Bağlam belirleme adımları [30]

Liderlik

Bilgi güvenliğinin kurulumu ve etkin bir şekilde yönetilmesi, üst yönetimin sorumluluğudur. Üst yönetim, BGYS'nin ayrılmaz bir parçasıdır ve kurumun bilgi güvenliği stratejilerinin ve hedeflerinin sürdürülmesinin ve iyileştirilmesinin sağlanmasından doğrudan sorumludur. Bilgi güvenliği şartları ile kurum süreçlerindeki uyumun temininden sorumludur. BGYS'nin yürütülmesi esnasında ihtiyaç duyulan kaynakların teminini sağlamalıdır. Sürekli iyileştirmelerin desteklenmesi gerekmektedir.

Bilgi güvenliği politikası

Kurum tarafından belirlenen kapsam ve bağlama bağlı olarak kurumun bilgi güvenliği politikası belirlenir. Belirlenen BGYS politikası, bilgi güvenliğinin hedeflerini ortaya koymak için bir çerçeve çizmeli, iş ve yasal ya da düzenleyici gereksinimleri ve sözleşmeye ilişkin güvenlik yükümlülüklerini dikkate almalıdır. Aynı zamanda belirlenen politika bilgi güvenliği ile ilgili uygulanabilir şartların karşılanmasına ve sürekli iyileştirilmesine dair bir taahhüt içermelidir. Bilgi güvenliği politikası, yazılı olarak mevcut olmalı, kurum içerisinde duyurulmuş olmalı ve uygun olan ilgili taraflarca dilendiği zaman erişilebilir olmalıdır.

Bilgi güvenliği olayı

Bilgi güvenliği olayı; kurum bünyesinde bulunan bir hizmetin, sistemin ya da bir ağın kurum güvenlik politikasında olası bir bozulma, ya da koruyucu unsurlarda arızalanma veya güvenliği tehlikeye düşürebilecek önceden tanımlanmış bir oluşumdur.

Risk

Bilgi güvenliğinin sağlanması ve etkili bir bilgi güvenliği yönetim sistemi kurulmasında en önemli konuların başında bilgi güvenliği risklerinin belirlenmesi ve risk analizi konuları gelmektedir.

Bilgi güvenliği çerçevesinde risk; kurum tarafından belirlenen kapsam dâhilinde bulunan bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik unsurlarının tamamı veya herhangi birini tehlikeye düşürebilme olasılığı bulunan olaylara verilen isimdir. Diğer bir değişle; kurulması amaçlanan BGYS işletim sürecinde karşılaşılabilecek belirsizlikler olarak ifade edilebilir. Bu sebeple kurumla bilgi güvenliği risklerini belirlerken gizlilik, bütünlük ve erişilebilirlik unsurlarını göz önünde bulundurmalı ve bu risk değerlendirme işlemlerini bu üç unsur için ayrı ayrı hesaplamalıdır [31].

Risklerin ISO27001 standardının 2005 versiyonunda net bir şekilde zafiyetlerin ve tehditlerin varlıklarla ilişkilendirilmesi yani varlık tabanlı bir risk analizi yapılması açık bir şekilde ifade edilirken standardın 2013 versiyonunda bu zorunluluk kaldırılmış ve kurum metodoloji seçme konusunda daha esnek bırakılmıştır. Risk metodolojilerinin işletilmesinde referans olarak ISO 31000 standardı referans olarak gösterilmektedir. Bu referans incelendiğinde ise süreçlere de riskler atanması yönünde tavsiyeler içerdiği görülmektedir. Süreç tabanlı risk işleme yöntemini izlemek isteyen kurumların yapması gereken; kurumsal süreçleri, hizmet ve servislerinin belirlemek ver varlıklarla süreçler arasındaki ilişkiden yola çıkarak ISO31000 de tanımlanan süreç tabanlı risk analizi işlemlerini gerçekleştirmektir.

Uygulanabilirlik bildirgesi

Uygulanabilirlik bildirgesi, standartta yer alan adıyla EK-A olarak bilinen kontrol listesinde yer alan maddelerden hangilerinin dâhil edildiği veya dışarıda bırakıldığı, dâhil edilme veya dışarda bırakılma nedenleri ve bu nedenlerin açıklamasını içermektedir. Risk işleme ile ilgili alınan kararlar için temel teşkil eder [32].

Tanımlanan güvenlik gerekliliklerine dayanarak, kuruluşun güvenlik gereksinimlerine uygunluğu sağlayan güvenlik kontrollerini oluşturmak için gereklidir. Güvenlik kontrolleri kurulmasında kullanılan ana belgeler standart ISO/IEC 27002'dir. Bu standart, ISO27001’in Ek-A listesinde yer alan güvenlik kontrollerinin nasıl uygulanacağıyla ilgili yönergeleri ve

tavsiyeleri içerir. ISO27001 standardının EK-A listesi bilgi güvenliği alanındaki kuruluşların genel gereksinimlerini ve hedeflerini kapsayan 114 güvenlik kontrolünden oluşan bir kontrol setinden oluşmaktadır ve ISO / IEC 27002 standardı da bu kontrolleri faaliyet gösterdikleri alanlara göre 14 ana gruba ayırır. Kuruluşların ve kuruluş tarafından kullanılan sistemlerin ve teknolojilerin belirlenen güvenlik gereksinimlerine dayanarak, kuruluşta uygulanması gereken 114 güvenlik kontrolü belirlenmiştir. Tüm süreç uygulanabilirlik beyanı ile belgelenmiştir [33].

İç tetkik

Kurumların kurmuş oldukları BGYS'nin gerekliliklerinin yerine getirilip getirilmediği, ne kadar aktif olduğunu, etkin olarak kullanılıp kullanılmadığını ve eksik veya hatalı yönlerini belirlemek amacıyla, kurum dışı bağımsız bir denetçiye veya kurum içi personel ile gerçekleştirdikleri denetimler ve uygulamalar bütünüdür. Asıl denetim olan belgelendirme denetimi yapılmadan önce de kurumunun belgelendirmeye ne kadar hazır olup olmadığı konusunda da kurumun durumunu belirlemek için önemli bir fırsattır [34].

Denetim

Türkiye'de belgelendirme denetimleri TSE ve akredite olmuş bazı özel kuruluşlar yapılabilmektedir. Bir firmanın ISO belgesi verebilmesi, yetkili makamlar tarafından belge verme konusunda akredite edilmiş olmasına bağlıdır. Türkiye'de tüm kurumlara akreditasyon verme yetkisi kamu kurumu olan TÜRKAK'tadır. TÜRKAK'ın verilerine göre 2019 yılı Ocak ayı itibariyle ISO27001 belgesi verme konusunda akredite edilmiş kurum sayısı 36'dır [35]. TURKAK ise akreditasyon faaliyetlerinde uluslararası akreditasyon birliklerince hazırlanmış kılavuz dokümanları dikkate almaktadır ve uluslararası akreditasyon kuruluşu olan European Co-operation for Accreditation – EA'nın üyesidir.

Denetimler, bağımsız denetim firmaları adına bağımsız denetçiler tarafından gerçekleştirilmektedir. ISO27001 denetimi gerçekleştirecek olan kişilerin dünyada geçerliliği olan sertifikalara sahip olmaları beklenmektedir. Eğitim konusunda yetkili eğitim kurumları tarafından verilen baş denetçi eğitimlerinin ardından, IRCA tarafından yapılan sınav sonucunda verilen ISO27001 LA (Lead Auditor) sertifikası ile kişiler, firmalarda bilgi güvenliği yönetim sistemi denetimi yapma hakkına sahip olabilirler [36].

Denetim sonrası verilen sertifikanın geçerlilik süresi 3 yıldır. İlk olarak yapılan belgelendirme denetiminden sonra, kurulan BGYS'nin varlığını, devamlılığını ve etkinliğini kontrol etmek amacıyla 2. ve 3. yıllarda gözetim denetimi yapılır.

ISO27001 gereksinim ve süreçleri

Bu bölümde ISO27001 standardizasyon süreçlerinin eksiksiz bir şekilde tamamlanması ve kurulan BGYS'nin etkin bir şekilde yürütülebilmesi amacıyla belirlenmiş adımlara ve süreçlere yer verilmiştir.

Kapsam ve bağlamın belirlenmesi

Bir kurumun bağlamının ve kapsamının belirlenmesi ISO27001'de yapılması zorunlu olan işlemlerden bir tanesidir. Standardın 4. Maddesinde bir kuruluşun bilgi güvenliği yapılanmasını ve yönetim planlamasını etkileyebilecek iç ve dış hususları belirlemesi gerektiği ifade edilir.

Bağlam ve kapsamın belirlenmesi aşamasında, kurumdaki çeşitli unsurların etkilerini tanımlamanız ve bu unsurların bilgi güvenliği yönetim sistemi, kurumun hedefleri, amaçları ve kültürü, süreçleri, kurum yapısının büyüklüğü, paydaşları vb. açısından kuruma etkilerinin belirlenmesi gerektiği anlamına gelmektedir.

Standart, kurumun bağlamı ve kapsamının belirlenmesi gerektiğini söyler fakat bazı temel hususlar dışında tam olarak nasıl olacağı konusunda bilgi vermemektedir. Bahsi geçen temel hususlar şu şekilde belirtilebilir;

İç ve dış hususlar

İç ve dış hususları belirlerken dikkatli olunması gerekir. Aksi halde belirlenen hususlar ya gereğinden fazla kapsamlı ya da genel resmi çizemeyecek kadar dar kapsamlı olabilir. Bu madde ile ilgili çalışma yapılırken bilgi güvenliğini etkileyebilecek hususların göz önünde bulundurulması gerekir.

Bir kurumun iç bağlamı BGYS'yi kurmak istediği ortamdır. İç bağlam bilgiye doğrudan veya dolaylı olarak erişebilen, üreten ve yöneten tarafları içerebilir. Dış bağlamın belirlenmesi için sosyal, ekonomik, teknolojik, çevresel, hukuksal vb. çevreden gelen

sorunlar göz önünde bulundurulabilir [37].

BGYS ile ilgili taraflar

BGYS kurulumunda özellikle bilgi güvenliği ile ilgili tarafların belirlenerek bu tarafların bilgi güvenliği gereksinimlerinin iyi tanımlanması gerekmektedir. İlgili tarafların bu gereksinimleri yasal ve sözleşmeden doğan hükümleri kapsıyor olabilir. Bu taraflar kurumsal bilgi varlıklarını doğrudan etkiliyor olabilirler [38].

Dokümantasyon

Bahsi geçen tüm iç dış huşular ve bunlara bağlı olarak oluşturulan kapsamın dokümante edilmesi gerektiği standartta belirtilmiştir. Belgelendirme kuruluşlar tarafından denetim esnasında; denetilen kurum ve belgelendirilecek bölüm hakkında bilgi sahibi olmak amacıyla ilk talep edilen dokümanlardır.

Oluşturulan bu dokümanlar düzenli aralıklarla gözden geçirilmeli ve gerekli güncellemeler ilgili tarafların onayı ile kontrollü bir şekilde yapılmalıdır.

Bilgi Varlıklarının Belirlenmesi

Bir kurumun kurumsal süreçlerini eksiksiz bir şekilde işletebilmesi amacıyla sahip olduğu bilgilerin tümüne bilgi varlıkları denir. Bir kurumun bilgi güvenliğini sağlaması için öncelikle her kurum bilgi varlıklarının farkına varacaktır. Sahip olduğu varlıkların önemini ve değerini tespit edecektir. Bu süreçte kurumsal bilgi varlıklarını eksiksiz bir şekilde tespit edilmesi, bu varlıkların zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması gerekmektedir. Bu varlıkların korunabilmesi için fiziksel güvenliğin, iletişim güvenliğinin, erişim güvenliğinin bütünleşik bir şekilde sağlanması ve bunların yanı sıra farklı güvenli unsurları ile de organize bir şekilde çalışılması gerekmektedir [39].

Politika ve Prosedürlerin Belirlenmesi

Bir kurumun, bilgi güvenliğinin sağlanması amacıyla oluşturduğu süreçlerin planlanması, ardından uygulanması, uygulama esnasında karşılaşılan sorunların iyileştirilmesi gibi aşamaların nasıl gerçekleştirileceğine dair yol gösterici kılavuzlara ve talimatlara ihtiyacı vardır.

Politikalar, üst yönetim tarafından üretilen ve desteklenen resmi talimatlar ve beyanlar olarak tanımlanabilir. Kurum çapında, konuya özel veya sisteme özel olabilirler. Kurumun politikaları, bilgi güvenliği hedeflerini yansıtır nitelikte olmalıdır.

Hazırlanan bu politikaların en temeli, belirlenen kapsama bağlı kalarak hazırlanan Bilgi Güvenliği Politikasıdır. Bu politika BGYS işletim sürecinde; kurumun stratejik yaklaşımı, amaçlar, görev ve sorumluklar, üst yönetimin liderlik konusunda gösterdiği irade, temel görev ve sorumluluklar gibi temel başlıkları içerir. BGYS kapsamında; Bilgi güvenliği politikasının çatı görevi gördüğü bir dizi alt politikalar da hazırlanmalıdır. Bunlara örnek olarak:

- Bilgi Güvenliği Durum İzleme Politikası
- Bilgi Güvenliği Olay Yönetim Politikası
- Bilgi Sistemleri Edinim Geliştirme Politikası
- Değişiklik Yönetim Politikası
- Denetim ve Uyum Politikası
- Erişim Yönetimi Politikası
- Fiziksel ve Çevresel Güvenlik Politikası
- Güvenli Yazılım Geliştirme Politikası
- İnsan Kaynakları Güvenliği ve Hizmet İçi Eğitim Politikası
- İş Sürekliliği Politikası
- Kriptografik Kontroller ve Anahtar Yönetimi Politikası
- Paydaş Bilgi Güvenliği Politikası
- Uygun Kullanım Politikası
- Üçüncü Taraf Güvenlik Politikası
- Varlık Yönetim Politikası

gibi politikalar verilebilir.

Prosedürler ise belirli bir amaç veya görevi yerine getirmek amacıyla adım adım talimatlar içeren dokümanlardır. Kurumlarda sık tekrarlanan bilgi güvenliği ile ilgili işlemler prosedürler üzerinden yürütülür. Bu sayede gerçekleştirilecek olan işlemlerin belirli bir düzen, güvenlik kontrollü, en az inisiyatif alınmış şekilde ve kaliteli bir biçimde yapılması

sağlanır. BGYS kapsamında oluşturulabilecek prosedürlere örnek olarak:

- Ağ ve Ağ Cihazları Yönetim Prosedürü
- Bilgi Değişim Yönetimi Prosedürü
- Disiplin Prosedürü
- Dışarıdan Alınan Hizmetlerin Yönetimi Prosedürü
- Doküman ve Kayıt Yönetim Prosedürü
- Düzeltici Faaliyet ve İyileştirme Prosedürü
- Etkinlik Ölçme ve Değerlendirme Prosedürü
- Güvenlik Testleri ve Yama Yönetim Prosedürü
- İç Tetkik Prosedürü
- İş Sürekliliği Prosedürü
- Kapasite Yönetim ve Sistem Kabul Prosedürü
- Kötü Niyetli Yazılımlara Karşı Güvenlik Prosedürü
- Kullanıcı Hesap ve Parola Yönetim Prosedürü
- Risk Değerlendirme ve İşleme Prosedürü
- Sunucu Yönetimi Prosedürü
- Uzaktan Erişim Yönetimi Prosedürü
- Yazılım Geliştirme Prosedürü
- Yedekleme Prosedürü
- Yönetim Gözden Geçirme Prosedürü

gibi prosedürler verilebilir.

Tehdit ve Zafiyetlerin Belirlenmesi

Kurumun bilgi varlıklarının zarar görmesine sebep olabilecek olaylara tehdit adı verilir. Tehditler kurum çalışanları gibi iç kaynaklı veya kötü niyetli saldırganlar gibi dış kaynaklı ve insan temelli olabilirler. Diğer taraftan kurum sistemlerinde meydana gelebilecek arızalar gibi teknik iç tehditler veya sel, deprem, yangın gibi doğal dış tehditlerde bilgi varlıklarına zarar verebilecek tehditler olarak değerlendirilebilir. BGYS kurulumu ve işletilmesi esnasında oluşabilecek tehditler iyi belirlenmeli ve oluşturabileceği zararlar risk analizleriyle ele alınmalıdır.

Diğer taraftan eğer bir bilgi varlığının bir tehditten zarar görme olasılığı bulunuyorsa bu durum ilgili bilgi varlığının zafiyeti olarak değerlendirilir. Bilgi varlıklarının sahip oldukları zafiyetlerin bir tehdit tarafından kullanılma olasılığı da risk olarak nitelendirilir. Bu sebeple kurumun bilgi varlıklarının envanteri çıkarılmalı ve bu varlıkların tehditler karşısında

zafiyetleri belirlenerek kurumsal anlamda değerleri ortaya konmalıdır. Bu işlemlerin belirli aralıklarla yapılarak kurumsal tehdit ve zafiyet kütüğünün güncel tutulması sağlanmalıdır [31].

Risk Değerlendirme

Bilgi güvenliği risk değerlendirmesi, bir kuruluşun güvenlik zafiyetlerini ve tehditleri tanımlamasını ve ardından olası tehditleri ele almak için hangi önlemleri seçeceğine karar vermesini sağlayan BGYS'nin en önemli parçasıdır [40]. Risk değerlendirmesini düzgün ve düzenli bir şekilde yapılmaması, kurum için itibar kaybı, yasal konular veya hatta doğrudan bir finansal etki gibi ciddi sonuçlar doğurabilir.

Risk değerlendirme sürecinin temel amacı, risklerin nitelik açısından incelenerek uygun bulunması halinde, ilgili riskin kaynağının, oluşması durumunda sonuçlarının, olma ihtimalinin, karşılaşılabilecek senaryo çeşitlerinin, sonrasında oluşturulacak kontrollerin ve bu kontrollerin etkililiğinin değerlendirilmesinin yapılmasıdır.

Risk analizi yapılırken farklı teknikler uygulanabilir. Kullanılacak teknikler koşullara ve kullanım amacına göre değişiklik gösterebilir. Yapılan risk analizi nitel, nicel veya bunlarım karışımı şeklinde yapılabilir.

ISO 31000 standardına göre risk analizi esnasında dikkat edilmesi gereken faktörler şu şekildedir:

- Karşılaşılabilecek olayların ve bunların olasılığı
- Sonuçlarının büyüklüğü
- Değişkenlik durumları
- Sonuçların niteliği ve büyüklüğü
- Kontrollerin etkinliği
- Güven seviyeleri

Risk değerlendirmesi sonucunda, kurumsal seviyede riskler bütüncül bir yaklaşımla ele alınabilmektedir. Risk değerlendirme metodolojisi, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik unsurları açısından görebileceği zararlar ele alınacak şekilde tasarlanmış olmalıdır [41].

Kontrolleri Seçilmesi

Etkin, canlı ve sürekli gelişen bir BGYS yönetiminin sağlanabilmesi için uygun kontrol ve bu kontrollere bağlı hedeflerin belirlenmesi gerekir. Kontrol seçimi yapılırken ISO/IEC 27002 standardı veya diğer kontrol kümeleri kullanılabilir. Seçim yapılırken kurumun özel ihtiyaçları göz önünde bulundurulmalıdır. Bu sebeple herhangi bir kontrol kümesine bağlı kalınmadan kuruma özel ve kurum tarafından belirlenmiş kontroller de oluşturulabilir. Bu sebeple kılavuz niteliği taşıyan kontrol kümeleri başlangıç noktası olarak kabul edilmelidir. Diğer taraftan kontroller seçilirken, kurum tarafından kabul edilen risk kabul kriterleri, risk işleme seçenekleri ve kurum risk yönetimi yaklaşımı dikkate alınmalıdır [42].

Risklerin İşlenmesi

Risk yönetiminde, risklerin değerlendirilmesinin ardından ikinci aşama olarak risklerin işlenmesi gerekmektedir. Bu aşamada belirlenen risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski tamamen ortadan kaldıracak veya azaltacak kontrollerin belirlenmesi gerekmektedir. Risklerin tamamen ortadan kaldırılması çoğu zaman imkânsızdır. Risk işleme için Şekil 2.10'da gösterilen risk işleme süreçleri uygulanır. Bu süreçler şu şekilde belirtilebilir:

Riskin kabulü

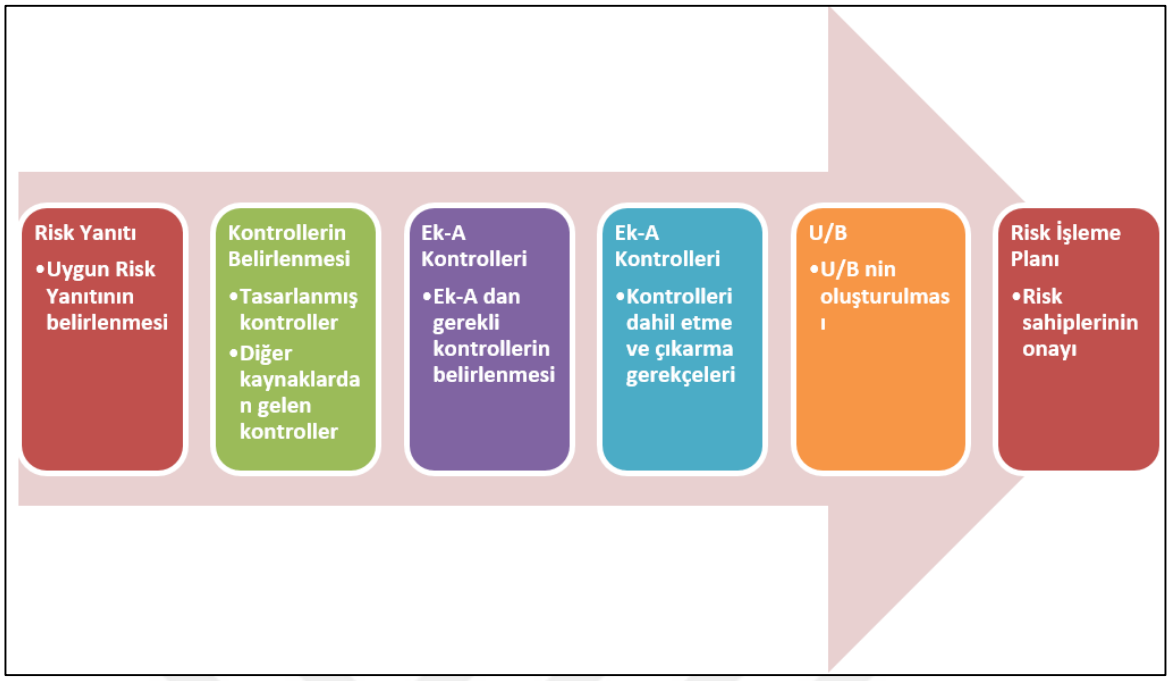
Riskin azaltılması veya tamamen ortadan kaldırılmasına yönelik herhangi bir kontrolün sağlanamaması durumunda BT sistemlerinin var olan durumu ile kullanılmasına devam edilmesi durumudur.

Riskten kaçınma

Riske sebep olan durumundan tamamen vazgeçilmesi şeklinde alınan önlemdir. Örneğin; kurum dışından erişim risklerinin kaldırılması amacıyla VPN erişimlerinin durdurulması.

Riskin Azaltılması

Belirlenen risklerin gerçekleşmesi olasılığının düşürülmesi veya gerçekleşmesi durumunda oluşabilecek zararların en aza indirilmesi amacıyla çalışmalar yapılmasıdır.



Şekil 2.10. Risk işleme süreçleri

Riskin Transferi

Riskin ortadan kaldırılmaksızın sonuçlarının üçüncü taraflara aktarılmasıdır. Örneğin; oluşabilecek zararlara karşı sigorta yaptırılması. Kurum yönetimi, risk işleme esnasında bilgi varlıklarına gelebilecek zararları en aza indirmek amacıyla en uygun ve en az maliyetli olan yönetimi seçmekle yükümlüdür [43].

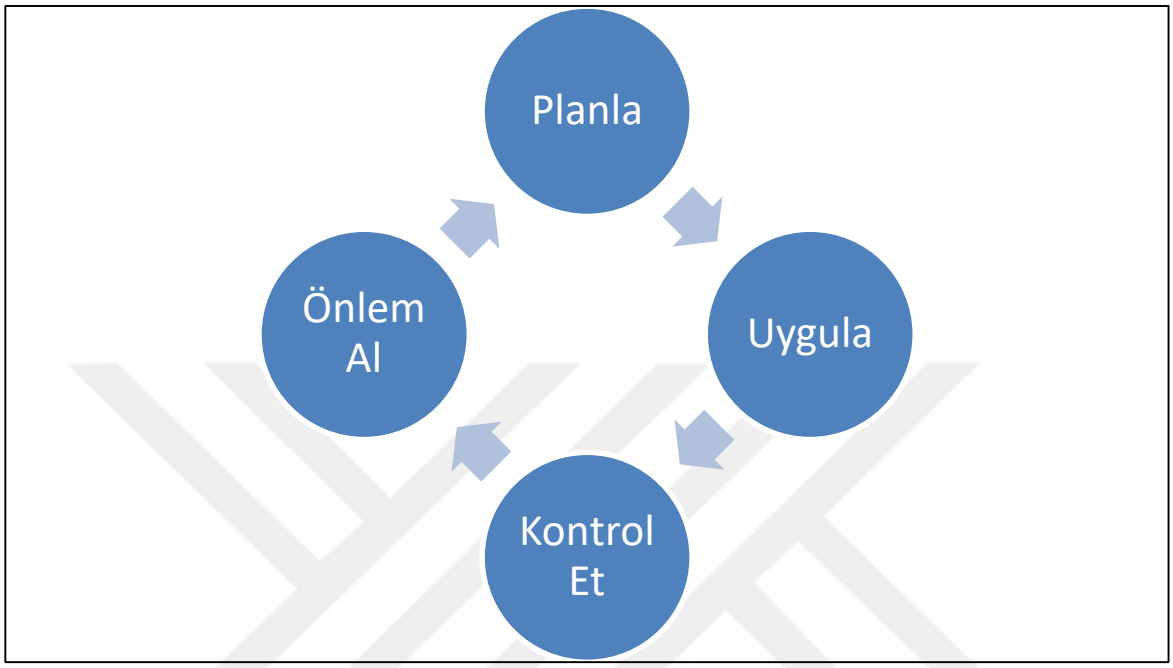
Sorumluluk ve Görevlerin Dağıtılması

BGYS'nin ISO27001 standardının gereklerini yerine getirmesinin sağlanması ve kurulan BGYS'nin performansı ile ilgi üst yönetime rapor verilmesi amacıyla; üst yönetim tarafından, bilgi güvenliği yönetim süreci ile ilgili sorumlulukların belirlenmesi, yetkililerin atanması ve duyurulması gerekmektedir. Üst yönetim, her ne kadar kurumun bilgi varlıklarının korunmasında nihai sorumluluğa olsa da, BGYS sürecinin yönetilmesi amacıyla yöneticiler ve ekip üyeleri de atayabilir.

Kontrollerin Uygulanması

ISO27001 standardı, yaşayan bir bilgi güvenliği yönetimi sisteminin teminini sağlamaya çalışır. Yani kurulmuş olan BGYS'nin, tehdit ve saldırılar karşısında anlık reaksiyonlar gösterebilen dinamik bir yapı kazanması amaçlanmaktadır. Bu sebeple ISO27001 standardı,

Şekil 2.11'de gösterilen, PUKÖ(Planla-Uygula-Kontrol Et- Önlem Al) döngüsü süreç modeli benimsemiştir. Bu modelde uygulanan tüm süreçlerin uygulanıp uygulanmadığını, gerekli önlemlerin alınıp alınmadığı kontrolleri düzenli olarak sağlanabilmektedir [44].



Şekil 2.11. PUKÖ döngüsü

Gereksinim ve süreçler başlığı altında şimdiye kadar planlama üzerinde durulmuş, kapsamın belirlenmesinden risklerin tanımlanmasına kar ki süreç ele alınmıştır. Kontrollerin uygulanması aşaması ise, planlama aşamasında belirlenen tüm faaliyetlerin, politika ve prosedürlerin uygulamaya alındığı, operasyonun gerçekleştiği adımdır. Bu adım uygulanacak olan BGYS'nin başarısını yansıtacak olması sebebiyle oldukça önemlidir [45].

Performansın izlenmesi

Kurum uygulama aşamasında yaşanabilecek aksaklıkları, eksiklikleri ve yenilikleri belirlemek amacıyla kurmuş olduğu BGYS'nin etkinliğini değerlendirmelidir. Bu aşamada kurum, BGYS süreçleri ve uygulanması beklenen kontroller de dâhil olmak üzere neyin izlenmesi ve ölçülmesi gerektiğine, gerekli izleme sonuçlarının elde edilmesi için uygulanması gereken ölçme yöntemleri ve araçlarına kendisi karar vermelidir. Tabi seçilen yöntem ve araçların kabul edilebilmesi için karşılaştırılmaya ve istendiğinde tekrar üretilmeye müsait çıktılar üretebilmesi gerekmektedir.

Dünyada ISO27001

ISO27001 standardının ilgili kurumun faaliyet gösterdiği sektörden bağımsız olarak bir bilgi güvenliği yönetim sisteminin gereksinimlerini tanımlaması, denetlenebilir olması ve diğer yönetim sistemleri ile uyum sağlayabilmesi sebebiyle uluslararası kabul görmüş en önemli standartlardan bir tanesidir. ISO organizasyonu tarafından yayınlanan istatistiklere göre, 2590 tanesi 2017 yılı içerisinde alınmış olan dünya çapında toplam 39501 adet kurumun ISO27001 belgesi sahibi olduğu belirtilmiştir. Çizelge 2.2'de en çok ISO27001 sertifika sahibi 15 ülke verilmiştir. Türkiye'nin ise belge sayısına göre 13. sırada olduğu görülmektedir.

Çizelge 2.2. Ülkelere göre ISO27001 sertifika sayıları (2017) [46]

	Ülke	**Belge Sayısı**
1	Japonya	9161
2	Çin	5069
3	Britanya	4503
4	Hindistan	3272
5	Amerika	1517
6	Almanya	1339
7	Çin	994
8	İtalya	958
9	Hollanda	913
10	İspanya	803
11	Yunanistan	727
12	Polonya	705
13	Türkiye	531
14	Macaristan	472
15	Çek Cumhuriyeti	463

Sektörler bazında oluşturulan listede ilk 15 incelendiğinde ise Çizelge 2.3'de belirtildiği üzere 2017 yılı sonu itibariyle en çok Bilgi Teknolojileri alanında faaliyet gösteren kurumların ISO27001 belgesi sahibi oldukları görülmekte iken kamu kurumlarının 11. sırada yer aldığı görülmektedir.

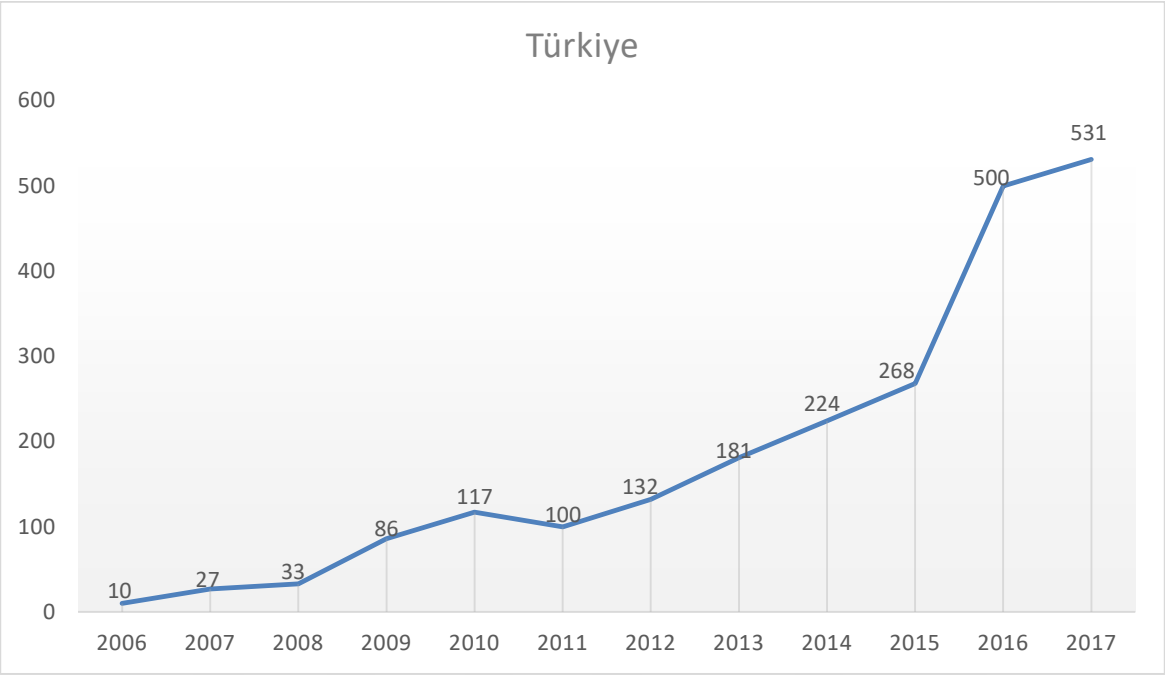
Çizelge 2.3. Dünyada sektörlere göre ISO27001 sertifika sayıları (2017) [46]

	Sektör	Belge Sayısı
1	Bilgi Teknolojileri	7478
2	Diğer Servisler	1369
3	Ulaştırma, Depolama ve İletişim	930
4	Mühendislik Hizmetleri	382
5	Finansal Aracılık, Emlak, Kiralama	344
6	Elektrikli ve Optik Donanım	316
7	Toptan ve Perakende Ticaret; Motorlu Taşıt	283
8	Sağlık ve Sosyal Çalışma	216
9	İnşaat	193
10	Baskı Şirketleri	187
11	Kamu Kurumları	185
12	Diğer Sosyal Hizmetler	105
13	Elektrik Kaynağı	87
14	Makine ve Ekipman	73
15	Eğitim	54

Türkiye'de ISO27001

Türkiye'de siber güvenlik alanında Ulaştırma ve Altyapı Bakanlığı tarafından kamu bilişim sistemlerine, kamu veya özel sektör tarafından yürütülen kritik altyapılara ait bilişim sistemlerinde ve küçük ve orta ölçekli tüzel kişilikleri kapsayacak 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı yayınlanmıştır [47]. Eylem planı çerçevesinde yürütülen çalışmalardan biri de kamu kurumlarının birbirleri olan iletişimlerinin sağlandığı KamuNet ağı kurulumudur. Resmi gazetede yayınlanan 21.07.2016 tarih ve 30103 sayılı "KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ" ile KamuNet ağı hakkında usul ve esaslar belirlenmiştir. Tebliğin, Kamu Kurumu yükümlülükleri ve asgari gereksinimlerin yer aldığı ikinci bölümü 4.maddesi a bendi uyarınca KamuNet bağlantısı yapacak tüm kamu kurumlarının birimleri ve sistemlerini kapsayacak şekilde Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmasını ve işletmesini zorunlu kılınmıştır. Yine aynı maddenin b bendi uyarınca ise kurumlar tarafından kurulan BGYS için ISO27001 standardı uyumluluğunun sağlanması ve belgelendirme işlemlerinin bağımsız belgelendirme kuruluşları tarafından yapılması zorunluluğu getirilmiştir [7]. Kamu

kurumları ve kamu kurumları ile iş yapan özel sektör kuruluşlarına getirilen bu zorunluluk ile birlikte Türkiye'de ISO27001 sertifikası sahibi kurum sayılarında artış olduğu gözlemlenmiştir.



Şekil 2.12. Yıllara göre Türkiye ISO27001 sertifika sayıları (2017) [46]

ISO organizasyonu tarafından yayınlanan istatistiklere göre 31 tanesi 2017 yılında alınmış olan toplam 531 adet ISO27001 sertifika sahibi kurum/kuruluş bulunmaktadır. Şekil 2.12'de yer alan verilere göre göre 2016 yılında alınan sertifika sayısının diğer yıllara göre daha fazla oranda artmış olduğu görülmektedir.

3. İLGİLİ ARAŞTIRMALAR

ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardı üzerine yapılmış çalışmalara aşağıda kısaca yer verilmiştir.

Çek (2017) tarafından yayınlanan yüksek lisans tezinde kurumsal bilgi güvenliği yönetişiminde insan faktörünün önemi üzerinde durmuştur. Bilgi güvenliği yönetişiminin kurumlarda sağlıklı bir şekilde yönetilebilmesi için yönetim desteğinin şart olduğu vurgulanmış ve bu desteğin en üst yönetimin tarafından verilmesi gerektiği belirtilmiştir. Diğer taraftan üst yönetiminin desteğinin şart olduğu fakat yeterli olmadığı vurgulanmış tüm kurum personelinin de bu süreçte aktif rol alması gerektiği belirtilmiştir. Bu sürece dâhil olmayan tek bir personelin bile bilgi güvenliği süreçlerini olumsuz etkileyeceği bu sebeple personelin bilgi güvenliği farkındalığının önemi özellikle vurgulanmıştır. Farkındalık oluşturma sürecinde ise her personelin kurumsal rol ve sorumlulukları çerçevesinde gerekli bilgi ve yönlendirmelerin yapılması büyük önem arz etmektedir [31].

King (2017) tarafından yayınlanan doktora tezinde kurumsal bilgi güvenliği yönetişimi ile bilgi güvenliği yönetim standartları arasında doğrusal bir ilişki olup olmadığının araştırılması amaçlanmıştır. Bu çalışma kapsamında Amerika Birleşik Devletleri Hawaii ve Alaska kentlerinde küçük ve orta ölçekli kuruluşlarda görevli 210 kişi üzerinde anket uygulanması yapılmıştır. Anket çalışması sonucunda kuruluşlarda etkin bir bilgi güvenliği yönetişimi ile bilgi güvenliği standartları arasında doğrusal bir ilişki olduğu tespit edilmiştir [48].

Güldüren (2015) tarafından yayınlanan doktora tezinde, yükseköğretim kurumlarında görevli öğretim üyeleri üzerinde bilgi güvenliği farkındalığı oluşturmaya yönelik, çoklu ortam materyalleri ile birlikte bir web sitesi geliştirilmesi ve bu geliştirilen web sitesinin farkındalık kazandırılması noktasındaki etkinliğinin ölçülmesi amaçlanmıştır. Yapılan çalışma kapsamında bilgi güvenliği farkındalık ölçeği geliştirilmiştir. Geliştirilen ölçek marifetiyle yapılan ölçümler sonucunda, bahse konu web sitesi ve geliştirilen diğer materyallerin bilgi güvenliği farkındalığı oluşturulması noktasında olumlu yönde katkı sağladığı sonucuna varılmıştır [49].

Gencer (2015) tarafından yürütülmüş olan araştırma kapsamında, ISO27001 süreçlerinin ve gerekliliklerinin dinamik bir yapı kazandırılarak, kurumlarda günlük yaşantının bir parçası haline getirilmesi amaçlanmıştır. İlgili araştırmada kurumsal ve uluslararası saygınlık ve kabul görmek için ISO27001 standardının gerekliliği dile getirilmiştir. Kamu kurumlarında son yıllarda daha fazla görülmeye başladığı dile getirilmiştir. Ayrıca ISO27001 uyum çalışmalarına kurumsal bilgi varlıkları envanterinin çıkarılarak başlanması gerektiği sonucuna ulaşılmıştır. Kurulan sitemin dinamik bir şekilde yönetilebilmesi, sertifikasyon süreçleri sonrasında da gerekli kontrollerin sağlanabilmesi amacıyla sistemin yönetiminin sağlandığı bir uygulamadan destek alınması gerektiği ve aynı zamanda sistemin en zayıf halkası olan insan faktörünün mümkün olduğu kadar azaltılmasının başarıyı olumlu yönde etkileyeceği sonucuna varılmıştır [50].

Akay (2014) tarafından ISO27001 standardının tarihsel gelişimi ve sürümler arasındaki farklılıklara yer verilmiştir. İlgili çalışmada, ISO27001 sertifikasyon sürecini tamamlamış ve isimleri gizili tutulmuş iki kuruluş ile yapılan mülakatlara yer verilmiş ve elde edilen bulgular ele alınmıştır. İlgili çalışma kapsamında, BGYS süreçlerinin teknik bir konu olarak algılandığı ve bu yanlış algının kurulan BGYS'nin etkinliğini olumsuz yönde etkilediği sonucuna varıldığına değinilmiştir. Diğer taraftan ISO27001 gereksinimlerinin uygulanması esnasında teoride ve pratikte paralellik sağlanması gerektiği vurgulanmıştır [51].

Gürcan (2014) tarafından yapılan çalışmada, finans kurumlarının bilgi güvenliği ihtiyaçlarının ISO27001 çatısı altında incelenerek belirlenmesi üzerinde durulmuştur. BU kapsamda ilgili kuruluşlara çeşitli anketler uygulanmıştır. Anket sonuçlarına göre, süreçlerin dokümantasyon bölümünün tamamlandığı fakat organizasyonel süreçler üzerinde uygulanmaya başlanması noktasında bazı aksaklıklar olduğu dile getirilmiştir. Özellikle mobil işgücü tarafında geliştirilmiş politikaların yeterli olmadığı ve diğer politika ve prosedürlerin uygulanması noktasında da %75 gibi bir yeterliliğe sahip olunduğu sonucuna varılmıştır [52].

Ganbat (2013) tarafından, ISO27001 ve ISO27005 standartlarının uygulanması konulu çalışmasında ISO27001'in nasıl uygulanması gerektiği ve ISO27005 Risk Yönetimi standardı ile ilişkisi üzerinde durulmuştur. Çalışma kapsamında, ISO27001 kapsamının ilgili kurum veya kuruluş tarafından belirlenebildiği ve sebeple kapsamın belirlenmesi esnasında detaylı bir çalışma yapılması gerektiği herhangi bir noktanın atlatılmaması için de ISO27005

standardından destek alınması gerektiği vurgulanmıştır. Aynı zamanda standartlara uygum süreçleri esnasında yönetim desteğinin şart olduğu vurgusu yapılmıştır [53].

Demirtaş (2013) tarafından yapılan çalışmada kamu ve özel sektör kuruluşları tarafından yürütülen BGYS'lerin başarı dayanakları değerlendirilmiş ve sistemi olumlu ya da oluşu yönde etkileyen unsurlar irdelenmiştir. Diğer taraftan ISO27001 sertifikasyon süreçlerinin etkin bir şekilde uygulanabilmesini teminen bir model önerisinde bulunulmuştur. Aynı zamanda ISO27001 sertifikası sahibi olmanın ilgili kuruluşların marka ve imaj değerini olumlu yönde etkileyeceği değerlendirmesinde bulunulmuştur. Çalışma kapsamında, bilgi güvenliğinin etkin bir şekilde sağlanabilmesi için teknik imkânların yeterli olmayacağı, bu imkânların personel farkındalığı, süreçler, politikalar ve prosedürlerle desteklenmesi gerektiği vurgulanmış bunun da en iyi şekilde bir sertifikasyon süreci ile mümkün olacağı sonucuna varılmıştır. Bilgi güvenliğinin sadece teknolojik bir süreç olmadığı aynı zamanda insan faktörünün de detaylı bir şekilde ele alınması gerektiği, gerekli farkındalık çalışmalarının ve eğitimlerin de uygulanması gerektiği vurgulanmıştır [11].

Haklı (2012) tarafından "*Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi*" başlıklı çalışmasında kamu kurumlarına özel olarak tasarlanmış ve ISO27001 kurulum süreçlerinin tamamının yönetilebileceği bir uygulama geliştirilmesi üzerinde durulmuştur. Çalışma kapsamında BGYS kurulum çalışmalarının başlatılabilmesi için ilk muhatabın, bilgi varlıklarının işlendiği, depolandığı ve yönetildiği yer olan kurumların Bilgi İşlem Merkezleri olduğu vurgulanmıştır. Bahse konu yazılım çalışmaları analiz aşamalarında bilgi işlem merkezleri ile çalışılmış ve kamu kurumlarına özel bilgi güvenliği modeli oluşturulmuştur [54].

Shoraka (2011) tarafından yürütülmüş olan tez çalışmasında ISO BGYS sertifikasyon sürecini tamamlanmış kuruluşlar arasında yaptığı bir araştırma ile sertifika sahibi olmanın ilgili kuruluşlara herhangi ekonomik değer kazandırıp kazandırmadığını araştırmıştır. Bahse konu araştırma sonucunda özellikle sermaye piyasalarında kuruluşların sertifika sahibi olmalarının duyurulması sonrasında herhangi bir değer artışı olmadığı yönünde bir tespit yapılmıştır. Sertifika sahibi olan kuruluşlar ile olmayan kuruluşlar arasında bilgi güvenliği ihlallerine alınan tepkiler arasında da herhangi bir fark olmaması sebebiyle ISO BGYS sertifikasyon sürecinin ilgili kuruluşlara herhangi bir ekonomik değer kazandırmadığı sonucuna varılmıştır [55].

Mete (2010) tarafından yürütülen çalışmada ISO27001 standardının bilgi işlem merkezlerine uygulanması araştırılmıştır. Çalışma kapsamında BGYS kurulumu yapmak isteyen bilgi işlem merkezlerine rehber niteliği taşıyan Türkçe bir kaynak oluşturulması amaçlanmıştır. Ayrıca BGYS kurulumu ve yönetimi esnasında yönetim desteğinin önemi ve aynı zamanda kurumsal süreçlere hâkim, standart hakkında gerekli bilgi düzeyi yüksek bir ekibin varlığının önemi vurgulanmıştır. Aynı zamanda ilgili süreçlerin BGYS ekibi ile kalmayıp tüm tabana yayılması gerektiği, ilgili tüm birimlerin gerekli katkılarının sağlaması yönünde gerekli iradenin gösterilmesi gerektiği dile getirilmiştir. BGYS'nin özellikle risk yönetim süreci olduğu ve kurumsal bilgi güvenliği risklerinin belirlenmesinin ve risk süreçlerinin etkin bir şekilde yönetilmesinin önemi vurgulanmış, bu süreç kapsamında her türlü detayın irdelenmesi gerektiği dile getirilmiştir. Bu sebeple kurulacak olan BGYS'nin tüm kurum tarafından sahiplenilmesinin önemi üzerinde durulmuştur [56].

Aydoğmuş (2010) tarafından hazırlanmış olan "*Türkiye'deki Organizasyonların Bilgi Güvenliği Olgunluk Seviyelerinin Belirlenmesi ve ISO/IEC 27001:2005 Standardına Uyumluluklarının Değerlendirilmesi*" başlıklı tez çalışması kapsamında kurumların bilgi güvenliği olgunluk seviyelerinin belirlenmesi amaçlanmıştır. Çalışma kapsamında hazırlanan anket sorularından elde edilen veriler kapsamında şu sonuçlar elde edilmiştir. Bilgi servisleri, finans, sigortacılık, telekomünikasyon, sağlık ve gayrimenkul sektörlerinin bilgi güvenli kontrol ve görevlerini büyük ölçüde tamamladıkları gözlemlenmiştir. Ayrıca birçok kuruluşta yönetim standardın gerekliliğinin farkındadır [57].

Bilgi güvenliği yönetim sistemleri ve ISO27001 standartları ile ilgili yapılan çalışmalar incelendiğinde kurulan sistemin etkinliği ve insan faktörünün öneminin özellikle vurgulandığı görülmektedir. Diğer taraftan yapılan araştırmalarda etkin bir BGYS kurulumu ve yönetimi için kurumsal üst yönetim desteğinin önemi de ayrıca vurgulanmıştır. Aynı zamanda bilgi güvenliği yönetiminde, yönetim, BGYS ekibi, kurum teknik personeli ve kurum personeli gibi çeşitli roller olduğu dile getirilmiş ve bu roller arasındaki uyumlu çalışmanın önemi vurgulanmıştır. Bahse konu roller arasındaki çalışmanın uyumu ve olgunluk seviyeleri ile ilgili çeşitli araştırmalar yapılmış ve kurumsal bilgi güvenliğinin olgunluk düzeyinin ölçülmesi amacıyla çeşitli modeller geliştirilmiştir.

İlgili olgunluk seviyelerinin belirli bir düzeye çıkarılması ve kurumsal bilgi güvenliği yönetim sisteminin daha etkin bir şekilde yönetilmesi amacıyla çeşitli uygulamalar

geliştirilmiş ve bu kapsamda çeşitli yüksek lisans ve doktora tez çalışmaları yapıldığı görülmüştür. Yapılan tüm çalışmalar ve geliştirilen tüm uygulamaların temelinde insan faktörü olduğu ve yapılan tüm çalışmalarda kurum personellerinin tüm kademelerde katılımcı rol almaları gerektiği yönünde çıkarımlar olduğu görülmektedir. Özellikle ISO27001 sertifikasyon sürecinin ve BGYS kurulumunun en önemli çalışması olarak risk belirleme ve işleme süreçleri olduğu vurgulanmıştır. Yapılan bazı araştırmalar kapsamında sertifikasyon sürecinin ilgili kuruluşlara her ne kadar ekonomik bir değer katmıyor olsa da marka ve imaj değeri açısından olumlu yönde katkı sağladığı sonucuna varıldığı görülmektedir. Diğer taraftan BGYS süreçler kapsamında yapılan çalışmaların sadece teknik personeller ile ilgili olmadığı kurum personelinin bu süreci günlük yaşantının bir parçası haline getirmesi gerektiği sonucuna varıldığı görülmektedir.

Sonuç olarak yapılan araştırmaların sertifikasyon süreçlerinden ziyade BGYS ve siber güvenlik alanında yapıldığı, personelin bilgi güvenliği farkındalığı ve kurulan BGYS'nin olgunluk seviyesinin değerlendirildiği görülmektedir. Diğer taraftan Türkiye'de 2017 yılında yayınlanan KamuNet tebliği [7] kapsamında kamu kurumlarına BGYS kurulumu ve ISO27001 sertifikasyon süreçlerinin tamamlanması zorunluluğu getirilmiştir. Bu kapsamda Türkiye'de kamu kurumları ve kamu kurumları ile ortak çalışma yürüten özel sektör kuruluşlarının da ISO27001sertifikası sahibi olmaları ile birlikte bazı temel yeterliliklere sahip olmaları beklenmektedir. Bu sebeple birçok kamu kuruma bahse konu tebliğde yer alan asgari güvenlik kriterleri ve ISO27001 sertifikasyon sürecinin tamamlamaları için belirli süreler tanınmıştır. Tanınan bu süreler içerisinde kamu kurumları gerekli çalışmaları tamamlamış ve BGYS ile birlikte ISO27001 sertifikası sahibi olmuşlardır. Bu çalışmada sertifikasyon sürecini tamamlamış olan ve bu güne kadar yapılan çalışmalarda dile getirilerek önemi vurgulanan üst yönetim, BGYS ekip üyeleri, teknik ekipler ve kurum personeli açısından kurumlarında çalışmaları tamamlanmış BGYS süreçleri hakkındaki görüşlerinin araştırılması planlanmıştır.

4. YÖNTEM

Bu bölümde araştırmanın nasıl yapılacağı, evren ve örneklem ve verilerin toplanması ile ilgili çalışmalar üzerinde durulmuştur.

4.1. Araştırma Modeli

Bilgi güvenliği yönetim sistemine sahip ve sertifikalandırmış olan kamu kurumlarının bu süreci ne ölçüde sahiplendikleri, sertifika sahibi olmanın bilgi güvenliğinin sağlanmasında yeterli olup olmadığı, bilgi güvenliği farkındalık seviyelerindeki gelişme gibi konuların belirlenmesi amacıyla betimsel çalışma uygulanmıştır. Bu çalışmanın örnekleri üzerinde anket çalışmaları yürütülmüş ve alınan cevaplar doğrultusunda ana problem ve alt problemlere cevap verilmeye çalışılmıştır.

4.2. Evren ve Örneklem

Araştırmanın evreni Ankara da bulunan ve ISO27001 sertifikası sahibi kamu kurum ve kuruluşlarından oluşmaktadır. Evrenin büyük olması ve bazı ISO27001 sahibi kurum ve kuruluşlar tarafından kurum personeline anket uygulanmasına izin verilmemesi, izin verilen kurumlarda ise katılımın tam olarak sağlanmaması sebebiyle örneklem alma yoluna gidilmiştir. Araştırmanın örneklemini 6 kamu kurumu ve bu kurumlarda görevli 539 kişi oluşturmaktadır.

4.3. Veri Toplama Araçları

Araştırmada Türkiye'de bulunan ISO27001 sertifika sahibi kurumların hâlihazırda çalışan 4 farklı personel grubuna (Üst Yönetim, BGYS Ekibi, Teknik Ekip ve Personel) uygulanmak üzere hazırlanmış 4 ayrı anketten oluşmaktadır. Hazırlanan tüm anketler 2 ana bölümden oluşmaktadır. Birinci bölümde kişilerin yaş, eğitim ve meslek gibi demografik bilgileri talep edilmiş, diğer bölümlerde ise hedef kitlesine dönük sorulara yer verilmiştir. İkinci bölümlerde yer alan sorularda 5'li likert ölçeği kullanılmıştır. Ölçeğin dereceleri ise "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum", "Kesinlikle Katılıyorum" şeklindedir. Anket soruları, bilgi güvenliği ve istatistik alanlarında uzmanların görüşleri alınarak oluşturulmuştur. Sorular hazırlanırken anlaşılır olması ve katılımcılar arasında farklı anlaşılmalara sebebiyet vermemesi için özen gösterilmiştir.

Likert tipi ölçek sorularında Cronbach Alpha (α) güvenilirlik analizi uygulanmış ve alınan güvenilirlik analizi sonuçlarının ardından, hazırlanan soruların güvenilirlik düzeylerinin yeterli olduğu sonucuna varılmıştır. Hazırlanan sorular son olarak Türk Dili uzmanları tarafından yazım yanlışı ve dilbilgisi hataları açısından incelenmiştir.

Anket sorularının oluşturulması esnasında ISO27001 standardında yer alan "*Bir kuruluşun bu standarda uyumluluk iddiasında bulunması durumunda, Madde 4 ila Madde 10 arasında belirtilen şartların herhangi birinin hariç tutulması kabul edilebilir değildir."* ifadesinde belirtilen ilgili maddelerden ve bilgi güvenliği konusunda daha önce hazırlanmış olan çeşitli tez çalışmalarından faydalanılmıştır. Oluşturulan anketler ve uygulanan analizlere ilişkin veriler şu şekildedir:

Yönetici

Kurum yöneticileri için hazırlanmış olan anket 16 adet sorudan oluşmaktadır. Anket soruları ile ISO27001 in olmazsa olmaz unsurlarından biri olan ve aynı zamanda ilgili standardın 5. Liderlik maddesi altında yer alan ve "Liderlik" rolüne olan yaklaşımlarının ve sistemin sahiplenilmesi ve işletilmesi konusunda göstermiş oldukları iradenin incelenmesi amaçlanmıştır.

Bu kapsamda yöneticiler için hazırlanmış olan anket sorularının 1., 2., 10., 11. ve 12. soruları, ilgili standardın 5.1 maddesinde yer alan, yönetim kademesinin BGYS ile ilgili olarak liderlik ve bağlılık göstermesi, sürekli iyileştirmenin desteklenmesi gerektiği yönündeki ifadelerden yola çıkarak hazırlanmış ve ilgili tarafların bu konu hakkındaki görüşlerinin alınması amaçlanmıştır. Yönetici anketinin 3. ve 4. soruları ise yine ISO27001 standardının 5.1.a ve 5.1.b maddelerinde yer alan kurumsal stratejik hedeflere erişim ve kurumsal süreçlere uyumluluk çalışmalarının yapılması gerektiği yönündeki ifadeden yola çıkılarak hazırlanmıştır. Diğer taraftan bahse konu anketin 5. sorusu yine ilgili standardın 7.3 maddesinde yer alan bilgi güvenliği farkındalığının sağlanması yönündeki çalışmalara ilişkin madde konusundaki görüşlerin alınması amacıyla hazırlanmıştır. Anketin 6., 7. ve 8. soruları ise ISO27001 standardının 5.2 ve 5.3 maddelerinde yer alan kurumsal BGYS politikası ve kurulan BGYS'de yer alan roller ve sorumluluklara ilişkin maddeler konusunda ilgili tarafların görüşlerinin alınması amacıyla hazırlanmıştır. Ankette yer alan 9. Soru ise standardın EK-A kontrol maddelerinden *"A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi"*

başlığı altında yer alan önlemlere ilişkin yönetim kadrosunun görüşlerinin alınması amaçlanmıştır.

Yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,932 olarak hesaplanmıştır.

BGYS Ekip Üyeleri

Kurumlarda ISO27001 in işletilmesi ve gerekli kontrollerinin sağlanmasından sorunlu olan ve üst yönetim tarafından atanan BGSY ekip üyelerinin çalışmaları esnasında yaşadıkları problemler üzerinde durulmaya çalışılmış ve yeterlilik seviyeleri sorgulanmaya çalışılmıştır. BGYS ekip üyeleri için hazırlanan anket 18 sorudan oluşmaktadır. Uzman görüşlerinin ardından 2 soru çıkarılmıştır. Ardından yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,876 olarak hesaplanmıştır.

Bu kapsamda BGYS ekip üyelerine uygulanmak amacıyla anket soruların hazırlanırken, ISO27001 standardında yer alan BGYS ekip üyelerine ilişkin gereklilikler ve sorumluluklar göz önünde bulundurulmuştur. 1. ve 5. sorular arasında yer alan sorular ilgili standardın 7. Destek başlığı altında yer alan BGSY yönetim süreçlerinin etkin bir şekilde yürütülmesinin temini edilmesi amacıyla gerekli olan eğitimlerin alınması ve yeterliliklerin sağlanması gerekliliği hakkındaki, BGYS ekip üyelerinin görüşlerinin alınması amaçlanmıştır. 6., 7. ve 8. Sorular oluşturulurken ilgili standardın 6.1 Risk ve fırsatları ele alan faaliyetlerin gerçekleştirilmesi esnasında kurum personeli ile yapılan çalışmaların uyumu ve etkinliği ile ilgili görüşlerin alınması amaçlanmıştır. Diğer taraftan 9. ve 14. sorular arasında ise yine ISO27001 standardının 5.1 maddesi altında yer alan kurulun BGYS'ye bağlılık ve süreçlerin sahiplenilmesi ile ilgili görüşlerin alınması amaçlanmıştır.

Teknik Ekip

Kurumların teknik ekipleri için hazırlanan soru setinde ise ekibin ISO27001 in gerekliliklerini yerine getirme noktasında göstermiş oldukları irade ve yeterliliklerin sorgulanması amaçlanmıştır. Teknik ekip için hazırlanan anket 17 sorudan oluşmaktadır. Uzman görüşlerinin ardından 1 soru çıkarılmıştır. Ardından yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,932 olarak hesaplanmıştır.

Bu kapsamda kurum teknik ekiplerine uygulanmak üzere oluşturulan sorularda ISO27001 standardının bahse konu ekiplerin için uyguladığı görev ve sorumluluklar göz önünde bulundurulmuş ve bu görev ve sorumluluklar ile ilgili görüşlerinin alınması amaçlanmıştır. Özellikle Standardın 7.2.a maddesinde yer alan BGYS performansının etkileyen teknik ekip için gerekli yeterliliklerin belirlenmesi ve 7.2.b maddesinde de bu yeterliliklerin temin edilmesi gerektiği yönünde talimatlar bulunmaktadır. İlgili anketin 1. ve 3. soruları bu kapsamda hazırlanılmış olup teknik ekip üyelerinin bu konular hakkındaki görüşlerinin alınması amaçlanmıştır. Diğer taraftan ISO27001 standardının 9. ve 10. ana başlıkları altında yönetilen BGYS'nin performansının belirli aralıklarla izlenmesi ve belirlenen aksaklıkların yapılan çalışmalarla giderilmesi gerektiği yönünde talimatlar bulunmaktadır. Bahse konu anketin 4. ve 11. Soruları arasında kalan tüm soruların izleme, değerlendirme ve sürekli iyileştirme noktasında ilgili standardın sağlayacağı katkılar hakkında teknik ekibin düşüncelerinin alınması amaçlanmıştır.

Personel

Personel için hazırlanan soru setinde ise ISO27001 tarafından zorunlu kılınan personel tarafının farkındalığı ile ilgili gerçekleştirilmesi gereken farkındalığın geliştirilmesi sürecine ilişkin personelin yaklaşımı ve süreçten memnuniyet düzeyleri sorgulanmaya çalışılmıştır. Personel için hazırlanan anket 16 sorudan oluşmaktadır. Uzman görüşlerinin ardından 3 soru çıkarılmıştır. Ardından yapılan ön çalışmanın analizleri sonucunda yönetim anketinin güvenilirlik katsayısı 0,845 olarak hesaplanmıştır.

İnsan unsurundan ötürü kurumsal bilgi güvenliği yönetimlerinin etkinliği ve sürekliliği devamlı sorgulanmaktadır. Bu sebeple bilgi güvenliğinin üç temel unsurundan biri olan insan faktörü, ISO27001 standardının önemle üzerinde durduğu faktörlerden biridir. Standardın birçok bölümünde süreçlerin insanla ilişkilendirilmiş olması da bunun en önemli göstergelerinden biridir. BGYS süreçlerinin en zayıf halkası olan son kullanıcılar için hazırlanmış olan anket sorularında özellikle farkındalık konuları üzerinde durulan 7. Destek ana başlığı altında yer alan konular hakkında personelin görüşlerinin alınması planlanmıştır. Özellikle EK-A kontrollerinden A.7.2.2 başlığı altında yer alan talimat gereğince belirli aralıklarla düzenlenmesi gereken farkındalık eğitimleri ile ilgili, hazırlanan anket soruları ile personel görüşleri alınmaya çalışılmıştır.

4.4. Verilerin Toplanması

Hazırlanan anketler, hem ankete özel hazırlanmış web sitesi hem de alınan çıktılar a 6 adet kamu kurumuna uygulanmıştır. Toplam 573 adet anket cevaplanmış, cevaplanan bu anketlerden 34 tanesinin eksik cevaplanmış olması sebebiyle değerlendirmeye alınmamıştır. Değerlendirmeye alınan 539 adet anketin; 78 adedi üst yönetim ve birim yöneticileri, 42 adedi BGYS ekip üyeleri, 90 adedi kurum teknik ekipleri, 329 adedi kurum personelleri tarafından cevaplanmıştır. Anketlerin kurumlara göre dağılımı Çizelge 4.1'de verilmiştir. Kurum isimleri güvenlik nedeniyle ve kurumlardan alınan izinler doğrultusunda gizli tutulmuştur.

Çizelge 4.1. Anketlerin kurumlara göre dağılımı

Kurumlar	**A**	**B**	**C**	**D**	**E**	**F**	**Toplam**
Yönetim	11	9	15	19	16	8	**78**
BGYS Ekip Üyeleri	5	7	8	9	6	7	**42**
Teknik Ekip	12	15	11	14	12	26	**90**
Personel	45	47	43	124	31	39	**329**
Toplam	**73**	**78**	**77**	**166**	**65**	**80**	**539**

4.5. Verilerin Çözümü ve Yorumlanması

Araştırma ile ilgili elde edilen veriler uygun istatistik teknikler kullanılarak analiz edilmiş, daha sonra çizelgeler ve tablolar oluşturularak açıklanmış ve yorumlanmıştır.

ISO/IEC sertifikasyon sürecinin tamamlamış ve aktif BGYS'ye sahip olan kamu kurumlarında görevli yönetim kademesinde olan kişiler, Kurumsal bilgi güvenliği yönetim sisteminin kurulumu ve etkin bir şekilde yönetiminden sorumlu olan ve üst yönetim tarafından görevlendirilmiş kamu kurumlarında görevli BGYS ekip üyeleri, ISO27001 sahibi kamu kurumlarında görevli BGYS ekip üyeliği dışında, bilgi güvenliğinden dolaylı olarak sorumlu olan diğer teknik personel ve ISO27001 sertifikasyon sürecini tamamlamış ve etkin bir şekilde BGYS yürütülen kamu kurumlarında görevli ve teknik olmayan personel görüşlerinin belirlenmesi amacı için frekans ve yüzde dağılımları kullanılmıştır.

5. ARAŞTIRMA BULGULARI

Bu bölümde tez araştırması kapsamında uygulanmış olan anket verilerine ilişkin elde edilen bulgular ve bu bulgular doğrultusunda yapılan yorumlara yer verilmiştir. Her anket ayrı bir alt başlık altında incelenmiştir.

5.1. Yönetim Kademesinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Görüşleri

Bu bölümde araştırmaya katılan ve ISO27001 sahibi kamu kurumlarında görevli üst yönetici veya birim yöneticileri tarafından elde edilen veriler incelenecektir. Altı kamu kurumunda görevli toplan 78 yöneticinin ankete katılım sağladığı görülmektedir. Anket 12 sorudan oluşmaktadır. Yöneticilerin anketlere vermiş olduğu cevaplara ilişkin veriler soru bazlı olarak incelenmiştir.

5.1.1. ISO27001 Standardının kurumlar için gerekliği konusundaki görüşleri

Yönetim kademesinin ISO27001 standardının kurumları için gerekli olup olmadığı yönündeki sorulara ilişkin verilen cevapların frekans ve yüzdelik dağılımları Çizelge 5.1'de verilmiştir.

Çizelge 5.1. Yönetici anketi soru-1 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	3,8	3,8	
Katılmıyorum	4	5,1	9,0	
Kararsızım	1	1,3	10,3	**4,37**
Katılıyorum	23	29,5	39,7	
Kesinlikle Katılıyorum	47	60,3	100,0	

Verilen cevaplar incelendiğinde ankete katılım sağlayan 78 yöneticinin 47'sinin "*Kesinlikle Katılıyorum*" ve 23'ünün "*Katılıyorum*" cevabı vermiştir. Bu kapsamda 70 kişinin ISO27001'in kurumları içim gerekli olduğu düşüncesine katıldıkları görülmektedir. Verilen cevaplarının ortalamasının ise 4,37 olduğu görülmektedir. Buradan yöneticilerin genel anlamda ISO27001'in kurumları için gerekli olduğu düşüncesinin baskın olduğu sonucuna varılabilmektedir.

5.1.2. ISO27001 Sertifika sahibi olmanın kazandırdığı ulusal ve uluslararası saygınlık hakkındaki görüşleri

ISO27001 sertifika sahibi olmanın ulusal ve uluslararası saygınlık kazandırıp kazandırmadığı hakkında yöneticilerin vermiş olduğu cevaplara ilişkin frekans ve yüzdelik dağılımları Çizelge 5.2'de verilmiştir.

Çizelge 5.2. Yönetici anketi soru -2 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	2	2,6	2,6	
Katılmıyorum	4	5,1	7,7	
Kararsızım	8	10,3	17,9	**4,19**
Katılıyorum	27	34,6	52,6	
Kesinlikle Katılıyorum	37	47,4	100,0	

Verilen cevapların incelendiğinde, katılım sağlayanların %47,4'ünün *"Kesinlikle Katılıyorum"* ve %34,6'sının ise "Katılıyorum" şeklinde olumlu görüş bildirdikleri görülmektedir. ISO27001 sertifikasının kuruma saygınlık kazandırdığı noktasında olumlu görüşün hâkim olduğu görülmüştür.

5.1.3. ISO27001 Bilgi Güvenliği alanındaki kurumsal hedeflerime de sağladığı kolaylık hakkındaki görüşleri

ISO27001 sertifikası sahibi olmanın ilgili kuruma hedeflere erişme noktasında sağladığı kolaylık ve katkılara ilişkin sorulan soruya verilen cevapların frekans ve yüzdelik dağılımları Çizelge 5.3'de verilmiştir.

Çizelge 5.3. Yönetici anketi soru -3 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	6	7,7	7,7	
Katılmıyorum	1	1,3	9,0	
Kararsızım	4	5,1	14,1	**4,14**
Katılıyorum	32	41,0	55,1	
Kesinlikle Katılıyorum	35	44,9	100,0	

Verilen cevaplar incelendiğinde 4,14 olduğu ve genel görüşün olumlu olduğu görülmektedir.

Katılımcıların sorulan soruya %44,9 oranından "*Kesinlikle Katılıyorum*", %41 oranında "*Katılıyorum*" şeklinde cevap verdikleri görülmektedir.

5.1.4. ISO27001 Bilgi Güvenliği politikalarının kurumsal süreçlerin uygulanması konusunda sağladığı faydalar hakkındaki görüşleri

Yöneticiler tarafından ISO27001 sertifikası sahibi olmanın kurumsal iş süreçlerinin uygulanması noktasında herhangi bir olumlu katkı sağlamadığı konusunda yöneltilen soruya verilen cevapların frekans ve yüzdelik dağılımları Çizelge 5.4'de verilmiştir.

Çizelge 5.4. Yönetici anketi soru -4 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	1	1,3	1,3	
Katılmıyorum	7	9,0	10,3	
Kararsızım	3	3,8	14,1	**4,21**
Katılıyorum	31	39,7	53,8	
Kesinlikle Katılıyorum	36	46,2	100,0	

Verilen cevaplar incelendiğinde genel ortalamanın 4,21 olduğu görülmektedir. Bu sonuçtan yola çıkarak genel görüşün olumlu olduğu görülmüştür. Katılımcıların %46,2'si *"Kesinlikle Katılıyorum"*, %39,7'si ise *"Katılıyorum"* şeklinde görüş bildirmiştir.

5.1.5. ISO27001'in kurum yöneticilerinin Bilgi Güvenliği farkındalığına sağladığı katkılar hakkındaki görüşleri

ISO27001'in en önemli görevlerinden birisi olan "Bilgi güvenliği farkındalığı oluşturmak" konusunda kurum yöneticilerinin ilgili soruya verdikleri cevapların frekans ve yüzdelik dağılımları Çizelge 5.5'de verilmiştir.

Çizelge 5.5. Yönetici anketi soru -5 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	1	1,3	1,3	
Katılmıyorum	6	7,7	9,0	
Kararsızım	3	3,8	12,8	**4,32**
Katılıyorum	25	32,1	44,9	
Kesinlikle Katılıyorum	43	55,1	100,0	

Verilen cevaplar incelendiğinde, yöneticilerin %55,1'i *"Kesinlikle Katılıyorum"*, %32,1'i ise *"Katılıyorum"* şeklinde görüş bildirmiştir. Buradan da ISO27001'in bilgi güvenliği farkındalığı oluşturma konusunda fayda sağladığı şeklinde olumlu görüş bildirdikleri görülmektedir. Diğer taraftan 1 kişinin "Kesinlikle Katılmıyorum", 6 kişinin "*Katılmıyorum*" şeklinde görüş bildirdiği ve 3 kişinin de bu konuda kararsız olduğu görülmektedir.

5.1.6. Bilgi Güvenliği Yönetim Sisteminin sürdürülebilir olmasına yönetim desteğinin katkısı hakkındaki görüşleri

ISO27001'in olmazsa olmazlarından biri olan yönetim desteği ve kurulan sistem arkasında gerekli iradenin gösterilmesi noktasında katılımcılar tarafından verilen cevapların frekans ve yüzdelik dağılımları Çizelge 5.6'da verilmiştir.

Çizelge 5.6. Yönetici anketi soru -6 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	3,8	3,8	
Katılmıyorum	3	3,8	7,7	
Kararsızım	4	5,1	12,8	**4,49**
Katılıyorum	11	14,1	26,9	
Kesinlikle Katılıyorum	57	73,1	100,0	

Verilen cevaplar incelendiğinde yöneticilerin %73,1'i *"Kesinlikle Katılıyorum"*, %14,1'i ise *"Katılıyorum"* şeklinde görüş bildirdiği ve bu konuda olumlu cevabın ağır bastığı görülmüştür. Genel ortalamaya bakıldığında ise en yüksek ortalamanın bu soruya ait olduğu görülmektedir.

5.1.7. ISO27001 Bilgi Güvenliği Yönetim Sisteminde yer alan, yönetimin üzerine düşen görevlerin uygulanabilirliği hakkındaki görüşleri

BGYS standardizasyonunun sağlanması sonrasında kurulmuş olan BGYS'nin kurum yönetimine yüklediği görev ve sorumluluklarının uygulanabilir olup olmadığı yönünde sorulan soruya verilen cevapların frekans ve yüzdelik dağılımları Çizelge 5.7'de verilmiştir.

Verilen cevaplar incelendiğinde ortalamanın 3,99 olduğu görülmektedir.

Çizelge 5.7. Yönetici anketi soru -7 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	5,1	5,1	
Katılmıyorum	3	3,8	9,0	
Kararsızım	9	11,5	20,5	**3,99**
Katılıyorum	36	46,2	66,7	
Kesinlikle Katılıyorum	26	33,3	100,0	

Yöneticilerin %33,3'iü *"Kesinlikle Katılıyorum"*, %46,2'si ise *"Katılıyorum"* şeklinde görüş bildirdiği ve bu konuda olumlu cevap verdiği görülmüştür. Katılımcılar arasından %11,5'lik bir bölüme denk gelen 9 kişinin ise bu konuda kararsız olduğu görülmektedir.

5.1.8. ISO27001 standartlarının uygulanmasının kurumsal süreçlerin uygulanması sırasında getirdiği ek iş yükü hakkındaki görüşleri

Katılımcılara bu soru ile ISO27001 standardının kurumsal süreçlerin uygulanması esnasında herhangi bir iş yükü getirip getirmediği noktasında görüşleri sorulmuştur. İlgili soruya verilen cevapların frekans ve yüzdelik dağılımları Çizelge 5.8'de verilmiştir.

Çizelge 5.8. Yönetici anketi soru -8 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	14	17,9	17,9	
Katılmıyorum	12	15,4	33,3	
Kararsızım	22	28,2	61,5	**3,00**
Katılıyorum	20	25,6	87,2	
Kesinlikle Katılıyorum	10	12,8	100,0	

Verilen cevaplar incelendiğinde olumlu ve olumsuz tarafta dağılımların birbirine yakın olduğu ve %28,2 ile verilen en yüksek cevap oranının "*Kararsızım*" şeklinde olduğu görülmektedir. Bununla birlikte katılımcıların %17,9'unun "*Kesinlikle Katılmıyorum*", %15,4'ünün "*Katılmıyorum*", şeklinde cevap vererek iş yükü getirmediği şeklinde görüş bildirdiği, Diğer taraftan %12,8'inin "Kesinlikle Katılıyorum", %25,8'in "*Katılıyorum*" şeklinde cevap vererek ISO27001 süreçlerinin kendilerine ek iş yükü getirdiği yönünde cevap verdikleri görülmüştür.

5.1.9. ISO27001 Bilgi Güvenliği ve Yönetim Sistemi üst yönetim olarak bu sistem içerisindeki ayrıcalıkları hakkındaki görüşleri.

Kurulmuş olan BGYS kapsamında yönetici statüsünde bulunan personelin ayrıcalıklı olup olamamaları gerektiği konusunda sorulan soruya vermiş oldukları cevaplara ilişkin frekans ve yüzdelik dağılımları Çizelge 5.9'da verilmiştir.

Çizelge 5.9. Yönetici anketi soru -9 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	13	16,7	16,7	
Katılmıyorum	16	20,5	37,2	
Kararsızım	15	19,2	56,4	**3,08**
Katılıyorum	20	25,6	82,1	
Kesinlikle Katılıyorum	14	17,9	100,0	

Sorulan sorunun olumsuz ifade içermesi sebebiyle verilen cevapların değerlendirilmesi aşamasında ters kodlama yapılmıştır. Verilen cevaplar incelendiğinde ise yöneticilerin %17,9'unun "*Kesinlikle Katılıyorum*", %25,6'sının ise "*Katılıyorum*" şeklinde cevap vererek ayrıcalıklı olmaları gerektiği yönünde görüş bildirdikleri görülmektedir. Diğer taraftan %16,7'lik bölümünün "*Kesinlikle Katılmıyorum*", %20,5'lik bölümünün ise "*Katılmıyorum*" şeklinde cevap vererek ayrıcalıklı olmamaları gerektiği yönünde görüş bildirdikleri ve geri kalan %19,2'lik bölümünün ise bu konuda kararsız olduğu görülmektedir.

5.1.10. ISO27001 in sağladığı kurum dışı ve kurum içi güvenlik hakkındaki görüşleri

ISO27001 sahibi kurumların kurum dışından gelecek olan tehlikelerin yanı sıra kurum içerisinden gelebilecek tehlikelere karşı da bir korunmaya sahip olup olmadıkları yönündeki düşüncelere ilişkin sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.10'da verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,88 olması genel görüşün olumlu olduğu yönünde değerlendirilmektedir

Çizelge 5.10. Yönetici anketi soru -10 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	1	1,3	1,3	**3,88**
Katılmıyorum	6	7,7	9,0	
Kararsızım	9	11,5	20,5	
Katılıyorum	47	60,3	80,8	
Kesinlikle Katılıyorum	15	19,2	100,0	

Katılımcıların %19,2'sinin "*Kesinlikle Katılıyorum*", %60,3'ünün "*Katılıyorum*" şeklinde cevap vererek olumlu yönde görüş bildirdiği, %11,5'lik bölümünün kararsız görüş bildirdiği ve geri kalan bölümünün ise olumsuz yönde görüş bildirdiği görülmektedir.

5.1.11. Genel ve yerel güvenlik problemleri karşısından ISO27001 sağlayacağı koruma hakkındaki görüşleri

ISO27001 sahibi kurumların sahip oldukları BGYS'nin muhtemel bilgi güvenliği olaylarına kurumu ve kurum personelini koruyup koruyamayacağı ile ilgili düşüncelere ilişkin sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.11'de verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,78 olması genel görüşün olumlu olduğu yönünde değerlendirilmektedir

Çizelge 5.11. Yönetici anketi soru -11 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	1	1,3	1,3	**3,78**
Katılmıyorum	8	10,3	11,5	
Kararsızım	9	11,5	23,1	
Katılıyorum	49	62,8	85,9	
Kesinlikle Katılıyorum	11	14,1	100,0	

Toplamda %11,5'lik bir bölümün "*Kesinlikle Katılmıyorum*" ve "*Katılmıyorum*" şeklinde cevap verdiği görülmektedir. Diğer taraftan katılımcıların %14,1'inin "*Kesinlikle Katılıyorum*", %62,8'inin "*Katılıyorum*" şeklinde cevap verdiği görülmüştür. Buradan büyük çoğunluğun ISO27001'in sağlayacağı katkının olumlu olacağı görüşünün ağır bastığı görülmektedir.

5.1.12. ISO27001 sertifikasyonunun ve kurulan BGYS'nin verimliliği arasındaki ilişki hakkındaki görüşleri

Kurumların sahip oldukları BGYS'lerin verimli ve etkin bir şekilde yönetilebilmesi ISO27001 sertifikasyonunun gerekli olup olmadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.12'de verilmiştir.

Çizelge 5.12. Yönetici anketi soru -12 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	5,1	5,1	
Katılmıyorum	12	15,4	20,5	
Kararsızım	14	17,9	38,5	**3,56**
Katılıyorum	32	41,0	79,5	
Kesinlikle Katılıyorum	16	20,5	100,0	

Verilen cevaplar incelendiğinde katılımcıların %20,5'lik bir bölümünün "*Kesinlikle Katılıyorum*", %41'lik bölümünün "*Katılıyorum*" şeklinde cevap vererek sertifikasyonun etkinlik noktasında gerekli olduğu, %20,5'lik bölümünün ise "*Kesinlikle Katılmıyorum*" ve "*Katılmıyorum*" şeklinde cevap vererek BGYS yönetimi için sertifikasyon gerekmediği şeklinde ve yaklaşık %17,9'lik bölümünün ise "*Kararsızım*" şeklinde görüş bildirdiği görülmektedir.

5.2. Bilgi Güvenliği Yönetim Sistemi Ekip Üyelerinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Düşünceleri

Bu bölümde ISO27001 sahibi kamu kurumlarının BGYS kurulumu ve işletilmesinden sorumlu personellerden elde edilen veriler incelenecektir. 6 kamu kurumundan toplam 42 ekip üyesi yapılan ankete katılım sağlamıştır. Sorulan sorularda BGYS ekip üyelerin kurumlarında yürüttükleri görevler ve BGYS hakkındaki görüşlerinin alınması planlanmıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar soru bazlı olarak incelenmiştir.

5.2.1. Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilmesi amacıyla alınan danışmanlık hizmetlerinin gerekliliği hakkındaki görüşleri

Kurumların büyük bir bölümünün, personellerinin BGYS kurulumu ve yönetimi konusunda yeterli tecrübeye sahip olmamaları sebebiyle profesyonel kuruluşlardan danışmanlık hizmeti alımı yapmaları söz konusu olabilmektedir. Kurumlarda BGYS hizmetlerini yürütmek ve

devamlılığını sağlamak ile görevli personellere, kurumlarında danışmanlık hizmetine ihtiyaç olup olmadığı yönünde iletilen soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.13'de verilmiştir.

Çizelge 5.13. BGYS ekip anketi soru -1 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	6,8	6,8	
Katılmıyorum	5	11,4	18,2	
Kararsızım	6	13,6	31,8	**3,77**
Katılıyorum	15	34,1	65,9	
Kesinlikle Katılıyorum	15	34,1	100,0	

Verilen cevaplar incelendiğinde katılımcıların yaklaşık "*Kesinlikle Katılıyorum*" ve "*Katılıyorum*" cevaplarının eşit oranda %34,1 olduğu görülmüştür. Buradan büyük bir çoğunluğun danışmanlık hizmetlerinin gerekli olduğu yönünde görüş sonucu çıkarılabilir. Diğer taraftan %6,8 oranında "*Kesinlikle Katılmıyorum*", %11,4 oranında "*Katılmıyorum*" cevabı verildiği ve danışmanlık hizmetine ihtiyaç olmadığı yönünde ve 13,6'lık bölümünün ise karasız görüş bildirdiği görülmektedir.

5.2.2. Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilebilmesi için kurum personelinin yeterliliği hakkındaki görüşleri

BGYS süreçlerinin yönetilmesi, sürekliliğinin sağlanması ve sürekli geliştirilmesi amacıyla oluşturulan BGYS yönetim ekip üyelerinin kurum personellerinden oluşması ve üst yönetim tarafından gerekli görevlendirilmelerin yapılması zorunludur. Bu kapsamda BGYS ekip üyelerinin ilgili süreçlerin yönetimi ve sürekliliğinin sağlanması konusunda yeterli olup olmadığı yönündeki soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.14'de verilmiştir.

Çizelge 5.14. BGYS ekip anketi soru -2 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	9,1	9,1	
Katılmıyorum	8	18,2	27,3	
Kararsızım	19	43,2	70,5	**2,98**
Katılıyorum	11	25,0	95,5	
Kesinlikle Katılıyorum	2	4,5	100,0	

Verilen cevaplar incelendiğinde katılımcıların büyük oranda, kurum personelini ya yetersiz gördüğü ya da bu konuda kararsız kaldığı görülmektedir. Katılımcıların %4,5'lik bölümünün "Kesinlikle Katılıyorum", %25'lik bölümünün ise "*Katılıyorum*" cevabı vererek toplamda sadece %29,5'lik bölümünün bu konuda olumlu görüş bildirdiği görülmüştür. Diğer taraftan %43,2'lik "*Kararsızım*" cevabı ile katılımcıların büyük çoğunluğunun yeterlilikler konusunda kararsız kaldıkları görülmüştür. Verilen cevapları ortalaması 2,98'dir ve bu değer genel değerlendirmenin olumsuz yönde olduğu görüşünü desteklemektedir.

5.2.3. Ekip üyelerinin eğitim ihtiyaçları hakkındaki görüşleri

BGYS ekip üyelerinin, bilgi güvenliği süreçlerinin, ilgili politika ve prosedürlerin uygulanmasının ve tanımlanmış risklerin etkin bir şekilde işletilebilmesi amacıyla herhangi bir eğitime ihtiyaçlarının olup olmadığı yönündeki soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.15'de verilmiştir.

Çizelge 5.15. BGYS ekip anketi soru -3 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	6,8	6,8	
Katılmıyorum	2	4,5	11,4	
Kararsızım	2	4,5	15,9	**4,30**
Katılıyorum	9	20,5	36,4	
Kesinlikle Katılıyorum	28	63,6	100,0	

Verilen cevaplar incelendiğinde katılımcıların %63,6lık bölümünün "*Kesinlikle Katılıyorum*" ve %20,5'lik bir bölümünün "*Katılıyorum*" şeklinde cevap vererek ekip üyelerinin eğitim ihtiyaçları olduğu yönünde ve geri kalan %16'lık bölümünün ise bu konuda çekimser veya ihtiyaç olmadığı yönünde görüş bildirdikleri görülmektedir. Verilen cevapları ortalaması 4,30 olarak hesaplanmıştır.

5.2.4. Ekip üyelerinin bilişim personellerinden oluşup oluşmaması gerektiği hakkındaki görüşleri

Üst yönetim tarafından kurumsal BGYS süreçlerinin yönetilmesi amacıyla oluşturulması gereken ekip üyelerinin tamamının bilişim personellerinden oluşup oluşmaması gerektiği

yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.16'da verilmiştir.

Çizelge 5.16. BGYS ekip anketi soru -4 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	6,8	6,8	
Katılmıyorum	11	25,0	31,8	
Kararsızım	11	25,0	56,8	**3,18**
Katılıyorum	13	29,5	86,4	
Kesinlikle Katılıyorum	6	13,6	100,0	

Verilen cevaplar incelendiğinde katılımcılar arasında görüş birliği olmadığı, görüşlerin herhangi bir cevap üzerinde yoğunlaşmadığı görülmüştür. Bahse konu soruya ilişkin olarak %32'lik "*Kesinlikle Katılmıyorum*" ve "Katılıyorum" şeklinde cevap vererek bir bölümünün BGYS ekip üyelerinin bilişim personellerinden oluşmaması gerektiği yönünde, %25'lik bölümünün çekimser ve geri kalan %43'lük bölümün ise "*Kesinlikle Katılıyorum*" ve "*Katılıyorum*" şeklinde cevap vererek BGYS ekip üyelerinin bilişim personellerinden oluşması gerektiği yönünde görüş bildirdikleri görülmektedir. Verilen cevapları ortalaması 3,18 olarak hesaplanmıştır.

5.2.5. BGYS ekip üyelerinin sayısı hakkındaki görüşleri

Üst yönetim tarafından kurumsal BGYS süreçlerinin yönetilmesi amacıyla oluşturulan ekip üyeleri sayısının süreçlerin sağlıklı bir şekilde yönetilebilmesi için yeterli olup olmadığı yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.17'de verilmiştir.

Çizelge 5.17. BGYS ekip anketi soru -5 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	5	11,4	11,4	
Katılmıyorum	12	27,3	38,6	
Kararsızım	12	27,3	65,9	**2,91**
Katılıyorum	12	27,3	93,2	
Kesinlikle Katılıyorum	3	6,8	100,0	

Verilen cevaplar incelendiğinde katılımcılar arasında genel anlamda bir görüş birliği olmadığı, genel ortalamanın ise 2,91 olarak hesaplandığı ve genel görüşün olumsuz olarak değerlendirilebileceği görülmüştür. Bahse konu soruya ilişkin olarak "*Kesinlikle Katılmıyorum*", "*Katılmıyorum*" ve "*Kararsızım*" şeklinde görüş bildirerek %66'lık bölümünün BGYS ekip üyelerinin sayısal anlamda yetersiz olduğu yönünde veya bu konuda çekimser olduğu geri kalan %34'lük bölümünün ise "*Katılıyorum*" ve "*Kesinlikle Katılıyorum*" yönünde cevap vererek BGYS ekip üyelerinin sayısının yeterli olduğu yönünde görüş bildirdikleri görülmektedir.

5.2.6. BGYS yönetimi ile kurum personeli arasındaki çalışma uyumu hakkındaki görüşleri

BGYS ekip üyelerinin, BGYS süreçlerinin etkin ve sağlıklı bir şekilde yönetebilmesi için özellikler sistemin en önemli paydaşlarından olan kurum personeli ile uyumlu bir çalışma gerçekleştirip gerçekleştirmediği yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.18'de verilmiştir.

Çizelge 5.18. BGYS ekip anketi soru -6 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	2	4,5	4,5	
Katılmıyorum	8	18,2	22,7	
Kararsızım	15	34,1	56,8	**3,25**
Katılıyorum	15	34,1	90,9	
Kesinlikle Katılıyorum	4	9,1	100,0	

Verilen cevaplar incelendiğinde katılımcıların %4,5'inin "*Kesinlikle Katılmıyorum*", %18,2'sinin ise "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %34,1'lik bölümünün bu konuda kararsız kaldığı ve geri kalan %43,2'lik bölümünün ise "*Kesinlikle Katılıyorum*" ve "*Katılıyorum*" şeklinde görüş bildirerek kurum personeli ile sağlıklı bir çalışma yürütebildiği yönünde olumlu görüş bildirdikleri görülmektedir. Genel ortalama ise 3,25 olarak hesaplanmıştır.

5.2.7. Kurumsal risk çalışmalarının yürütülmesi hakkındaki görüşleri

BGYS kapsamında yapılan çalışmaların en önemli unsurlarından biri olan kurumsal risklerin belirlenmesi ve belirlenen riskler üzerinde yapılması gereken çalışmaların takip edilerek

risklerin olası etkilerinin en aza indirilmesi gerekmektedir. Bahse konu çalışmaların sağlıklı ve etkin bir şekilde işletilebilmesi için kurum personelleri ile yapılan çalışmalar büyük önem arz etmektedir. Bu kapsamda kurumsal risk süreçlerinin işletilmesi sırasından kurum personeli tarafından beklenen desteğin alınıp alınamadığı yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.19'da verilmiştir.

Çizelge 5.19. BGYS ekip anketi soru -7 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	9,1	9,1	
Katılmıyorum	15	34,1	43,2	
Kararsızım	10	22,7	65,9	**2,84**
Katılıyorum	14	31,8	97,7	
Kesinlikle Katılıyorum	1	2,3	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 2,84 olması genel görüşün olumsuz olduğu yönünde değerlendirilmektedir. Katılımcıların %43,2'sinin "*Kesinlikle Katılmıyorum*" ve "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %23'lük bölümünün bu konuda kararsız kaldığı ve geri kalan %34'lük bölümünün ise "*Kesinlikle Katılıyorum*" ve "*Katılıyorum*" şeklinde görüş bildirerek kurum personeli ile risk süreçlerinin işletilmesi çalışmalarında yeterince destek alınabildiği yönünde olumlu görüş bildirdikleri görülmektedir.

5.2.8. ISO27001 süreçlerinin uygulanabilirliği hakkındaki görüşleri

BGYS kapsamında yapılan çalışmaların ve kurumsal BGYS süreçlerinin sağlıklı bir şekilde uygulanıp uygulanamadığı yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.20'de verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,00 olduğu ve görüşlerin genel olarak kararsıza yakın olduğu görülmektedir.

Çizelge 5.20. BGYS ekip anketi soru -8 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	5	11,4	11,4	**3,00**
Katılmıyorum	8	18,2	29,5	
Kararsızım	17	38,6	68,2	
Katılıyorum	10	22,7	90,9	
Kesinlikle Katılıyorum	4	9,1	100,0	

Katılımcıların %11,4'ünün "*Kesinlikle Katılmıyorum*", %18,2'sinin "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %38,6'lık bölümünün bu konuda kararsız kaldığı ve geri kalan %31,8'lik bölümünün ise "*Kesinlikle Katılıyorum*" ve "*Katılıyorum*" şeklinde görüş bildirerek kurumsal BGYS süreçlerinin sağlıklı bir şekilde işletilebildiği yönünde görüş bildirdikleri görülmektedir.

5.2.9. ISO27001 Standardının bilgi güvenliği açısından gerekliliği hakkındaki görüşleri

ISO27001 sertifikasyon sürecinin kurumsal BGYS süreçlerinin etkin bir şekilde yürütülebilmesi için gerekli olduğunu düşünüp düşünmedikleri yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.21'de verilmiştir.

Çizelge 5.21. BGYS ekip anketi soru -9 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	9,1	9,1	**3,80**
Katılmıyorum	3	6,8	15,9	
Kararsızım	5	11,4	27,3	
Katılıyorum	18	40,9	68,2	
Kesinlikle Katılıyorum	14	31,8	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,80 olduğu ve olumlu görüşün daha ağı bastığı görülmektedir. Katılımcıların yaklaşık %9,1'inin "*Kesinlikle Katılmıyorum*" ve %6,8'inin "*Katılmıyorum*" şeklinde cevap vererek olumsuz görüş bildirdiği, %11,4'ünün bu konuda kararsız kaldığı ve %31,8'lik bölümünün "*Kesinlikle Katılıyorum*", %40,9'luk bölümün ise "Katılıyorum" şeklinde cevap verdiği ve ISO27001 sertifikasyonun BGYS

süreçlerinin etkin bir şekilde yürütülebilmesi için gerekli olduğu yönünde olumlu görüş bildirdikleri görülmektedir.

5.2.10. ISO27001 kurum dışı ve kurum içi güvenliğin sağlanması hakkındaki görüşleri

ISO27001 sertifikasyon sahibi olan kurumların kurum içi veya kurum dışından gelmesi muhtemel bilgi güvenliği olaylarına karşı tam olarak güvenli olup olmadıkları yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.22'de verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,20 olduğu görülmektedir. Katılımcıların %9,1'inin "*Kesinlikle Katılmıyorum*", %13,6'sının "*Katılmıyorum*" şeklinde cevap vererek olumsuz görüş bildirdiği, yaklaşık %36,4'lük bölümünün bu konuda kararsız kaldığı görülmüştür.

Çizelge 5.22. BGYS ekip anketi soru -10 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	9,1	9,1	
Katılmıyorum	6	13,6	22,7	
Kararsızım	16	36,4	59,1	**3,20**
Katılıyorum	13	29,5	88,6	
Kesinlikle Katılıyorum	5	11,4	100,0	

Diğer taraftan kalan %40,9'luk bölümünün ise "*Kesinlikle Katılıyorum*" ve "*Katılıyorum*" şeklinde cevap vererek ISO27001 sertifikasyon sahibi olmanın ilgili kurumu hem dış hem de iç güvenlik açısından tam olarak koruyabileceği yönünde olumlu görüş bildirdikleri görülmüştür.

5.2.11. ISO27001 kapsamında alınan güvenlik önlemleri hakkındaki görüşleri

ISO27001 sertifikasyon sahibi olan kurumların, sistem kapsamında alınan önlemler ile kurum içinden veya kurum dışından gelmesi muhtemel kritik bilgi güvenliği problemlerine karşı sistemin kendilerini koruyup koruyamayacağı yönündeki soruya yine ekip üyeleri

tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.23'de verilmiştir.

Çizelge 5.23. BGYS ekip anketi soru -11 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	6,8	6,8	
Katılmıyorum	8	18,2	25,0	
Kararsızım	9	20,5	45,5	**3,30**
Katılıyorum	21	47,7	93,2	
Kesinlikle Katılıyorum	3	6,8	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,30 olduğu görülmektedir. Katılımcıların yaklaşık %6,8'inin "*Kesinlikle Katılmıyorum*", %18,2'sinin "Katılmıyorum" şeklinde cevap vererek bu konuda olumsuz görüş bildirdiği görülmüştür. Diğer taraftan %20,5'lik bölümünün kararsız kaldığı ve %6,8'lik bölümün "*Kesinlikle Katılıyorum*", %47,7'lik bölümünün ise "*Katılıyorum*" şeklinde cevap verdiği ve ISO27001 sertifikası sahibi kurumların yapmış olduğu çalışmalar kapsamında almış olduğu önlemlerin kurum içinden veya kurum dışından gelebilecek kritik bilgi güvenliği problemlerine karşı koruyabileceği yönünde olumlu görüş bildirdikleri görülmektedir.

5.2.12. ISO27001 sistemine geçiş sürecindeki personelin alışkanlıklarını terk edebilmesi hakkındaki görüşleri

ISO27001 sertifikasyon sahibi olan kurumlar, BGYS çalışmaları kapsamında kurumsal süreçleri gözden geçirerek, ilgili süreçlerin bilgi güvenliği çerçevesinde yeniden değerlendirilmesi ve bilgi güvenliğini tehlikeye düşürmesi muhtemel durumları ortadan kaldırmak amacıyla gerekli değişiklikleri yapmakla yükümlüdürler. Yapılan değişiklikler doğrultusunda kurum personelinin alışkanlıklarını değiştirmekte zorlanıp zorlanmadıkları yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.24'de verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,73 olduğu görülmektedir.

Çizelge 5.24. BGYS ekip anketi soru -12 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	6,8	6,8	**3,73**
Katılmıyorum	6	13,6	20,5	
Kararsızım	6	13,6	34,1	
Katılıyorum	14	31,8	65,9	
Kesinlikle Katılıyorum	15	34,1	100,0	

Katılımcıların toplam %20,4'ünün "*Kesinlikle Katılmıyorum*" ve "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %13,6'lık bölümünün kararsız kaldığı ve geri kalan %65,9'luk bölümünün ise "*Kesinlikle Katılıyorum*" ve "Katılıyorum" şeklinde cevap vererek kurum personelinin değişiklikler konusunda alışkanlıklarını değiştirme konusunda zorlandıkları yönünde görüş bildirdikleri görülmektedir.

5.2.13. ISO27001 sisteminin bilişim personeli üzerindeki iş yükü hakkındaki görüşleri

ISO27001 sertifikasyon sürecini tamamlanmış ve etkin bir şekilde BGYS süreçlerini işleten bir kurumda bilişim personeli üzerindeki iş yükünün azalıp azalmadığı yönündeki soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.25'de verilmiştir.

Çizelge 5.25. BGYS ekip anketi soru -13 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	15	34,1	34,1	**2,27**
Katılmıyorum	13	29,5	63,6	
Kararsızım	8	18,2	81,8	
Katılıyorum	5	11,4	93,2	
Kesinlikle Katılıyorum	3	6,8	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 2,27 olduğu ve genel anlamda bilişim personelinin iş yükünün azalmadığı yönünde görüşün ağır bastığı görülmektedir. Katılımcıların %34,1'inin "*Kesinlikle Katılmıyorum*" ve %29,5'inin "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği ve bilişim personeli iş yükünün arttığı, %18,2'lik bölümünün kararsız kaldığı ve geri kalan toplam %18,2'lik bölümünün "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde cevap vererek ISO27001 sertifikasyonunun

kurum bilişim personeline herhangi bir iş yükü getirmediği yönünde görüş bildirdiği görülmektedir.

5.2.14. ISO27001 çerçevesinde uygulanan politika ve prosedürlerin geçerliliği hakkındaki görüşleri

ISO27001 sertifikasyon süreci tamamlanmış ve etkin bir şekilde BGYS süreçlerini kapsamında uygulanan politika ve prosedürlerin kurumsal süreçlere sağladığı katkılara ilişkin sorulan soruya yine ekip üyeleri tarafından verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.26'da verilmiştir.

Çizelge 5.26. BGYS ekip anketi soru -14 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	6,8	6,8	**3,14**
Katılmıyorum	9	20,5	27,3	
Kararsızım	16	36,4	63,6	
Katılıyorum	11	25,0	88,6	
Kesinlikle Katılıyorum	5	11,4	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,14 olduğu görülmektedir. Katılımcıların toplam %27,3'lük bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %36,4'lük bölümünün kararsız kaldığı ve %11,4'ünün "*Kesinlikle Katılıyorum*", %25'lik bölümünün ise "*Katılıyorum*" şeklinde cevap vererek olumlu yönde görüş bildirdikleri görülmektedir.

5.3. Teknik Personelin Bilgi Güvenliği Yönetim Sistemi ve Yeterlilikler Hakkındaki Görüşleri

Bu bölümde ISO27001 sahibi kamu kurumlarında görevli, ağ uzmanı, sistem uzmanı yazılım uzmanı vb. teknik personellerden elde edilen veriler incelenecektir. 6 kamu kurumunda görevli toplam 90 teknik personel yapılan ankete katılım sağlamıştır. Sorulan sorularda kurumsal BGYS ve ISO27001 süreçleri hakkında teknik personellerin görüşlerinin alınması planlanmıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar soru bazlı olarak incelenmiştir.

5.3.1. BGYS süreçlerinin sağlıklı bir şekilde yürütülmesi için teknik personelin yeterlilikleri hakkındaki görüşleri

ISO27001 sertifikasyon sürecini tamamlanmış bir kamu kurumda görevli teknik personelin, kurumsal BGYS süreçlerinin sağlıklı bir şekilde yürütülebilmesi için teknik açıdan yeterli olup olmadıkları yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.27'de verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,16 olduğu ve farklı görüşlerin eşit oranda dağılım gösterdiği görülmektedir.

Çizelge 5.27. Teknik ekip anketi soru -1 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	8	8,9	8,9	
Katılmıyorum	28	31,1	40,0	
Kararsızım	8	8,9	48,9	**3,16**
Katılıyorum	34	37,8	86,7	
Kesinlikle Katılıyorum	12	13,3	100,0	

Katılımcıların %8,9'u "*Kesinlikle Katılmıyorum*" ve %31,1'i "*Katılmıyorum*" şeklinde cevap vererek bu konuda olumsuz görüş bildirdiği, yaklaşık %8,9'luk bölümünün bu konuda kararsız kaldığı ve geri kalan %51,1'lik bölümünün ise "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde görüş bildirerek bahse konu soruya olumlu yanıt verdiği yani teknik ekiplerinin yeterli olduğunu düşündükleri görülmektedir.

5.3.2. ISO27001 standardının kurumsal bilişim süreçlerinde uygulanabilirliği hakkındaki görüşleri

ISO27001 standardı ile gelen ve kurumların bilişim süreçlerini etkileyen politika ve prosedürlerin uygulanabilir olup olmadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.28'de verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,71 olduğu ve olumlu görüşün ağır bastığı görülmektedir.

Çizelge 5.28. Teknik ekip anketi soru -2 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	2	2,2	2,2	**3,71**
Katılmıyorum	7	7,8	10,0	
Kararsızım	18	20,0	30,0	
Katılıyorum	51	56,7	86,7	
Kesinlikle Katılıyorum	12	13,3	100,0	

Katılımcıların toplam %10'luk bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %20'lik bölümünün ise bu konuda kararsız kaldığı görülmektedir. Diğer taraftan geri kalan %13,3'lük bölümünün "*Kesinlikle Katılıyorum*" ve %56,7'lik bölümünün "Katılıyorum" şeklinde olumlu yanıt verdiği yani ISO27001 standardının kurumsal süreçlerde uygulanabilir olduğu yönünde görüş bildirdiği tespit edilmiştir.

5.3.3. ISO27001 ile ilgili eğitim/eğitimler gerekliliği hakkındaki görüşleri

ISO27001 standardına sahip kamu kurumlarında görevli teknik personellerin görevlerinin yanı sıra ayrıca ISO27001 ile ilgili eğitimlere de ihtiyaç olup olmadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.29'da verilmiştir.

Çizelge 5.29. Teknik ekip anketi soru -3 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	4,4	4,4	**4,08**
Katılmıyorum	5	5,6	10,0	
Kararsızım	5	5,6	15,6	
Katılıyorum	42	46,7	62,2	
Kesinlikle Katılıyorum	34	37,8	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 4,08 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların %10'luk bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %5,6'lık bölümünün ise bu konuda kararsız kaldığı görülmektedir. Diğer taraftan %37,8'lik bölümünün "*Kesinlikle Katılıyorum*", %46,7'lik bölümünün ise "*Katılıyorum*" şeklinde olum görüş bildirdiği

görülmektedir. Buradan teknik ekip üyelerinin büyük çoğunluğunun ISO27001 ile ilgili eğitimler almasının faydalı olacağı yönünde görüş bildirdiği tespit edilmiştir.

5.3.4. ISO27001 süreçlerinin teknik ekip üyelerine sağladığı faydalar hakkındaki görüşleri

ISO27001 standardına sahip kamu kurumlarında görevli teknik personellere yöneltilen bu soruda, ilgililerin görevlerini daha etkin ve sağlıklı bir şekilde yürütebilmeleri noktasında ISO27001 standardının olumlu yönde katkı sağlayıp sağlamadığı anlaşılmaya çalışılmıştır. Verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.30'da verilmiştir. Verilen cevaplar incelendiğinde, genel ortalamanın 3,59 olduğu ve olumlu görüşün ağır bastığı görülmektedir.

Çizelge 5.30. Teknik ekip anketi soru -4 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	3,3	3,3	
Katılmıyorum	9	10,0	13,3	
Kararsızım	23	25,6	38,9	**3,59**
Katılıyorum	42	46,7	85,6	
Kesinlikle Katılıyorum	13	14,4	100,0	

Katılımcıların %3,3'ünün "*Kesinlikle Katılmıyorum*" ve %10'luk bölümünün "*Katılmıyorum*" şeklinde olumsuz görüş bildirdikleri görülmüştür. Diğer taraftan %25,6'lık bölümünün ise bu konuda kararsız kaldığı, geri kalan yaklaşık %61,1'lik bölümünün ise bahse konu soruya "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde olumlu yanıt verdiği yani ISO27001'in görevlerinin etkin ve sağlıklı bir şekilde yürütülebilmesi noktasında faydalı olacağı yönünde görüş bildirdiği tespit edilmiştir.

5.3.5. ISO27001 kapsamında alınan önlemlerin sağladığı katkılar hakkındaki görüşleri

BGYS'ye sahip kamu kurumlarının, ISO27001 standardizasyon sürecini tamamladıktan sonra, önceki dönemlere göre yaşanan bilgi güvenliği olaylarında azalma olup olmadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.31'de verilmiştir.

Çizelge 5.31. Teknik ekip anketi soru -5 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	3,3	3,3	
Katılmıyorum	5	5,6	8,9	
Kararsızım	15	16,7	25,6	**3,82**
Katılıyorum	49	54,4	80,0	
Kesinlikle Katılıyorum	18	20,0	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,82 olduğu ve olumlu görüşün daha ağır bastığı görülmektedir. Katılımcıların %8,9'luk bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %16,7'lik bölümünün bu konuda kararsız kaldığı ve diğer taraftan %20'lik bölümünün "*Kesinlikle Katılıyorum*", %54,4'lük bir oranının "*Katılıyorum*" şeklinde bahse konu soruya olumlu yanıt verdiği yani ISO27001'in sonrasında bilgi güvenliği olaylarında azalma yaşandığı yönünde görüş bildirdiği görülmüştür.

5.3.6. ISO27001 Standardının, geliştirilen kurumsal uygulamaların güvenliğine sağladığı olumlu katkılar hakkındaki görüşleri

BGYS'ye sahip kamu kurumlarında geliştirilen kurumsal uygulamaların güvenliğine ISO27001 standardizasyon sürecinin olumlu bir katkı sağlayıp sağlamadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.32'de verilmiştir.

Çizelge 5.32. Teknik ekip anketi soru -6 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	2	2,2	2,2	
Katılmıyorum	5	5,6	7,8	
Kararsızım	11	12,2	20,0	**3,91**
Katılıyorum	53	58,9	78,9	
Kesinlikle Katılıyorum	19	21,1	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,91 olduğu ve olumlu görüşün daha ağır bastığı görülmektedir. Katılımcıların yaklaşık %2,2'sinin "*Kesinlikle Katılmıyorum*", %5,6'sının "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %12,2'lik bölümünün bu

konuda kararsız kaldığı görülmüştür. Diğer taraftan geri kalan toplam %80'lik bölümünün "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde yanıt vererek bahse konu soruya olumlu yanıt verdiği tespit edilmiştir.

5.3.7. ISO27001'in bilgi güvenliği ihlal olaylarının azalmasına katkıları ile ilgili görüşleri

ISO27001 sertifikasına sahip kamu kurumlarında, standardizasyon sürecinin bilgi güvenliği ihlal olaylarının azalması noktasında olumlu bir katkı sağlayıp sağlamadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.33'de verilmiştir.

Çizelge 5.33. Teknik ekip anketi soru -7 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	2	2,2	2,2	**3,72**
Katılmıyorum	5	5,6	7,8	
Kararsızım	20	22,2	30,0	
Katılıyorum	52	57,8	87,8	
Kesinlikle Katılıyorum	11	12,2	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,72 olduğu ve olumlu görüşün daha ağır bastığı görülmektedir. Katılımcıların toplam %7,8'lik bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %22,2'lik bölümünün bu konuda kararsız kaldığı görülmüştür. Geri kalan toplam %70'lik bölümünün "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" cevabı vererek ISO27001 standardizasyonunun bilgi güvenliği olaylarının azalmasına olumlu yönde katkı sağladığı şeklinde görüş bildirdikleri tespit edilmiştir.

5.3.8. ISO27001'in düzenleyici ve önleyici faaliyetlerin uygulanabilirliği ile ilgili görüşleri

ISO27001 uyum süreçleri ve BGYS çalışmaları kapsamında yürütülen risk yönetim ve denetim süreçleri kapsamında tespit edilen bilgi güvenliği açıklarının ve sonrasında yapılacak işlemlerin belirlenmesi gerekmektedir. Bahse konu işlemlerden biri olan düzenleyici ve önleyici faaliyetlerin bilgi güvenliği yönetim sürecinde ilgili kuruma faydalı

yönde katkı sağlayıp sağlamadığı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.34'de verilmiştir.

Çizelge 5.34. Teknik ekip anketi soru -8 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	2	2,2	2,2	
Katılmıyorum	6	6,7	8,9	
Kararsızım	2	2,2	11,1	**4,09**
Katılıyorum	52	57,8	68,9	
Kesinlikle Katılıyorum	28	31,1	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 4,09 olduğu ve olumlu görüşün belirgin bir şekilde ağır bastığı görülmektedir. Katılımcıların toplam %8,9'luk bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %2,2'lik bölümünün bu konuda kararsız kaldığı görülmüştür. Diğer taraftan %31,1'lik oranının "*Kesinlikle Katılıyorum*", %57,8'lik oranının "*Katılıyorum*" şeklinde görüş bildirerek düzenleyici ve önleyici faaliyetlerin olumlu yönde katkı sağladığını düşündükleri görülmüştür.

5.3.9. ISO27001 kapsamında alınan güvenlik önlemlerinin katkıları ile ilgili görüşleri

ISO27001 uyum süreçleri ve BGYS çalışmaları kapsamında alınan önlemlerin artırılması ve sistemin daha fazla sıkılaştırılması sonucu sistem üzerinde daha az problem yaşanıp yaşanmayacağı yönünde sorulan soruya verilen cevaplara ait frekans ve yüzdelik dağılım bilgileri Çizelge 5.35'de verilmiştir.

Çizelge 5.35. Teknik ekip anketi soru -9 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	1	1,1	1,1	
Katılmıyorum	8	8,9	10,0	
Kararsızım	13	14,4	24,4	**3,92**
Katılıyorum	43	47,8	72,2	
Kesinlikle Katılıyorum	25	27,8	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,92 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların toplam %10'luk bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %14,4'lük bölümünün bu konuda kararsız kaldığı, %27,8'inin "*Kesinlikle Katılıyorum*" ve %27,8'inin "*Katılıyorum*" şeklinde görüş bildirerek bahse konu önlemlerin artırılması sonrasında daha az bilgi güvenliği olayı yaşanacağı yönünde olumlu katkı sağladığını düşündükleri görülmüştür.

5.3.10. ISO27001'in olası risklerin önceden tespiti ile ilgili görüşleri

ISO27001 uyum süreçleri ve kontrol maddelerinin sağlanması durumunda kurumsal bilgi güvenliği risklerinin gerçekleşmeden önce tespit edilebilip edilemeyeceği yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.36'da verilmiştir.

Çizelge 5.36. Teknik ekip anketi soru -10 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	3	3,3	3,3	**3,91**
Katılmıyorum	4	4,4	7,8	
Kararsızım	12	13,3	21,1	
Katılıyorum	50	55,6	76,7	
Kesinlikle Katılıyorum	21	23,3	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,91 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların yaklaşık %7,7'lik bölümünün "*Kesinlikle Katılmıyorum*" ve "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %13,3'lük bölümünün bu konuda kararsız kaldığı, %23,3'lük bölümünün "*Kesinlikle Katılıyorum*" ve %55,6'sının ise "*Katılıyorum*" şeklinde cevap vererek toplamda %78,9'luk oranın bahse konu soruya olumlu yönde görüş bildirdiği görülmüştür. Buradan da bilgi güvenliği risklerinin önceden tespitine olumlu yönde katkı sağlandığı şeklinde olumlu görüş bildirildiği görülmektedir.

5.4. Kurum Personellerinin Bilgi Güvenliği Yönetim Sistemi ve Farkındalık Eğitimleri Hakkındaki Görüşleri

Bu bölümde ISO27001 sahibi kamu kurumlarında görevli personelden elde edilen veriler incelenecektir. Personele sorulan sorular ile personelin bilgi güvenliği yönetim sistemi çalışmaları kapsamında almış oldukları farkındalık eğitimleri, sistem ile ilgili genel görüşleri hakkında bilgi sahibi olunmaya çalışılmıştır. 6 kamu kurumunda görevli toplam 329 personel yapılan ankete katılım sağlamıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar aşağıda soru bazlı olarak incelenmiştir.

5.4.1. ISO27001 hakkında verilen bilgilendirme eğitimlerinin süreleri hakkındaki görüşleri

ISO27001 süreçlerinin en önemlilerinden birisi de kurumsal bilgi güvenliği farkındalığının oluşturulmasıdır. Bu kapsamda kurum personeline görevleri doğrultusunda çeşitli bilgilendirme eğitimleri verilmektedir. Verilen eğitimlerin süresinin yeterli olup olmadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.37'de verilmiştir.

Çizelge 5.37. Personel anketi soru -1 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	13	4,0	4,0	**3,56**
Katılmıyorum	40	12,2	16,1	
Kararsızım	61	18,5	34,7	
Katılıyorum	181	55,0	89,7	
Kesinlikle Katılıyorum	34	10,3	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,56 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların toplamda %16,2'lik bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde cevap vererek olumsuz görüş bildirdiği, %18,5'lik bölümünün bu konuda kararsız kaldığı, geri kalan toplam %65,3'lük bölümünün ise bahse konu soruya "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde olumlu yönde cevap verdiği yani verilen eğitimlerin süresinin yeterli olduğu şeklinde görüş bildirdiği görülmüştür.

5.4.2. ISO27001 hakkında verilen bilgilendirme eğitimlerinin içerikleri hakkındaki görüşleri

BGYS kapsamında kurum personeline verilen eğitimlerin içeriğinin yeterli olup olmadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.38'de verilmiştir.

Çizelge 5.38. Personel anketi soru -2 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	8	2,4	2,4	**3,54**
Katılmıyorum	43	13,1	15,5	
Kararsızım	78	23,7	39,2	
Katılıyorum	162	49,2	88,4	
Kesinlikle Katılıyorum	38	11,6	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,54 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların %2,4'ünün "*Kesinlikle Katılmıyorum*", %13,1'lik bölümünün "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %23,7'lik bölümünün ise bu konuda kararsız kaldığı görülmüştür. Diğer taraftan %11,6'lik bölümünün "*Kesinlikle Katılıyorum*" ve %49,2'sinin "*Katılıyorum*" şeklinde cevap vererek bahse konu soruya olumlu yönde cevap verdiği yani verilen eğitimlerin içeriklerinin yeterli olduğu şeklinde görüş bildirdiği görülmüştür.

5.4.3. ISO27001 kapsamında yürütülen farkındalık eğitimleri esnasında verilen materyallerin yeterliliği hakkındaki görüşleri

BGYS kapsamında kurum personeline verilen eğitimler esnasında verilen materyal ve örneklerin yeterli veya güncel olup olmadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.39'da verilmiştir.

Verilen cevaplar incelendiğinde, genel ortalamanın 3,50 olduğu ve olumlu görüşün ağır bastığı görülmektedir.

Çizelge 5.39. Personel anketi soru -3 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	12	3,6	3,6	**3,50**
Katılmıyorum	30	9,1	12,8	
Kararsızım	99	30,1	42,9	
Katılıyorum	159	48,3	91,2	
Kesinlikle Katılıyorum	29	8,8	100,0	

Katılımcıların %3,6'sının "*Kesinlikle Katılmıyorum*", %9,1'inin "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %30,1'lik bölümünün bu konuda kararsız kaldığı, geri kalan toplam %57,1'lik bölümünün ise "*Kesinlikle Katılmıyorum*" ve "*Katılıyorum*" şeklinde bahse konu soruya olumlu yönde cevap verdiği yani eğitimler esnasında verilen materyallerin ve örneklerin yeterli olduğu şeklinde görüş bildirdiği görülmüştür.

5.4.4. Bilgi güvenliği farkındalık eğitimlerinin faydası hakkındaki görüşleri

BGYS kapsamında kurum personeline verilen eğitimlerin, bilgi güvenliği farkındalığı oluşturma ve güncel tehditler hakkında bilgi sahibi olma noktasında faydalı olup olmadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.40'da verilmiştir.

Çizelge 5.40. Personel anketi soru -4 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	10	3,0	3,0	**3,81**
Katılmıyorum	25	7,6	10,6	
Kararsızım	54	16,4	27,1	
Katılıyorum	168	51,1	78,1	
Kesinlikle Katılıyorum	72	21,9	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,81 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların toplamda %10,6'lık bölümünün "*Kesinlikle Katılmıyorum*" ve "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %16,4'lük bölümünün bu konuda kararsız kaldığı, %21,9'luk bölümünün "*Kesinlikle Katılıyorum*", %51,1'lik bölümünün ise bahse konu soruya "*Katılıyorum*" şeklinde olumlu yönde cevap verdiği yani toplamda %73'lük bölümünün eğitimlerin kendileri için faydalı olduğu şeklinde görüş bildirdiği görülmüştür.

5.4.5. Farkındalık eğitimleri kapsamında verilen bilgilerin kurumsal süreçler açısından uygulanabilirliğinin hakkındaki görüşleri

BGYS süreçleri kapsamında yapılan farkındalık eğitimlerinde verilen bilgilerin kurumsal süreçler açısından uygulanabilir olup olmadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.41'de verilmiştir.

Çizelge 5.41. Personel anketi soru -5 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	4	1,2	1,2	**3,70**
Katılmıyorum	27	8,2	9,4	
Kararsızım	80	24,3	33,7	
Katılıyorum	170	51,7	85,4	
Kesinlikle Katılıyorum	48	14,6	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,70 olduğu ve olumlu görüşün ağır bastığı görülmektedir. Katılımcıların toplamda %9,4'lük bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, yaklaşık %24,3'lük bölümünün bu konuda kararsız kaldığı, %14,6'lık bölümünün "*Kesinlikle Katılıyorum*", %51,7'lik bölümünün ise bahse konu soruya "*Katılıyorum*" şeklinde olumlu yönde cevap verdiği yani toplamda %66,3'lük oranda eğitimlerde verilen bilgilerin kurumsal süreçler açısından uygulanabilir olduğunun düşünüldüğü görülmüştür.

5.4.6. Farkındalık eğitimlerinin içeriği hakkındaki görüşleri

BGYS süreçleri kapsamında yapılan farkındalık eğitimlerinin süresinden ziyade içeriklerinin önemli olması gerekip gerekmediği yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.42'de verilmiştir.

Çizelge 5.42. Personel anketi soru -6 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	10	3,0	3,0	**4,08**
Katılmıyorum	11	3,3	6,4	
Kararsızım	44	13,4	19,8	
Katılıyorum	143	43,5	63,2	
Kesinlikle Katılıyorum	121	36,8	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 4,08 olduğu ve oldukça önemli bir çoğunluğun olumlu görüş bildirdiği görülmektedir. Katılımcıların toplam %6,3'lük bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği, %13,4'lük bölümünün bu konuda kararsız kaldığı, toplamda %80,3'lük bölümünün "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde bahse konu soruya olumlu yönde cevap verdiği yani farkındalık eğitimlerinin süresinden ziyade içeriklerinin önemli olduğu yönünde görüş bildirdikleri görülmüştür.

5.4.7. Farkındalık eğitimlerinin yöntemi hakkındaki görüşleri

BGYS süreçleri kapsamında yapılan farkındalık eğitimlerinin sadece slaytlar üzerinden yapılmasının yeterli olup olmadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.43'de verilmiştir.

Çizelge 5.43. Personel anketi soru -7 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	38	11,6	11,6	
Katılmıyorum	108	32,8	44,4	
Kararsızım	89	27,1	71,4	**2,77**
Katılıyorum	79	24,0	95,4	
Kesinlikle Katılıyorum	15	4,6	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 2,77 olduğu olumsuz görüşün ağırlıkta olduğu görülmektedir. Katılımcıların %11,6'sının "*Kesinlikle Katılmıyorum*", %32,8'lik bölümünün "*Katılmıyorum*" şeklinde olumsuz görüş bildirdiği yani slaytların eğitimlerin etkin bir şekilde yapılabilmesi için yeterli olmadığı, %27,1'lik bölümünün bu konuda kararsız kaldığı, geri kalan %28,6'lık bölümünün ise bahse konu soruya olumlu yönde cevap verdiği yani slaytlar üzerinden yapılan eğitimim yönteminin yeterli olduğu yönünde görüş bildirdiği görülmüştür.

5.4.8. Farkındalık eğitimi veren firmanın yeterlilikleri hakkındaki görüşleri

BGYS süreçleri kapsamında yapılan farkındalık eğitimlerinde, eğitim veren firmaların veya eğitmenlerin diğer kurumlardan da edindiği tecrübeleri personele aktarıp aktarmadığı

yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.44'de verilmiştir.

Çizelge 5.44. Personel anketi soru -8 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	15	4,6	4,6	
Katılmıyorum	37	11,2	15,8	
Kararsızım	102	31,0	46,8	**3,41**
Katılıyorum	148	45,0	91,8	
Kesinlikle Katılıyorum	27	8,2	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,41 olduğu ve olumlu görüşlerin ağırlıkta olduğu görülmektedir. Katılımcıların toplam %15,8'lik bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde bu konuda olumsuz görüş bildirdiği görülmüştür. %31'lik bölümünün ise bu konuda kararsız kaldığı belirlenmiştir. Diğer taraftan katılımcıların %8,2'sinin "*Kesinlikle Katılıyorum*", %45'lik bölümünün ise "*Katılıyorum*" şeklinde bahse konu soruya olumlu yönde cevap verdiği, eğitim alınan firma veya eğitmenlerin diğer kurumlardan edindiği en güncel bilgi ve tecrübeleri aktardığı yönünde olumlu görüş bildirdiği görülmüştür.

5.4.9. BGYS kapsamında alınan güvenlik önlemlerin yetkiler üzerindeki etkileri hakkındaki görüşleri

BGYS süreçleri kapsamında ilgili politika ve prosedürlerle belirlenmiş, bilgi sistemleri üzerinde alınan önlemlerin ve yapılan kısıtlamaların personelin yetkilerini aşırı derecede kısıtlayıp kısıtlamadığı yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.45'de verilmiştir.

Çizelge 5.45. Personel anketi soru -9 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	31	9,4	9,4	
Katılmıyorum	109	33,1	42,6	
Kararsızım	90	27,4	69,9	**2,83**
Katılıyorum	82	24,9	94,8	
Kesinlikle Katılıyorum	17	5,2	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 2,83 olduğu görülmektedir. Katılımcıların %9,4'ünün "*Kesinlikle Katılmıyorum*", %33,1'inin "*Katılmıyorum*" şeklinde cevap vererek bu konuda olumsuz görüş bildirdiği yani yetkilerin aşırı derece de kısıtlanmadığı yönünde görüş bildirdikleri görülmüştür. %27,4'lük bölümünün ise bu konuda kararsız kaldığı görülmüştür. Diğer taraftan geri kalan toplamda %30,1'lik bölümünün ise "*Kesinlikle Katılıyorum*" veya "*Katılıyorum*" şeklinde cevap vererek bahse konu soruya olumlu yönde cevap verdiği, yani yetkilerinin aşırı derece kısıtlandığı yönünde görüş bildirdikleri görülmüştür.

5.4.10. Kurumsal BGYS'nin iyi bir şekilde yönetilip yönetilmediği ile ilgili görüşleri

ISO27001 sertifikasyon sürecini tamamlanmış kamu kurumlarında, kurum personeline yöneltilen, BGYS süreçlerinin iyi bir şekilde yürütülüp yürütülmediği yönünde sorulan soruya verilen cevaplara ilişkin frekans ve yüzdelik dağılım bilgileri Çizelge 5.46'da verilmiştir.

Çizelge 5.46. Personel anketi soru -10 cevap dağılımı

	Sayı(Adet)	*Oran(%)*	*Toplam Oran(%)*	***Ortalama***
Kesinlikle Katılmıyorum	8	2,4	2,4	
Katılmıyorum	19	5,8	8,2	
Kararsızım	89	27,1	35,3	**3,71**
Katılıyorum	159	48,3	83,6	
Kesinlikle Katılıyorum	54	16,4	100,0	

Verilen cevaplar incelendiğinde, genel ortalamanın 3,71 olduğu görülmektedir. Katılımcıların toplamda %8,2'lik bölümünün "*Kesinlikle Katılmıyorum*" veya "*Katılmıyorum*" şeklinde cevap vererek bu konuda olumsuz görüş bildirdiği ve %27,1'lik bölümünün bu konuda kararsız kaldığı görülmüştür. Diğer taraftan %16,4'ünün "*Kesinlikle Katılıyorum*", %48,3'ünün ise "*Katılıyorum*" şeklinde cevap vererek olumlu yönde görüş bildirdiği görülmüştür. Sonuç olarak toplamda %64,7 bölümünün bahse konu soruya olumlu yönde cevap verdiği, yürütülen BGYS'nin iyi bir şekilde yönetildiği şeklinde görüş bildirdikleri görülmüştür.

6. SONUÇ VE ÖNERİLER

Bu bölümde uygulanan anket sorularına verilen cevaplar doğrultusunda elde edilen sonuçlar ve bu sonuçlar doğrultusunda geliştirilen önerilere yer verilmiştir.

6.1. Sonuç

Kurumsal bilgi güvenliği yönetimlerinin veya bu sistemlerin herhangi bir standardizasyona uyumlu hale getirilmiş olması, kurumsal süreçlerde bilgi güvenliğinin tam olarak sağlandığı anlamına gelmediği açıktır. Kurulan sistemlerin, özellikle kurum yönetimi ve tüm kademeleriyle kurum personeli tarafından sahiplenilmesi büyük önem arz etmektedir. Bu sebeple özellikle ISO27001 uyum süreçlerinin olmazsa olmaz unsurlarından biri de sistemin arkasında sağlam bir iradenin varlığının kanıtlanması ve bu iradenin ilgili süreçlerin etkin bir şekilde yürütülebilmesi için gerekli çalışmaları yapmış olduğunu kanıtlaması beklenmektedir. Diğer taraftan kurulan BGYS süreçlerinin, gerek teknik personel tarafından gerekse operasyonel süreçleri yürüten personel tarafından anlaşılması ve sahiplenilmesi de büyük önem arz etmektedir. Bu kapsamda da ISO27001 tüm kademeden personel için yapılması zorunlu bir takım bilgilendirme ve farkındalık oluşturma çalışmalarını zorunlu tutar.

Bilgi güvenliğinin insan, teknoloji ve süreç, üç temel unsurudur ve bu üç unsurdan herhangi birinin aksaması bilgi güvenliğinin tam olarak sağlanamayacağı anlamına gelmektedir. Bu üç unsur teknolojik gelişmeler ve değişimler sebebiyle sürekli güncelliğini korumalıdır. Teknoloji ve süreç unsurları her ne kadar kusursuz ve güncel bir şekilde kurgulanmış ve konumlandırılmış olursa olsun insan unsuru gelişmeler ve değişimler karşısında güncel olmadığı sürece bir anlam ifade etmemektedir. Bu sebeple insan unsurundan ötürü kurumsal bilgi güvenliği yönetimlerinin etkinliği ve sürekliliği devamlı sorgulanmaktadır ve sorgulanmalıdır.

Bu tez çalışmasında, bilgi güvenliğinin en önemli unsuru olan kurum personeli üzerinde bir araştırma yapılmıştır. Bu kapsamda, ISO27001 sertifikası sahibi olan kamu kurumlarının çeşitli kademe ve görevlerden personel grupları üzerinden incelenmesine yer verilmiştir. İnceleme sonucunda elde edilen bulgular ve sonuçlar aşağıda sunulmuştur.

Kurum yönetici kademelerinin vermiş olduğu cevaplar incelendiğinde, genel anlamda ISO27001 standardizasyon süreçleri ve kurumsal katkıları yönünde olumlu görüşün hâkim olduğu görülmektedir. ISO27001 in genel anlamda kurumlar için gerekli olduğu ve kurumsal anlamda itibar ve güven göstergesi olduğu yönünde görüşlerin ağır bastığı görülmektedir. Diğer taraftan ISO27001'in kurumsal bilgi güvenliği hedeflerine erişmesinde ve BGYS kapsamında geliştirilen kurumsal politikaların işletilmesi ve etkinliğinin artırılmasına katkı sağladığı konusunda da yönetici kademesinin olumlu görüş bildirdikleri görülmektedir. Aynı zamanda kurumsal bilgi güvenliği farkındalığı oluşturma noktasında da ISO27001 olumlu yönde katkı sağladığı düşünülmektedir.

ISO27001 sertifikasyon sürecinin ve BGYS'nin gerekliliklerinin yerine getirilmesi noktasında yönetim desteğinin büyük önem arz ettiği ve bu noktada yönetim kademesinin üzerine düşen görevlerin kabul edilebilir seviyede olduğu görüşü de elde edilen verilerden çıkarılan önemli sonuçlardan biridir. Diğer taraftan ISO27001 ile gelen yetkilendirme politikaları kapsamında yöneticilerin ayrıcalıklı olmaları gerektiği ve ilgili BGYS süreçlerinin ek iş yükü getirip getirmediği noktasında yöneticiler arasında fikir birliği olmadığı görülmektedir. Ek iş yükü getirdiğini düşünen yönetici sayısı ile getirmediği düşünen ve ayrıcalık sahibi olmaları gerektiğini düşünen ve düşünmeyen yönetici sayılarının birbirine yakın olduğu görülmüştür. Genel anlamda yönetim kademesinin ISO27001 süreçlerini olumlu buldukları ve sürecin kurumsal bilgi güvenliğine olumlu yönde katı sağladığını düşündükleri görülmüştür.

ISO27001 uyum süreçlerinin yönetilmesi ve geliştirilmesi amacıyla oluşturulmuş olan BGYS ekip üyeleri tarafından verilmiş cevaplar incelendiğinde, öncelikli olarak ekip üyelerinin ISO27001 in kurumsal bilgi güvenliğinin sağlanması noktasında gerekli olduğunu düşündükleri görülmektedir. Bu görüşle paralel olarak, ISO27001'in kurumu iç ve dış tehditlere karşı koruma noktasında faydalı olduğu yönünde görüş bildirildiği de görülmüştür. ISO27001 uyum süreçlerin kurumun sahip olduğu sayısal anlamda insan kaynağı ile yönetilmesinin zor olduğu ve kurum dışından profesyonel danışmanlık desteği alınması gerektiği yönünde görüşün ağır bastığı görülmüştür. Bununla birlikte, kurumlar sahip oldukları insan kaynağının, tecrübe ve bilgi açısından yetersiz olduğu, süreçlerin yönetiminin sağlıklı bir şekilde yürütülebilmesi amacıyla BGYS ekip üyelerinin eğitimler alması gerektiğini düşündükleri görülmektedir. Bununla birlikte kurulacak olan BGYS ekibinin bilişim personellerinden oluşup oluşmaması gerektiği yönünde bir fikir birliği

olmadığı zıt görüşlerin ve kararsızların sayılarının birbirine yakın olduğu görülmüştür. ISO27001 uyum süreçleri kapsamında kurum personeli ile uyumlu çalışma yapılabileceği fakat kurumsal bilgi güvenliği risk süreçlerinin yönetimi noktasında yeterli desteğin alınamadığı yönünde görüş bildirildiği görülmektedir.

Kurum personelinin ISO27001 ile gelen süreç değişikliklerine, eski alışkanlıklarını terk etmekte zorlandıkları için uyum sağlamakta güçlük çektikleri yönünde görüşün daha ağır bastığı da görülmüştür. Bilişim personeli açısından bakıldığında ise ISO27001'in iş yükünü azaltıp azaltmadığı sorusuna, iş yükünün azalmadığı yönünde geri dönüşün daha fazla olduğu görülmüştür. Genel anlamda bakıldığında, BGYS ekiplerinin gerek tecrübe, gerek sayısal olarak yeterli olmadıklarını ve eğitime ihtiyaç duyduklarını düşündükleri, personel ile çalışma noktasında özellikle risk çalışmalarında yeterli desteği göremedikleri yönünde görüş bildirdikleri görülmüştür. ISO27001'in her ne kadar kurum için gerekli olduğu yönünde görüş bildirilmiş olsa da iş yükünün azalmadığı yönünde de görüş bildirildiği görülmüştür.

Kurumlarda görevli bilgi sistemleri ve teknik altyapının yönetiminden ve kurumsal ihtiyaçlar doğrultusunda çözümler üretmekle görevli teknik personelin vermiş olduğu cevaplar incelendiğinde genel olarak sorumlu teknik personelin teknik açıdan ve sayısal yeterli olup olmadığı noktasında bir görüş birliği olmadığı görülmektedir. Bunun sebebi olarak faklı kamu kurumlarında yer alan teknik ekip sayı yeterliliklerin farklılık göstermesi olduğu düşünülmektedir. ISO27001 in kurumsal teknik süreçler üzerinde uygulanabilir olduğu görüşünün ağır bastığı görülmektedir. Aynı zamanda teknik ekiplerinde ISO27001 süreçleri hakkında eğitim ihtiyaçlarının olduğu yönünde görüş bildirdikleri de görülmüştür. Diğer taraftan teknik ekip tarafından geliştirilen kurumsal uygulamalarının güvenliğine de ISO27001 uyum sürecinin olumlu yönde katkı sağladığı şeklindeki görüşlerin ağırlıkta olduğu görülmüştür. Aynı zamanda verilen cevaplar doğrultusunda, ISO27001'e geçiş ile birlikte yaşanan bilgi güvenliği olaylarının sayısında önemli ölçüde bir azalma olduğu yönünde de değerlendirme yapılabilmektedir.

Kurum personelinin genel farkındalık seviyeleri, almış oldukları eğitimler ve BGYS hakkındakileri düşüncelerinin öğrenilmeye çalışıldığı bu bölümde alınan cevaplar incelendiğinde, genel olarak personelin almış oldukları farkındalık eğitimlerinden memnun oldukları, içeriklerinin ve sürelerinin yeterli olduğu fakat sadece slaytlar üzerinde yapılan

eğitimlerin yeterli olmayacağı şeklinde görüş bildirdikleri görülmüştür. Aynı zamanda eğitim firmalarının veya eğitmenlerin eğitimde vermiş oldukları bilgilerin güncel ve diğer kurumlar elde etmiş oldukları bilgileri de içerdiği yönünde görüş bildirdikleri görülmüştür. Bununla birlikte personelin yetkilerinin aşırı derece kısıtlanıp kısıtlanmadığı şeklindeki soruya verilen cevapta ise olumlu ve olumsuz cevapların birbirine yakın olduğu farklı görüşler arasında çok önemli bir fark olmadığı görülmüştür.

Sonuç olarak, Personel açısından yapılan inceleme sonucunda ise kurum personeline verilen bilgi güvenliği farkındalık eğitimlerinin içeriği, süresi ve sağladığı fayda açısından olumlu bulunduğu görülmüştür. Diğer taraftan personel tarafında da uygulanan kontrolleri ve yetki kısıtlamalarının çok fazla olduğu yönünde görüşlerin olduğu da görülmektedir. Genel anlamda personel tarafında kurulan sisteme karşı bir güven olduğu, ISO27001 in kurum personeli tarafından benimsendiği ve kurumlarında BGYS süreçlerinin etkin bir şekilde yönetildiğini düşündükleri yönünde görüş bildirdikleri görülmüştür.

6.2. Öneriler

Bu bölümde uygulanan anket çalışmalarından elde edilen bulgulara dayalı olarak geliştirilen öneriler aşağıda farklı başlıklar altında verilmiştir.

Yönetim kademesine yönelik öneriler

- Yönetim kademesinin büyük oranda üzerine düşen sorumluluklar konusunda bilgi sahibi olmadıkları görülmüştür. Bunun için Siber Eylem Planları veya genelgelerle yönetim kademesine özel yönlendirmeler yapılabilir.
- Yönetim kademesine uygun farkındalık ve sahiplenme seviyelerinin ölçümünün yapılabilmesi amacıyla bir çalışma yapılabilir.
- BGYS çalışmalarının öneminin özellikle yönetim kademesine daha detaylı aktarılarak sahiplenme seviyelerinin artırılması sağlanabilir.
- Kurulan bilgi güvenliği yönetim sisteminin gerekliliğin yönetim kademesi tarafından daha iyi algılanabilmesi için risk çalışmaları dâhil edilmesi sağlanabilir.
- Kamu yöneticileri ile bir çalışma yürütülerek ortak BGYS kurulum yönergesi oluşturulması üzerinde çalışılabilir.

- Kamu yöneticileri ile birlikte kamu kurumlarına özel risk ve fırsatların çalışması yapılabilir.

BGYS ekibine yönelik öneriler

- BGYS ekiplerinin kurulumuna daha fazla özen gösterilmelidir. Kurulan ekibin sorumlulukları net bir şekilde belirlenmeli ve eğitim seviyesi uygun personeller arasından seçilmelidir.
- BGYS ekip üyelerinin sayılarının yetersiz olduğu düşünülmektedir. Bu konuda kurum personel sayısı ile doğru orantılı olacak şekilde ekip üyeleri belirlenmelidir.
- Ekip üyeleri her ne kadar farkındalık eğitimlerinde kurum personeline tanıtılıyor olsa da personelin büyük çoğunluğunun ekip üyelerini tanımadıkları görülmüştür. Bununla ilgili bilgilendirmelerin daha etkin bir şekilde yapılması sağlanabilir.
- Ekip üyelerinin çalışmalarının kolaylaştırılması amacıyla, üst yönetim tarafından tüm birimlerden atama yolu ile görevlendirmeler yapılarak ve kurum personelinin de BGYS yönetim süreçlerini sahiplenmesi sağlanabilir.
- BGYS ekip üyelerinin kurumsal risk çalışmalarında kurum personeli ile uyumlu bir şekilde çalışamadığı tespit edilmiştir. Bu süreçte görevlendirilen kurum personeline risk belirleme ve işleme konularında eğitim verilmesi sürecin daha etkin bir şekilde yönetilmesine katkı sağlayabilir.
- BGYS ekip üyelerinin sahiplenme seviyelerinin artırılması amacıyla çalışmalar yapılabilir.
- BGYS ekip üyelerinin kendilerini yetersiz buldukları ve eğitim ihtiyaçları olduğu yönünde görüş bildirdikleri görülmüştür. Bu kapsamda ihtiyaç duyulacak tüm eğitim içeriğinin belirlenmesi ve görevlendirme öncesinde tüm eğitimlerin alınması sağlanabilir.
- BGYS ekip üyelerinin tamamen bilgi işlem personellerinden oluşmaması gerektiği yönünde bir görüş bildirenlerin olduğu görülmüştür. Ekip üyelerine bilgi işlem personeli dışında da görevlendirmeler yapılabilir.
- BGSY ekip üyeleri ile ilgili daha detaylı bir çalışma yapılarak, ekip üyelerinin görev tanımlarının netleştirilmesi ve hatta ekibe özel kadro çalışması yapılması sağlanabilir.
- BGYS ekip üyelerinin görev tanımları siber eylem planları veya yönergeler ile desteklenebilir.

Teknik ekibe yönelik öneriler

- Teknik personel sayılarının yetersiz olduğu yönünde görüşün ağırlıklı bir şekilde dile getirildiği görülmüştür. Bu kapsamda teknik ekip üyelerinin sayılarının artırılması sağlanmalıdır.
- ISO27001 konusunda teknik ekiplerin bilgi seviyelerinin yeterli olmadığı fakat buna rağmen süreci sahiplendikleri görülmektedir. Bunun sebebi olarak operasyonel süreçlerin yönetilmesi sistemin olumlu yönde katkı sağladığı düşünülebilir. Bu sebeple teknik ekibin ISO27001 hakkında farkındalık seviyelerinin artırılması sebebiyle temel BGYS eğitimleri verilebilir.
- Yazılım ekiplerinin, çalışmaları sırasında bilgi güvenliği konularına daha fazla özen göstermeleri sağlanabilir. Bu kapsamda güvenli kod geliştirme, temel BGYS, temel ağ güvenliği gibi giriş seviyesinde eğitimler verilerek farkındalık seviyelerinin artırılması sağlanabilir.
- BGYS kapsamında yapılan sızma testlerine yazılım ekiplerinin daha aktif katılımları sağlanabilir.

Personele yönelik öneriler

- Farkındalık eğitimlerinin sunumlardan ziyade uygulamalı şekilde ve somut örnekler üzerinden verilmesinin daha faydalı olacağı düşünülmektedir.
- Farkındalık eğitimlerinin sürelerinin ve içeriklerinin yeterli olduğu fakat içeriğinin her eğitimde aynı olmasının katılım isteğini olumsuz yönde etkilediği görülmüştür. Bu sebeple eğitim süreleri mümkün olduğu kadar kısa ve eğitim içeriği de her eğitimde değiştirilerek planlanabilir.
- BGYS kapsamında alınan önlemler doğrultusunda yapılan kısıtlamaların personelin bir kısmı tarafından fazla bulunduğu görülmüştür. Bunun personelin farkındalık seviyeleri ile ilişkili olduğu düşülmektedir. Farkındalık eğitimlerinde özellikle yetkilendirmeler ile ilgili bilgilendirmelere ağırlık verilmesi sağlanabilir.

İlerde yapılabilecek araştırmalara yönelik öneriler

- Anket katılım oranlarının yüz yüze yapılan anketlerde daha fazla olduğu görülmüştür. Yapılması muhtemel benzer çalışmalarda katılım oranının artırılması için anketlerin elektronik ortamın yanı sıra yüz yüze de yapılması sağlanabilir.

- Yapılan çalışma yönetim kademesi özeline indirgenerek derinleştirilebilir.
- Üst yönetim ile daha alt kademedeki yönetimler arasında ISO27001 ile ilgili görüş ayrılıkları olduğu sonucuna varılmıştır. Sonraki çalışmalardaki bunun nedenleri araştırılabilir.
- Özellikle kamu kurumlarında anket uygulama izinlerinin alınabilmesinin zor olduğu ve bununla ilgili titiz bir çalışma gerektiği unutulmamalıdır.
- Yapılan çalışma Ankara ili sınırlandırılmıştır. Araştırmanın kamu kurumları taşra teşkilatını veya özel sektör kuruluşlarını da kapsayacak şekilde genişletilmesi sağlanabilir.
- Yapılan çalışma kamu kurumu yöneticilerine indirgenerek daha derinlemesine bir çalışma yürütülebilir.
- Yapılacak sonraki çalışmalar danışmanlık firmaları ve eğitmenler açısından da incelenebilir.
- Kamu kurumlarının genelinde veya herhangi bir kamu kurumunun özelinde mevzuat ve ISO27001 arasındaki ilişki hukuksal yönden incelenebilir.
- Kamu kurumlarında KVKK ve ISO27001 arasındaki ortak veya ayrışan yönlerin araştırması yapılabilir.

KAYNAKLAR

1. Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report.* 14(4), 186-196.

2. Arce, I. (2003). The weakest link revisited [information security]. *IEEE Security & Privacy.* 1(2), 72-76.

3. Asosheh, A., Hajinazari P., ve Khodkari H. (2013). A practical implementation of ISMS. in *7th International Conference on e-Commerce in Developing Countries:with focus on e-Security*. 2013 of Conference. Kish Island, Iran.

4. Canbek, G. ve Sağıroğlu Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi.* 9(3), 165-174.

5. Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective.* 19(3), 132-141.

6. Rhodes-Ousley, M. (2013). ed.^eds. Information Security, Complete Reference. (Issue), McGraw-Hill Education: San Francisco.

7. İnternet: UDHB (2017). KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ. URL: http://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm. Son Erişim Tarihi: 03.05.2019

8. İnternet: TDK (2018). Güncel Türkçe Sözlük. URL: http://www.tdk.org.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c077623a1d893.11548437. Son Erişim Tarihi: 04.03.2019

9. İnternet: Bours, D. (2015). The Answer is 42. On Data, Information and Knowledge. URL: https://www.climate-eval.org/blog/answer-42-data-information-and-knowledge. Son Erişim Tarihi: 09.05.2019

10. Hilton, B.C. (2001). *Information warfare: An evolving perspective,* Baylor University Master of Science in Information Systems, Texas, USA

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

12. İnternet: Governence, I. (2017). Implementing an ISMS. URL: https://www.itgovernance.co.uk/blog/how-to-implement-an-isms. Son Erişim Tarihi: 17.07.2019

13. İnternet: Başaranoğlu, İ.E. (2016). Bilgi Güvenliği Unsurları. URL: https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/. Son Erişim Tarihi: 04.02.2019

14. Kılıç, M.Ç. ve Gökçöl O. (2010). Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi. in *3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu*. Ankara.

15. Achmadi, D., Suryanto Y. ve Ramli K. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. in *2018 International Workshop on Big Data and Information Security (IWBIS)*. Jakarta, Indonesia.

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

17. Morse, E.A. ve Raval V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review.* 24(6), 540-554.

18. İnternet: ISACA (2019). ISACA Web Sayfası. URL: http://www.isaca.org/COBIT/Pages/default.aspx. Son Erişim Tarihi: 12.05.2019

19. Lainhart, J.W. (2000). COBIT™: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities. *Journal of Information Systems.* 14(s-1), 21-25.

20. Raflesia, S.P., Surendro K., ve Passarella R. (2017). The user engagement impact along information technology of infrastructure library (ITIL) adoption. in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*. Palembang, Indonesia.

21. Al-Aqeeli, S., Al-Rodhaan M., ve Tian Y. (2017). Privacy preserving risk mitigation strategy for access control in e-healthcare systems. in *2017 International Conference on Informatics, Health & Technology (ICIHT)*. Riyadh, KSA.

22. İnternet: ISO (2019). Uluslararası Standart Organizayonu Web Sayfası. URL: https://www.iso.org/. Son Erişim Tarihi: 04.01.2019

23. ISO/IEC (2017). *ISO/IEC:27003 Bilgi Güvenliği Yönetim Sistemleri - Rehberlik.*

24. ISO/IEC (2016). *ISO/IEC:27004 İzleme, Ölçüm, Analiz ve Değerlendirme*.

25. ISO/IEC (2015). *ISO/IEC:27006 Bilgi Güvenliği Yönetim Sistemlerinin Denetim ve Belgelendirmesini Sağlayan Kuruluşlar İçin Şartlar*.

26. ISO/IEC (2017). *ISO/IEC:27007 Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Rehber*.

27. von Solms, R. (1998). Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security*. 6(5), 224-225.

28. Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri,* Yüksek Lisans Tezi Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara

29. İnternet: UEKAE (2008). BGYS Kapsamı Belirleme Kılavuzu. 11]. URL: https://docplayer.biz.tr/101255-Bgys-kapsami-belirleme-kilavuzu.html. Son Erişim Tarihi: 17.07.2019

30. İnternet: Dilek, C. (2015). Kuruluşun Bağlamı Nasıl Tanımlanır? URL: http://5s.com.tr/iso-9001-2015de-kurulusun-baglami/. Son Erişim Tarihi: 04.03.2019

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

32. Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması. *Akademik Bilişim*, 511-516.

33. Matúš, H. ve Martın J. (2009). Implementatıon Of Securıty Controls Accordıng To ISO/IEC 27002 In A Small Organısatıon.

34. Kemmler, B. ve arkadaşları (2018). An Integrated Service and Security Management System. 6(1), 1 -12.

35. İnternet: TÜRKAK (2019). Türkiye Akreditasyon Kurumu. URL: http://www.turkak.org.tr/. Son Erişim Tarihi: 04.03.2019

36. İnternet: Kıraç, İ.S. (2015). Bilgi Teknolojileri Denetimi. URL: http://www.btdenetim.net/iso-27001-sertifika-ve-akreditasyon/. Son Erişim Tarihi: 12.02.2019

37. Humphreys, E. (2018). The Future Landscape of ISMS Standards. *Datenschutz und Datensicherheit - DuD*. 42(7), 421-423.

38. ISO/IEC (2013). *ISO/IEC:27001 Bilgi Güvenliği Yönetim Sistemi*.

39. Baykara, M., Daş R., ve Karadoğan İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. in *1st International Symposium on Digital Forensics and Security (ISDFS'13)*. Elazığ.

40. Shameli-Sendi, A., Aghababaei-Barzegar R., ve Cheriet M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*. 57, 14-30.

41. ISO/IEC (2018). *ISO 31000 Risk Yönetimi*.

42. Almeida, L. ve Respício, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems.* 27(sup1), 173-180.

43. Gaşpar, M.L. ve Popescu, S.G. (2018). Integratıon Of The Gdpr Requırements Into The Requırements Of The Sr En ISO/IEC 27001:2018 Standard, Integratıon Securıty Management System In A Software Development Company.

44. Nurul, A. (2018). Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. in *International Conference on Computation in Science and Engineering*. Jakarta, Indonesia.

45. Nurbojatmiko (2016). Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO Depok City. in *2016 4th International Conference on Cyber and IT Service Management*. Bandung, Indonesia.

46. İnternet: ISO (2017). Uluslararası Standart Organizasyonu 2017 İstatistik Raporu. URL: https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1. Son Erişim Tarihi: 07.01.2019

47. İnternet: UHDB (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. URL: http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf. Son Erişim Tarihi: 17.07.2019

48. King, K.E. (2017). *Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management*, Ph.D., Minneapolis, USA

49. Güldüren, C. (2015). *Yükseköğretim Kurumlarındaki Öğretim Elemanlarının Bilgi Güvenliği Farkındalık Düzeylerinin Değerlendirilmesi,* Doktora Tezi Ankara Üniversitesi Eğitim Bilimleri Enstitüsü, Ankara

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

51. Akay, İ.G. (2014). *Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları,* Bilecik Şey Edebali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik

52. Gürcan, İ.A. (2014). *Finans sektörü için bilgi güvenliği yönetim gereksinimlerinin ISO 27001 tabanlı incelenmesi,* Bahçeşehir Üniversitesi İstanbul

53. Ganbat, O. (2013). *Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması,* Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir

54. Haklı, T. (2012). *Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi,* Yüksek Lisans Tezi Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta

55. Shoraka, B. (2011). *An Empirical Investigation of the Economic Value of Information Security Management System Standards,* Ph.D., Nova Southeastern University Graduate School of Computer and Information Sciences, Florida, USA

56. Mete, H. (2010). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması,* Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya

57. Aydoğmuş, E. (2010). *Türkiye'deki organizasyonların bilgi güvenliği olgunluk seviyelerinin belirlenmesi ve ISO/IEC 27001:2005 standardına uyumluluklarının değerlendirilmesi,* İstanbul Teknik Üniversitesi Bilim ve Teknoloji Enstitüsü, İstanbul

EKLER

EK-1. Anket formları

A. Bilgi Güvenliği Yönetim Sisteminin Üst Yönetim Açısından İncelenmesi

Bölüm I. Kişisel Bilgiler

Aşağıda kişisel özelliklerinizin belirlenmesi amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) *işareti koyunuz.*

1. **Cinsiyet?**
   ( )Kadın ( )Erkek

2. **Yaşınız?**
   - 20 yaş ve altı
   - 21 – 30 yaş arası
   - 31 – 40 yaş arası
   - 41 – 50 yaş arası
   - 51 – 60 yaş arası
   - 60 yaş üzeri

3. **Öğrenim Düzeyiniz?**
   ( )Lise ( )Ön lisans ( )Lisans ( )Lisans Üstü

   ( )Doktora ( )Diğer

4. **Mesleğiniz?**
   …….

EK-1. (devam) Anket formları

Bölüm 2. ISO27001 Bilgi Güvenliği Yönetim Sistemi

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1.	ISO/IEC 27001 Standardının kurumumuz için gerekli olduğunu düşünüyorum.					
2.	ISO/IEC 27001 Sertifika sahibi olmanın ulusal ve uluslararası saygınlık kazandırdığını düşünüyorum					
3.	ISO/IEC 27001'in bilgi güvenliği alanındaki kurumsal hedeflerimize erişme konusunda kolaylık sağladığını düşünüyorum.					
4.	ISO/IEC 27001'in bilgi güvenliği politikalarının kurumsal süreçlerin uygulanması konusunda faydalı olduğunu düşünüyorum.					
5.	ISO/IEC 27001'in kurum yöneticilerinin bilgi güvenliği farkındalığına olumlu yönde katkı sağladığını düşünüyorum.					
6.	Bilgi Güvenliği Yönetim Sisteminin sürdürülebilir olması için yönetim desteğinin önemli olduğunu düşünüyorum					
7.	ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminde, yönetimin üzerine düşen görevlerin uygulanabilir olduğunu düşünüyorum.					
8.	ISO/IEC 27001 standardının uygulanmasının ek iş yükü getirdiğini düşünüyorum.					
9.	Üst yönetimin bilişim sistemleri içerisinde ayrıcalıklı olması gerektiğini düşünüyorum.					
10.	ISO/IEC 27001 in kurum dışı olduğu kadar kurum içi güvenliği de tam olarak sağladığını düşünüyorum.					
11.	ISO/IEC 27001 kapsamında genelde veya yerelde gerçekleşecek kritik bir güvenlik probleminde sistemin bizi koruyacağını düşünüyorum.					
12.	ISO/IEC 27001 sertifikasyonu sağlanmadan bilgi güvenliği yönetim sisteminin verimli olarak yönetilemeyeceğini düşünüyorum.					

EK-1. (devam) Anket formları

B. Bilgi Güvenliği Yönetim Sisteminin, Bilgi Güvenliği Yönetim Sistemi Ekip Üyeleri Açısından İncelenmesi

Bölüm I. Kişisel Bilgiler

Aşağıda kişisel özelliklerinizin belirlenmesi amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) *işareti koyunuz.*

1. **Cinsiyet?**
   ( )Kadın ( )Erkek

2. **Yaşınız?**
   - 20 yaş ve altı
   - 21 – 30 yaş arası
   - 31 – 40 yaş arası
   - 41 – 50 yaş arası
   - 51 – 60 yaş arası
   - 60 yaş üzeri

3. **Öğrenim Düzeyiniz?**
   ( )Ön lisans ( )Lisans ( )Lisans Üstü

   ( )Doktora ( )Diğer

4. **Mesleğiniz?**
   ……

EK-1. (devam) Anket formları

Bölüm 2. ISO27001 Yönetim Süreci

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1.	Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilmesi amacıyla mutlaka danışmanlık hizmeti alınması gerektiğini düşünüyorum.					
2.	Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilebilmesi için kurumumuz personelinin yeterli olduğunu düşünüyorum.					
3.	Bilgi Güvenliği yönetim Sistemi süreçlerinin yönetilmesi için ekip üyelerinin eğitim alması gerektiğini düşünüyorum.					
4.	Kurulacak olan ekibin bilişim personellerinden oluşması gerektiğini düşünüyorum.					
5.	Kurumumuz Bilgi Güvenliği yönetimi ekip üyelerinin sayısının ISO27001 süreçlerinin sağlıklı bir şekilde yönetilebilmesi için yeterli olduğunu düşünüyorum.					
6.	ISO/IEC 27001 süreçlerinin yönetimi esnasında kurum personeli ile sağlıklı bir çalışma yürütülebileceğini düşünüyorum.					
7.	Kurumsal risk çalışmaları sırasında kurum personelinden yeterince destek alınabileceğini düşünüyorum.					
8.	ISO/IEC 27001 süreçlerinin kurumumuzda sağlıklı bir şekilde uygulanabildiğini düşünüyorum.					
9.	ISO/IEC 27001 standardının kurumsal bilgi güvenliği açısından gerekli olduğunu düşünüyorum.					
10.	ISO/IEC 27001 kurum dışı olduğu kadar kurum içi güvenliği de tam olarak sağladığını düşünüyorum					
11.	ISO/IEC 27001 kapsamında alınan önlemlerin, kurum içinden veya dışından gelecek kritik bilgi güvenliği problemlerine karşı bizi koruyacağına inanıyorum.					
12.	ISO/IEC 27001 sistemine geçiş sürecinde insanların alışkanlıklarını terk etmelerinin zor olduğunu düşünüyorum.					
13.	ISO/IEC 27001 sistemine geçişin ardından bilişim personeli üzerindeki iş yükünün azaldığını düşünüyorum.					
14.	ISO/IEC 27001 çerçevesinde belirlenen politika ve prosedürlerin tıkanan kurumsal süreçlerini açtığını düşünüyorum.					

EK-1. (devam) Anket formları

C. Bilgi Güvenliği Yönetim Sisteminin Teknik Personel Ve Yeterlilikler Açısından İncelenmesi

Bölüm I. Kişisel Bilgiler

Aşağıda kişisel özelliklerinizin belirlenmesi amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) *işareti koyunuz.*

1. **Cinsiyet?**
   ( )Kadın ( )Erkek

2. **Yaşınız?**
   - 20 yaş ve altı
   - 21 – 30 yaş arası
   - 31 – 40 yaş arası
   - 41 – 50 yaş arası
   - 51 – 60 yaş arası
   - 60 yaş üzeri

3. **Öğrenim Düzeyiniz?**
   ( )Ön lisans ( )Lisans ( )Lisans Üstü
   ( )Doktora ( )Diğer

4. **Mesleğiniz?**
   …….

EK-1. (devam) Anket formları

Bölüm 2. ISO27001 Hakkındaki Genel Düşünceler

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1.	Bilgi Güvenliği Yönetim Sistemi süreçlerinin sağlıklı bir şekilde yürütülmesi için teknik personelin sayı bakımında yeterli olduğunu düşünüyorum.					
2.	ISO/IEC 27001 standardının kurumsal bilişim süreçlerinde uygulanabilir olduğunu düşünüyorum.					
3.	ISO/IEC 27001 ile ilgili eğitim/eğitimler almamız gerektiğini düşünüyorum.					
4.	ISO/IEC 27001 standardının uygulanmaya başlaması ile bilişim sistemlerinin yönetilmesinin kolaylaştığını düşünüyorum.					
5.	ISO/IEC 27001 görevimle ilgili süreçleri etkin ve zamanında yerine getirebilmemde fayda sağladığını düşünüyorum.					
6.	ISO/IEC 27001 kapsamında alınan önlemler sayesinde bilgi güvenliği olaylarında azalma yaşandığını düşünüyorum.					
7.	ISO/IEC 27001 standardının, geliştirilen kurumsal uygulamaların güvenliğine olumlu katkı sağladığını düşünüyorum.					
8.	ISO/IEC 27001 sayesinde, bilgi güvenliği ihlal olaylarının kontrol edilebilir noktaya geldiğini düşünüyorum.					
9.	Bilişim sistemlerinde tespit edilen aksaklıklar üzerinde düzenleyici ve önleyici faaliyetler uygulanmasının faydalı olduğunu düşünüyorum.					
10.	ISO/IEC 27001 kapsamında güvenlik açısından daha fazla önlem alınmış bir sistem üzerinde daha az problem yaşanacağını düşünüyorum.					
11.	ISO/IEC 27001 standardının bütün süreçlerinin en iyi şekilde işletilmesi durumunda olası risklerin önceden tespit edilebileceğini düşünüyorum.					

EK-1. (devam) Anket formları

D. Bilgi Güvenliği Yönetim Sisteminin Personel Açısından İncelenmesi

Bölüm I. Kişisel Bilgiler

Aşağıda kişisel özelliklerinizin belirlenmesi amacıyla sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) *işareti koyunuz.*

1. **Cinsiyet?**
   ( )Kadın ( )Erkek

2. **Yaşınız?**
   - 20 yaş ve altı
   - 21 – 30 yaş arası
   - 31 – 40 yaş arası
   - 41 – 50 yaş arası
   - 51 – 60 yaş arası
   - 60 yaş üzeri

3. **Öğrenim Düzeyiniz?**
   ( )Ön lisans ( )Lisans ( )Lisans Üstü

   ( )Doktora ( )Diğer

4. **Mesleğiniz?**
   …….

EK-1. (devam) Anket formları

Bölüm 2. ISO27001 Hakkındaki Genel Düşünceler

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1.	ISO/IEC 27001 hakkında verilen bilgilendirme eğitimlerini süresinin yeterli olduğunu düşünüyorum.					
2.	ISO/IEC 27001 hakkında verilen bilgilendirme eğitimlerinin içeriğinin yeterli olduğunu düşünüyorum.					
3.	ISO/IEC 27001 hakkında verilen bilgilendirme eğitimleri esnasında verilen materyal ve örneklerin yeterli ve güncel olduğunu düşünüyorum.					
4.	Almış olduğum bilgi güvenliği ile ilgili eğitimlerin faydalı olduğunu düşünüyorum.					
5.	Eğitimler kapsamında verilen bilgilerin kurumsal süreçler açısından uygulanabilir olduğunu düşünüyorum.					
6.	Danışmanlık kapsamında verilen eğitimlerin süresinden ziyade içeriklerinin dolu olması gerektiğini düşünüyorum.					
7.	Eğitimlerin sadece slaytlar üzerinden yapılmasının yeterli olduğunu düşünüyorum.					
8.	Eğitimi veren firmanın diğer müşterilerinden elde ettiği tecrübeleri de bize aktardığını düşünüyorum.					
9.	Bilgi güvenliği kapsamında alınan önlemlerin kullanıcı yetkilerini aşırı derecede kısıtladığını düşünüyorum.					
10.	Kurumumuzda yürütülen bilgi güvenliği yönetim sisteminin iyi bir şekilde yönetildiğini düşünüyorum.					

EK-2. Etik Komisyon Kararı

Evrak Tarih ve Sayısı: 22/06/2018-E.93206

T.C.
GAZİ ÜNİVERSİTESİ
Etik Komisyonu

Sayı : 77082166-302.08.01-
Konu : Bilimsel ve Eğitim Amaçlı

BİLİŞİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 14/03/2018 tarihli ve 73247369-302.08.01- 43676 sayılı yazı.

İlgi yazınız ile göndermiş olduğunuz, Bilişim Sistemleri Anabilim Dalı **Yüksek Lisans Öğrencisi Mehmet TUYGUN'un, Dr.Öğr. Üyesi Hüseyin ÇAKIR'ın** danışmanlığında yürüttüğü ***"ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardının Uygulanabilirliğinin Araştırılması"*** adlı tez çalışması ile ilgili konu Komisyonumuzun **08.05.2018** tarih ve **04** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi ve gereğini rica ederim.

e-imzalıdır
Prof. Dr. Alper CEYLAN
Komisyon Başkanı

Araştırma Kod No : 2018-279

Ek:1 Liste

Ankara
Tel:0 (312) 202 20 57 - 0 (312) 2... Faks:0 (312) 202 38 76
İnternet Adresi :http://etikkomisyon.gazi.edu.tr/
Bilgi için :Burak Çitrak
Genel Evrak Sorumlusu
Telefon No:0312 202 26 61

EK-2. (devam) Etik Komisyon Kararı

GAZİ ÜNİVERSİTESİ
ETİK KOMİSYONU KATILIM LİSTESİ

TOPLANTI TARİHİ : 08/05/2018	TOPLANTI SAYISI : 04
ADI-SOYADI	**İMZA**
Prof.Dr.Alper CEYLAN BAŞKAN	
Prof.Dr.Mustafa N.İLHAN BAŞKAN YRD.	KATILAMADI
Prof.Dr.Mehmet KÜÇÜKKURT	KATILAMADI
Prof.Dr.Aymelek GÖNENÇ	
Prof.Dr.Rahmi ÜNAL	
Prof.Dr.Mehmet Savım KARACAN	
Prof.Dr.Naciye YILDIZ	
Prof.Dr.Mustafa SARIKAYA	
Prof.Dr.İbrahim DOĞAN	
Prof.Dr.C. Haluk BODUR	
Prof.Dr.Mustafa İLBAŞ	
Prof.Dr.Füsun DEMİREL	
Doç.Dr.Nihan KAFA	

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: TUYGUN, Mehmet
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 10.12.1979, Akdağmadeni
Medeni hali	: Evli
Telefon	: 0 (312) 409 61 46
Faks	: 0 (312) 409 60 09
E-mail	: mehmettygn@gmail.com

Eğitim Derecesi	Okul Program	Mezuniyet yılı
Yüksek lisans	Gazi Üniversitesi / Bilişim Sistemleri	2019
Lisans	Anadolu Üniversitesi / İktisat	2012
Lisans	Gazi Üniversitesi / Matematik	2003
Lise	Hasanoğlan Anadolu Öğretmen Lisesi	1997

İş Deneyimi

Yıl	Çalıştığı Yer	Görev
2010-Halen	Türkiye Ulusal Ajansı	Bilişim Uzmanı
2008-2010	İçişleri Bakanlığı	Programcı
2003-2008	Sınav Dershaneleri	Matematik Öğretmeni

Yabancı Dil

İngilizce

Yayınlar

1. Tuygun, M. (2018). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Kamu Kurumlarına Uygulanabilirliğinin İncelenmesi, *5. Uluslararası Yönetim Bilişim Sistemleri Konferansı (IMISC 2018)*, 25 -27 Ankara.

Hobiler

Bilişim teknolojileri, Kahve, Sinema, Futbol

GAZİLİ OLMAK AYRICALIKTIR