PREMIUM E-JOURNAL OF SOCIAL SCIENCES

2687-5640

Yıl / Year	:	2022	Makale Geliş / Received	:	29.08.2022
Cilt / Volume	:	6	Yayınlama / Published	:	30.09.2022
Sayı / Issue	:	22	Article Type/Makale Türü	:	Araştırma Makalesi / Research Article
ss / pp	:	303-310			http://dx.doi.org/10.37242/pejoss.4254

Dr. Öğr. Üyesi Remzi BAŞAR
https://orcid.org/0000-0002-1114-825x
Düzce Üniversitesi, İşletme Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Düzce / TÜRKİYE

TÜRKİYE'DE ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ SERTİFİKASINA SAHİP ÇEŞİTLİ KURULUŞLARIN BGYS YAKLAŞIMLARI ÜZERİNE BİR İNCELEME

A REVIEW OF ISMS APPROACHES OF VARIOUS ORGANIZATIONS WITH ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM CERTIFICATE IN TURKEY

ÖZET

Bilgi, günümüzde bireyler ve özellikle kurumlar için en az diğer ekonomik varlıklar kadar kıymetli ve vazgeçilmez bir unsurdur. Teknoloji ve iletişimin gelişmesi hayata dair birçok kolaylık sağlarken birçok risk ve tehdidi de beraberinde getirmektedir. Ortaya çıkan bu risk ve tehditlerin bir sonucu olarak bilgi güvenliği kavramı ciddi önem kazanarak; işletme, devlet ve diğer tip örgütlerin sahip oldukları bilgiyi saklamak, korumak ve yönetmek amacıyla en uygun bilgi güvenliği çözümlerine yönelmeleri kaçınılmaz olmaktadır. Örgütler kendi stratejilerine, hedeflerine, ihtiyaçlarına ve süreçlerine en uygun olan ITIL, COBIT, ISO 27001 gibi standartlara ve yasal düzenlemelere uyumlanmaya çalışmaktadırlar.

Bu çalışma ile Türkiye'de ISO 27001 bilgi güvenliği yönetim sistemi sertifikasına sahip olan çeşitli kuruluşların ISO 27001 standardı ve bilgi güvenliği yönetim sistemi hakkındaki düşüncelerinin analiz edilmesi amaçlanmaktadır.

Bu araştırma kapsamında, sınırlandırılmış evren olarak; kolayda örnekleme metodu ile Türkiye'de büyükşehirlerde faaliyet gösteren, ISO 27001 bilgi güvenliği yönetim sistemi sertifikasına sahip 20 kuruluş seçilmiştir. Bu örgütlerde görevli 632 personel ile çalışma örneklemi oluşturulmuş ve anket yoluyla elde edilen veriler betimsel analiz yöntemi ile analiz edilmiştir. Analiz sonuçlarına göre, kurulan ve işletilen bilgi güvenliği yönetim sistemlerinin benimsendiği, sisteme karşı güven duyulduğu ve bilgi güvenliği yönetim sistemi süreçlerinin etkin bir şekilde yönetildiği yönünde genel kanaat olduğu anlaşılmaktadır.

Anahtar Kelimeler: Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi, Bilgi Güvenliği Standardı, ISO 27001, BGYS.

ABSTRACT

In today's world, information is a valuable and indispensable asset for individuals and especially institutions as much as other economic assets. While the development of technology and communication provides many conveniences in life, it also brings many risks and threats. As a result of these emerging risks and threats, the concept of information security has gained serious importance; it's inevitable for businesses, institutions and states to turn to the most appropriate information security solutions in order to store, protect and manage the information they have. Organizations are trying to comply with the standards and legal regulations such as ITIL, COBIT, and ISO 27001, which are most suitable for their strategies, goals, needs, and processes.

Within the scope of this research, as a bounded universe; with the convenience sampling method, 20 organizations operating in metropolitan cities in Turkey that have ISO 27001 information security management system certificates were selected, and a study sample was created with 632 personnel working in these organizations, and the data obtained through the questionnaire were analyzed with the descriptive analysis method. In this way, it's aimed to analyze the opinions about the ISO 27001 standard and ISMS applied in these organizations.

Keywords: Information Security, Information Security Management System, Information Security Standard, ISO 27001, ISMS.

1. GİRİŞ

Bilgi; Türk Dil Kurumu sözlüğüne göre "İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat" veya "İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf" şeklinde tanımlanmaktadır. Bilgi, günümüzde hem bireyler hem de kurumlar için o denli önemli bir hale gelmiştir ki içinde yaşadığımız çağ bile bilgi çağı olarak adlandırılmaktadır ve ekonomik olarak değer verilen en önemli varlıklar arasına bilgi de eklenmiştir. Bilginin değeri arttıkça, sağladığı avantaj ve güç de artmaktadır. Bu sebeple sadece devletler ve toplum için değil tüm kurumlar ve hatta bireyler içinde bilgi değerli ve önemlidir (Önder, 2018: 90).

Bilgi güvenliği, bilginin izinsiz olarak; kullanılması, ifşa edilmesi, değiştirilmesi, yok edilmesi veya zarar verilmesine karşı koruma ve bilgiye izinsiz erişimleri engelleme faaliyetlerinin genel adı olup gizlilik, bütünlük ve erişilebilirlik olmak üzere üç temel unsurdan meydana gelmektedir. Bu temel unsurlardan birinin bile zarar görmesi güvenlik açığı oluşturmaktadır (Şen ve Yerlikaya, 2013: 677).

Kurumsal bilgi güvenliği; kurumların sahip olduğu bilgi varlıkları ile bu varlıklara ait zayıflıkların tespit edilerek, çeşitli tehdit ve tehlikelerden korumak için gerekli güvenlik analizlerinin yapılması ve önlemlerin alınmasıdır. Kurumsal bilgi güvenliği; insan, eğitim, teknoloji gibi çeşitli faktörlerin aynı çatı altında yönetilmesini sağlayan karmaşık süreçlerden oluşmaktadır (Baykara, Daş ve Karadoğan, 2013: 3).

Bilgi Güvenliği Yönetim Sistemi (BGYS); bilginin gizliliği, bütünlüğü ve erişilebilirliğinin sürekli olarak sağlanması amacı ile sistemli, yönetilebilir, kurallara uygun, planlı ve dokümantasyonlu olarak uluslararası güvenlik standartlarını temel alan faaliyetler kümesidir (Ersoy, 2012: 8). BGYS sayesinde kurumlar; çalışanlar ve iş süreçleri ile bilgi teknolojilerini kapsayacak şekilde hassas bilgilerini koruyabilir ve yönetebilir.

Bilgi güvenliği standartları; kurum ve kuruluşların iş süreçlerini oluşabilecek risklere karşı korumak ve alınan tedbirlerin planlı bir şekilde uygulanabilmesi ile bu süreçlerini bu standartlara uygun hale getiren kurumların ilgili sertifika ile belgelendirilmesi amacıyla geliştirilmiştir (Şen ve Yerlikaya, 2013: 678). Bilgi güvenliği yönetim sistemi kurumlarda ancak üst yönetimin desteği ile ve belli bir bilgi güvenliği standardına bağlı olarak devreye alınabilir. Bilgi Güvenliği uygulamalarının kurumlarda belli bir plan dâhilinde yürütülebilmesi için dünya genelinde en yaygın standart olarak ISO 27001 öne çıkmaktadır. Orijinal adı "Information Technology-Security Technigues-Information Security Management Systems-Requirements" olan ISO 27001 bilgi güvenliği standardı; Türkçeye çevirisi "Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler" olarak Türk Standartları Enstitüsü (TSE) tarafından yapılan kurum içi ve dışı yanlış veya kötü amaçlı kullanıma karşı bilginin korunması için gerekli beklentileri tanımlayan bir standartlar kümesidir. Teknik bir standart olmayan ISO 27001 kurum ve kuruluşların güvenlik ihtiyaçlarını tanımlayarak nasıl uygulanacağını kurumlara bırakır. TSE'nin yayınladığı TS ISO/IEC 270001 isimli kitapçığa göre bu standart; Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak, uygulamak, izlemek ve iyileştirmek için bir model oluşturmak amacıyla geliştirilmiştir (Ersoy, 2012: 15; Yılmaz, 2014: 51).

2. ISO 27001 STANDARDI ve BGYS KAVRAMLARI

Literatür incelendiğinde ISO 27001 standardı ve BGYS sertifikası üzerine çeşitli çalışmalar olduğu görülmektedir. Bu çalışmalardan bazıları aşağıda özetlenmiştir.

Canbek ve Sağıroğlu tarafından 2006 yılında yapılan bir araştırmada; bilgi güvenliği ile ilgili riskleri sıfıra indirgemenin mümkün olmadığı ancak bilgi güvenliği farkındalığının sağlanması ve bilgi güvenliği standartlarına uygun şekilde oluşturulan güvenlik politikalarının etkin kullanımı sayesinde saldırılardan etkilenme olasılığının en aza indirgenebileceği paylaşılmıştır.

Doğantimur (2009), Marttin ve Pehlivan (2010), Evrin ve Demirer (2011) çalışmalarında ISO 27001 standardı ve bilgi güvenliği yönetim sistemi ile BGYS süreçleri hakkında çeşitli bilgiler vermişlerdir.

Demirtaş (2013), çalışmasında kamu ve özel sektör kuruluşlarınca yürütülen BGYS'lerin başarı faktörlerini değerlendirerek, sistemi olumlu ya da olumsuz yönde etkileyen unsurları incelemiştir.

Candiwan (2014), Endonezya'da gerçekleştirdiği araştırmasında uyguladığı anket sonuçlarına göre hem büyük işletmeler hem de KOBİ'lerin iş sürekliliği için bilgi güvenliğini dikkate aldığını ancak büyük işletmeler için uygulanan standartların KOBİ'ler için uygulananlardan sayıca fazla olduğunu belirtmektedir. Ayrıca büyük işletmeler ile KOBİ'lerin yönetimlerinin bilgi güvenliği politikasını

yüksek oranda dikkate aldığını ancak sistem edinme, geliştirme ile bakım ve tedarikçi ilişkilerinin olgunluk seviyesinin, işletmeler için hala düşük seviyede olduğunu paylaşmaktadır.

Gencer, 2015 yılında yürüttüğü çalışmada; ISO27001 süreçlerinin ve gerekliliklerinin kurumsal ve uluslararası saygınlık ve kabul görmek için ne denli önemli olduğu dile getirmiştir.

Alber ve Nabil tarafından 2015 yılında yapılan bir araştırmada, Mısır'daki 13 bankanın ISO 27001 BGYS sertifikasına sahip olması ile kârlılıkları arasındaki ilişki incelenmiştir. Çalışmada sadece BGYS ile sermaye kârlılığı (ROC) arasında istatistiksel olarak anlamlı ve pozitif yönlü bir ilişki bulunmuştur.

Uğuz (2018), çalışmasında ISO/IEC 27001 bilgi güvenliği standardını temel alarak BGYS sistemi uygulamak isteyen kurum ve işletmeler için küçük bir rehber niteliğinde açık kaynak kodlu bir BGYS yazılımı geliştirmiş bu yolla BGYS siteminin aşamaları ve bir BGYS yazılımının içeriği hakkında fikir vermeyi amaçlamıştır.

Yılmaz (2018), Konya'da ISO 27001 BGYS sertifikasına sahip kurumların sertifika alma safhasında karşılaştıkları sorunlar ve bunlara dair sunulan çözüm yollarını içeren yüksek lisans tez çalışması ile çeşitli kurumlarda, incelemeler gerçekleştirilmiştir. Yapılan incelemelerde BGYS'nin uygulanması için yürütülen tüm faaliyetlerin ilgili kurumlarda emek ve zaman kaybı olarak görüldüğü ve BGYS'ne geçiş ile sağlanacak faydaların kısa sürede değil uzun vadede kuruma yansıyacağı noktasındaki farkındalığın yok mertebesinde olduğu tespit edilerek sürece dair öneriler sunulmuştur.

Çakır ve Tuygun (2019), Ankara'daki 6 kamu kurumunda uygulanan ISO 27001 BGYS'ni etkinlik seviyesi, sahiplenme durumu ve teknik yeterlilik olarak incelemiş ve genel olarak ISO27001'in kurum çalışanları tarafından benimsendiği sonucuna ulaşmışlardır.

3. ARAŞTIRMANIN YÖNTEMİ

Bilgi güvenliği yönetim sistemine ve ISO 27001 sertifikasına sahip kuruluşların bu süreci ne kadar sahiplendikleri, sertifika sahibi olmanın bilgi güvenliğinin sağlanmasında işe yarayıp yaramadığı, bilgi güvenliği farkındalık seviyelerindeki gelişme gibi konuların belirlenmesi amacıyla betimsel analiz odaklı bir çalışma yürütülmüştür.

3.1. Araştırmanın Sorunsalı

Bu araştırmanın problemi olarak; kurum ve kuruluşların üst yönetimi ve çalışanlarının ISO 27001 standardı ve bilgi güvenliği yönetim sistemlerini olumlu veya olumsuz anlamda nasıl gördükleri anlamaya çalışılmaktadır. Çalışmada cevap aranan iki temel soru:

1- ISO 27001 standardı ve BGYS; kurumların üst yönetimi ile BGYS ekip üyeleri ve BT çalışanlarına göre gerekli midir, bilgi güvenliğine katkı sağlamakta mıdır?

2- 2- ISO 27001 standardı ve BGYS; üst yönetim, BGYS ekip üyeleri ve BT çalışanları tarafından ne ölçüde benimsenip sahiplenilmektedir?

Elde edilen sonuçların bilgi güvenliği yönetim sistemlerinin kurulması ve ilgili uygulamaların yürütülmesi aşamalarında yol gösterici olabileceği öngörülmektedir.

3.2. Araştırmanın Amacı

Çalışma için seçilen Türkiye'deki ISO 27001 bilgi güvenliği sertifikasına sahip olan çeşitli kamu ve özel sektör kuruluşlarında standardın gerekliliklerinin uygulanabilirliği ve çalışanlar tarafından benimsenme seviyesinin araştırılması amaçlanmıştır. Bu amaç kapsamında belirlenmiş alt amaçlar ise şunlardır:

1. ISO 27001 sertifikasyon sürecini tamamlamış ve hali hazırda bilgi güvenliği yönetim sistemi kullanan kuruluşlardaki üst yönetim kadrosundaki kişilerin görüşleri nelerdir?

2. Bilgi güvenliği yönetim sistemi kurulumu ve uygulanmasından sorumlu olan Bilgi Güvenliği Yönetim Sistemi ekip üyelerinin kanaatleri ne yöndedir?

3. ISO 27001 sertifikasına sahip kuruluşlarda görevli, bilgi güvenliği yönetim sistemi ekip üyeliği dışında diğer bilgi güvenliğinden dolaylı olarak sorumlu olan bilgi teknolojileri birim çalışanlarının görüşleri nelerdir?

3.3. Veri Toplama Yöntemleri

Bu araştırmada veri toplama yöntemi olarak anket yöntemi kullanılmış olup, anket soru ve cevapları ile araştırmanın problemlerine çözüm üretilmeye çalışılmıştır.

Araştırmanın evreni Türkiye'deki ISO 27001 sertifikası sahibi kamu ve özel sektör kuruluşlarından oluşmaktadır. Evrenin büyük olması ve ISO 27001 sahibi kuruluşların genelde anket uygulanmasına izin vermemesi sebebiyle bu çalışmada kolayda örnekleme metodu ile anket yapılmasına izin veren kurumlardan örneklem alma yoluna gidilmiştir. Kuruluşlar ile görüşülerek alınan izinler sonucunda İstanbul başta olmak üzere büyükşehirlerde faaliyet gösteren 20 kuruluşa anket uygulanabilmiştir. Bu sebeple araştırmanın örneklemini Türkiye'deki büyükşehirlerde faaliyet gösteren 20 kuruluş ve bu kuruluşlarda görevli 632 kişi oluşturmaktadır.

Araştırma üç farklı personel grubu; üst yönetim ile bilgi güvenliği yönetim sistemi ekipleri ve bilgi teknolojileri çalışanlarına uygulanmak üzere hazırlanan üç farklı anketten oluşmaktadır. 5'li Likert ölçeği kullanılan anketlerde ölçek dereceleri; "Kesinlikle Katılmıyorum", "Katılmıyorum", "Kararsızım", "Katılıyorum", "Kesinlikle Katılıyorum" şeklindedir. Anket soruları özenle hazırlanmış ve Likert tipi ölçek sorularında Cronbach Alpha (α) güvenilirlik katsayısı diğer adıyla içsel tutarlılık katsayısı hesaplanmıştır. Oluşturulan anketler ve uygulanan güvenilirlik analizine ait veriler aşağıdaki gibidir:

Üst yönetim için hazırlanmış olan anket 10 adet sorudan oluşmaktadır. Anket soruları ile üst yönetimin sistemin sahipliği ve işletilmesi konusundaki bakış açılarının incelenmesi amaçlanmıştır. Yapılan analizler sonucunda üst yönetim anketinin güvenilirlik katsayısı 0,705 olarak hesaplanmıştır.

Bilgi güvenliği yönetim sistemi ekip üyelerine yönelik olarak yapılan anket dâhilinde kuruluşlarda ISO 27001 standardının uygulanması, sürdürülmesi ve kontrol edilmesinden sorumlu olan ve yönetimce atanan ekip üyelerinin yeterlilikleri ve karşılaştıkları problemler incelenmiştir. Bilgi güvenliği yönetim sistemi ekip üyeleri için hazırlanmış olan ankette 14 adet soru bulunmaktadır ve bu sorulara verilen cevaplara yönelik yapılan analiz sonucunda bilgi güvenliği yönetim sistemi ekip üyeleri anketinin güvenilirlik katsayısı 0,703 olarak hesaplanmıştır.

Tablo 1: Anketlerin Kuruluşlara Göre Dağılımı

Kuruluş	Üst Yönetim	BGYS Ekibi	BT Çalışanı	Toplam
Kuruluş-1	3	5	23	31
Kuruluş-2	4	4	22	30
Kuruluş-3	2	3	20	25
Kuruluş-4	4	5	26	35
Kuruluş-5	1	2	10	13
Kuruluş-6	3	5	30	38
Kuruluş-7	2	3	29	34
Kuruluş-8	5	5	20	30
Kuruluş-9	2	4	25	31
Kuruluş-10	3	4	36	43
Kuruluş-11	2	3	30	35
Kuruluş-12	4	7	32	43
Kuruluş-13	5	10	40	55
Kuruluş-14	4	4	23	31
Kuruluş-15	3	4	24	31
Kuruluş-16	1	1	10	12
Kuruluş-17	4	8	42	54
Kuruluş-18	2	2	16	20
Kuruluş-19	4	4	24	32
Kuruluş-20	1	1	7	9
Toplam	59	84	489	632

Kuruluşlarda görevli bilgi teknolojileri personelleri için hazırlanan ankette çalışanların bilgi güvenliği yönetim sistemi ve ISO 27001 gerekliliklerini uygulama konusundaki yetenekleri ve yeterlilikleri incelenmiştir. Hazırlanan anket 10 sorudan oluşmaktadır. Yapılan analizler sonucunda bilgi teknolojileri ekip üyeleri anketinin güvenilirlik katsayısı 0,875 olarak hesaplanmıştır.

Hazırlanan anket soruları 20 farklı kuruluşa uygulanmıştır. Değerlendirmeye alınan 632 adet anketin; 59'unu üst yönetim, 84'ünü bilgi güvenliği yönetim sistemi ve 489'unu bilgi teknolojileri çalışanları tarafından cevaplanan anketler oluşturmaktadır. Anketlerin kuruluşlara göre dağılımı Tablo 1'de paylaşılmıştır. Kuruluş isimleri güvenlik nedeniyle ve kuruluşlardan alınan izinler kapsamında gizli tutulmuştur. Çalışma kapsamında elde edilen veriler analiz edilmiş ve sonuçlar tablolar halinde sunularak yorumlanmıştır.

3.4. Araştırmanın Analizi

Çalışmada çeşitli sektörlerden işletmeler ve kurumların olduğu yirmi farklı kuruluşun Üst Yönetim, Bilgi Güvenliği Yönetim Sistemi ve Bilgi Teknolojileri çalışanlarına üç ayrı anket uygulanmış, 5'li Likert ölçeği kullanılan sorular yöneltilmiştir. Anket sorularının güvenilirlik düzeyi için Cronbach Alpha (α) analizi yapılarak üç farklı çalışan grubuna yönelik soruların da güvenilir olduğu tespit edilmiş ve anket sonucu elde edilen veriler betimsel analiz yöntemi ile analiz edilmiştir.

4. ARAŞTIRMADA ELDE EDİLEN BULGULAR

Bu bölümde, uygulanan anket verilerine ait bulgular ve ilgili yorumlar yer almaktadır. Anket verileri üç ana başlık altında incelenmiştir.

4.1. Üst Yönetimin BGYS ve ISO 27001 Hakkındaki Görüşleri

Bu bölümde ankete katılan ve ISO 27001 sertifikasına sahip kuruluşlarda görev alan üst yönetim seviyesindeki yöneticiler tarafından cevaplanan anketlerden elde edilen veriler incelenmiştir. Yirmi farklı kuruluşta görevli toplam 59 yönetici, 10 sorudan oluşan ankete katılmış ve bu yöneticilerin ankete vermiş olduğu cevapların oransal dağılımı Tablo 2'de paylaşılmıştır.

Tablo 2: Üst Yönetimin Görüşleri

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1	ISO27001 Standardının kuruluşlar için gerekli olduğunu düşünüyorum	0%	0%	0%	29%	71%
2	ISO27001 Standardının kuruluşa saygınlık kazandırdığını düşünüyorum	0%	0%	0%	24%	76%
3	ISO27001 Standardının kuruluşa ekonomik imtiyazlar kazandırdığını düşünüyorum	0%	5%	12%	29%	54%
4	ISO27001 Standardının kuruluşun güvenliğine katkı sağladığını düşünüyorum	0%	0%	0%	14%	86%
5	ISO27001 Standardının kurumsal saygınlığı koruduğunu düşünüyorum.	0%	0%	0%	25%	75%
6	ISO27001 Standardının rekabet avantajı sağladığını düşünüyorum	0%	3%	14%	5%	78%
7	ISO27001 sertifikasyonu sağlanmadan bilgi güvenliği yönetim sisteminin verimli olacağını düşünüyorum.	29%	71%	0%	0%	0%
8	Bilgi Güvenliği Yönetim Sisteminin devamlı olmasında yönetim desteğinin önemli olduğunu düşünüyorum.	0%	0%	14%	0%	86%
9	ISO27001 Standardının riskleri minimize ettiğini düşünüyorum.	0%	0%	0%	29%	71%
10	ISO27001 Standardının iş sürekliliği sağladığını düşünüyorum.	0%	0%	8%	29%	63%

4.2. BGYS Ekip Üyelerinin BGYS ve ISO 27001 Hakkındaki Görüşleri

Bu bölümde ISO 27001 sahibi kuruluşlarda görev alan 84 bilgi güvenliği yönetim sistemi ekip personelinin katılım gösterdiği 14 sorudan oluşan ankete ait veriler incelenmiş ve BGYS ekip üyelerinin ankete vermiş olduğu cevaplar yüzdesel oran olarak Tablo 3'te paylaşılmıştır.

Tablo 3: Bilgi Güvenliği Yönetim Sistemi Ekibinin Görüşleri

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1	ISO27001 Standardının doğru, güvenilir ve geçerli bilgiler sağladığını düşünüyorum	0%	0%	0%	27%	73%
2	ISO27001 Standardının fazladan iş yükü ve gereksiz zaman kaybının önüne geçtiğini düşünüyorum	0%	0%	0%	8%	92%
3	ISO27001 Standardının kuruluş genelinde, bilgi sistemleri ve zayıflıkların nasıl korunacağı konusundaki farkındalığı arttırdığını düşünüyorum	0%	0%	0%	27%	73%
4	ISO27001 Standardının bilgi varlıklannın gizliliğinin korunmasını sağladığını düşünüyorum	0%	0%	0%	23%	77%
5	ISO27001 Standardının bilginin ve metotlarının doğruluğunun ve bütünlüğünün korunması, içeriğinin değişmemesini sağladığını düşünüyorum	0%	0%	0%	42%	58%
6	ISO27001 Standardının yasal tarafların zorunlu kıldığı kriterler sağladığını düşünüyorum	0%	0%	0%	8%	92%
7	ISO27001 Standardının bilgi varlıklarına erişimi koruduğunu düşünüyorum	0%	0%	0%	13%	87%
8	Bilgi Güvenliği Yönetim Sistemi için kurulacak olan ekibin bilgi teknolojileri personellerinden meydana gelmesi gerektiğini düşünüyorum	0%	0%	0%	23%	77%
9	ISO27001 standardının kuruluş içerisinde doğru bir şekilde uygulandığını düşünüyorum	0%	0%	0%	23%	77%
10	Kuruluşumuz içerisindeki BGYS personel sayısının yeterli olduğunu düşünüyorum	38%	48%	14%	0%	0%
11	BGYS yönetimi ve ISO27001 çalışmaları için danışmanlık hizmeti alınması gerektiğini düşünüyorum	13%	39%	29%	5%	14%
12	BGYS yönetimi ve ISO27001 çalışmaları için BGYS personelinin eğitim alması gerektiğini düşünüyorum	0%	0%	0%	13%	87%
13	BGYS yönetimi ve ISO27001 kapsamında alınan önlemlerin iç ve dış tehditlere karşı kuruluşumuzu koruyacağını düşünüyorum	0%	0%	0%	27%	73%
14	BGYS yönetimi ve ISO27001 kapsamında personelin yetkinliklerinin yeterli olduğunu düşünüyorum	0%	0%	0%	27%	73%

4.3. BT Ekip Üyelerinin BGYS ve ISO 27001 Hakkındaki Görüşleri

Bu bölümde ISO 27001 sertifikasına sahip 20 kuruluşta görevli toplam 489 bilgi teknolojileri personeline uygulanan 10 adet sorudan oluşan anket verileri incelenerek, BT ekip üyelerinin ankete vermiş olduğu cevapların yüzdesel oranları Tablo 4'te paylaşılmıştır.

Tablo 4: Bilgi Teknolojileri Birim Çalışanlarının Görüşleri

		Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1	BGYS yönetimi ve ISO27001 kapsamında bilgi teknolojileri personelinin yetkinliklerinin yeterli olduğunu düşünüyorum	0%	0%	0%	28%	72%
2	BGYS yönetimi ve ISO27001 çalışmaları için bilgi teknolojileri personelinin eğitim alması gerektiğini düşünüyorum	0%	0%	0%	25%	75%
3	BGYS yönetimi ve ISO27001 önlemleri ile Bilgi Güvenliği problemlerinde düşüşler yaşandığını düşünüyorum	0%	0%	0%	28%	72%
4	BGYS yönetimi ve ISO27001 sayesinde finansal kayıpların önüne geçildiğini düşünüyorum	0%	0%	0%	0%	100%
5	BGYS yönetimi ve ISO27001 sayesinde operasyonel kayıpların önüne geçildiğini düşünüyorum	0%	0%	0%	28%	72%
6	BGYS yönetimi ve ISO27001 sayesinde itibar kaybının önüne geçildiğini düşünüyorum	0%	0%	4%	4%	92%
7	BGYS yönetimi ve ISO27001 sayesinde hackerların tuzağına düştüğümde ne yapmam gerektiğini biliyorum	0%	0%	7%	0%	93%
8	BGYS yönetimi ve ISO27001 sayesinde olası Bilgi Güvenliği açığı olduğunu düşündüğüm durumlarda nasıl bir yol izlemem gerektiğini biliyorum	0%	0%	0%	28%	72%
9	BGYS yönetimi ve ISO27001 sayesinde ihlal durumlarının kontrol altında olduğunu düşünüyorum	0%	0%	0%	28%	72%
10	BGYS yönetimi ve ISO27001 sayesinde olası risklerin olay öncesinde tespit edilebildiğini düşünüyorum	0%	0%	0%	28%	72%

5. SONUÇ ve ÖNERİLER

Kuruluşlarda bilgi güvenliği yönetim sistemlerinin kurulmuş olması veya ISO 27001 standardına sahip olunması, kurum süreçlerinde bilgi güvenliğinin %100 sağlandığı anlamını taşımamaktadır.

Uygulanan bilgi güvenliği sistemlerinin ve uyumlanan standartların kullanılabilir ve sürdürülebilir olması kuruluşlar için çok önemlidir. Bunun gerçekleştirilebilmesi için kararlı bir üst yönetim desteği şarttır. Ayrıca bilgi güvenliği yönetim sistemi ile standartların BGYS ekip üyeleri ve BT çalışanları tarafından sahiplenilmesi çok önemlidir. Çünkü BGYS'yi uygulayacak ve devamlılığını sağlayacak kişiler başta bilgi güvenliği yönetim sistemi ekip üyeleri olmak üzere bilgi teknolojileri çalışanlarıdır.

Genel olarak üst yönetim kademesinde uygulanan anketin sonuçları incelendiğinde, olumlu görüşlerin hâkim olduğu, ISO 27001 standardının kuruluşlar için önemli ve gerekli olduğu, saygınlık, itibar ve güven gibi kurumun vazgeçilmez unsurlarına katkı sağladığı görülmektedir. ISO 27001 standardının kuruluşlar için rekabet avantajı sağladığına ve kuruluşlara imtiyazlar kazandırdığına dair görüşler ise yüksek orandadır. Genel anlamda üst yönetim kademesinin ISO 27001 standardını kuruluşları için olumlu buldukları ve kuruluşun bilgi güvenliğine katkı sağladığını düşündükleri görülmektedir.

Bilgi güvenliği yönetim sistemi ekip üyelerine uygulanan anketin sonuçları incelendiğinde, genel olarak ekip üyelerinin ISO 27001 standardının bilgi güvenliğinin sağlanması için gerekli olduğunu düşündükleri görülmektedir. Bunun yanı sıra, kuruluşları iç ve dış güvenlik tehditlerine karşı korumakta etkin olduğu görüşünün yüksek oranda kabul gördüğü anlaşılmaktadır. Anket sonuçlarında dikkat çeken diğer bir husus; ekip üyelerinin profesyonel danışmanlık desteğine çekimser kalmış olmasıdır. Anket uygulanan firmaların alanında uzman personeller ile çalışan ülkenin önde gelen kuruluşları olması bu sonucun ortaya çıkmasında etkili olduğu düşünülmekte ve danışmanlık yerine personele eğitim aldırılması konusunda yüksek bir görüş birliği olduğu görülmektedir. Eğitimlerin ilgili personeli güncel tuttuğu ve yeniliklere adapte olmak açısından avantaj sağladığı bilinen bir gerçektir.

Kurulacak olan bilgi güvenliği yönetim sistemi ekibinin bilgi teknolojileri personellerinden oluşması konusunda ise olumlu fikir bildirildiği görülmektedir. Bilgi güvenliği yönetim sistemi ekip üyeleri tarafından bakıldığında, ISO 27001 standardının fazladan iş yükü ve gereksiz zaman kaybının önüne geçtiği şeklindeki görüş bildirimi oldukça fazladır. Genel anlamda, bilgi güvenliği yönetim sistemi ekip üyelerinin kendilerini bu iş için yeterli gördükleri, iş yüklerinin azaldığını ifade ettikleri ve kuruluş için ISO 27001'in gerekli olduğu yönünde görüş bildirdikleri anlaşılmaktadır.

Bilgi teknolojileri ekip üyelerine uygulanan anketin sonuçları incelendiğinde; BT ekip üyelerindeki bilgi güvenliği farkındalığının ISO 27001 standardının uygulanması sayesinde yüksek olduğu görüşü öne çıkmaktadır. Yetkinlik ve yeterliliklerinin yüksek olduğu görüşüne sahip oldukları ve bilgi güvenliği açıklarının herhangi bir olay yaşanmadan evvel tespit edilebildiğine dikkat çekecek düzeyde görüş bildirimi yaptıkları görülmektedir. Ayrıca verilerden ISO 27001 BGYS'nin devreye alınması ile bilgi güvenliği problemlerinde düşüşler yaşandığına dair olumlu yanıt verildiği bilgisi elde edilmektedir.

Sonuç olarak, bu araştırma kapsamında kuruluşlarda yapılan incelemeler ve elde edilen verilerden; kurulan ve işletilen sisteme karşı güven duyulduğu, benimsendiği ve bilgi güvenliği yönetim sistemi süreçlerinin etkin bir şekilde yönetildiği yönünde ortak görüş birliği olduğu anlaşılmaktadır.

Bütün uygulamalarda olduğu gibi iş süreçlerinin bilgi güvenliği standartlarına uyumlu hale getirilmesi ve bilgi güvenliği yönetim sistemlerinin uygulamaya alınmasında da yürütülen uygulamaların kurum çalışanları tarafından benimsenmesi ve sahiplenilmesi bir zorunluluk olarak düşünülmelidir. Personelin aidiyet duygusu içinde olmadığı uygulama ve süreçlerin kurumlar içinde verimsiz olacağı ve uzun süre varlığını koruyamayacağı unutulmamalıdır. Bu nedenlerle kurum personelini aşırı sınırlayan, görevleri yerine getirmeyi zorlaştıran bilgi güvenliği uygulamalarından kaçınılmalıdır.

KAYNAKÇA

Alber, N. ve Nabil, M. (2015). The Impact Of Information Security On Banks' Performance In Egypt. *International Journal of Economics and Finance*, *7*(9), 219-225.

Baykara, M., Daş, R. ve Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, 231-239.

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

Candiwan, C. (2014). Analysis Of ISO27001 Implementation For Enterprises and SMEs in Indonesia. *In Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014)* Malaysia, 50-58.

Çakır, H. ve Tuygun, M. (2019). ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. *Uluslararası Yönetim Bilişim Sistemleri Ve Bilgisayar Bilimleri Dergisi*, *3*(2), 59-78.

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

Doğantimur, F. (2009). *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği*. Mesleki Yeterlilik Tezi, Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara.

Ersoy, E. V. (2012). ISO/IEC 27001 Bilgi Güvenliği Standardı. *Ankara: ODTÜ Geliştirme Vakfı Yayını*.

Evrin, V. ve Demirer, M. (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği. *IV. Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu*, Atılım Üniversitesi, Ankara, 25-33.

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

Marttin, V. ve Pehlivan İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı Ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, *1*(1), 49-56.

Önder, Ş. (2018). ISO 27001 Standardı Kapsamında Kurumsal Bilgi Güvenliği ve İşletme Performansı Arasındaki İlişki: Bist 100 Endeksinde Yer Alan İşletmeler Üzerine Bir Uygulama. *Ekonomik ve Sosyal Araştırmalar Dergisi*, *14*(1), 89-98.

Şen, Ş. ve Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. *XV. Akademik Bilişim Konferansı Bildirileri*, 677-681.

Uğuz, S. (2018). Kurumsal Bilgi Güvenliği Yönetim Sistemi Yazılımları: Örnek Bir Yazılım Geliştirilmesi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, *2*(1), 1-11.

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

Yılmaz, M. (2018). *İşletmelerde Bilgi Güvenliği Uygulama Sorunları ve Çözüm Önerileri; Konya Örneği.* KTO Karatay Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Konya.