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

***

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

Hüseyin ÇAKIR[*]
Mehmet TUYGUN[**]

DOI: 10.33461/uybisbbd.598989

Öz

Bu araştırmada, ISO27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) 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.

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.

Anahtar Kelimeler: *e-devlet, Bilgi Güvenliği, ISO27001.*

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 (ISMS) certification process. For this reason, in the scope of the research, different questionnaires were

[*] Dr. Öğr. Üyesi, Gazi Üniversitesi, Gazi Eğitim Fakültesi Bil. ve Öğr. Tek. Eğitimi Bölümü, hcakir@gazi.edu.tr
ORCID: 0000-0001-9424-2323
[**] Gazi Üniversitesi, Bilişim Enstitüsü, Bilişim Sistemleri Anabilim Dalı, mehmettygn@gmail.com
ORCID: 0000-0000-0000-0000

Geliş Tarihi / Received: 31.07.2019
Kabul Tarihi / Accepted: 24.11.2019

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.

Establishing a corporate ISMS, ensuring the continuity of the established system, continuously monitoring and identifying the deficiencies, making improvements, creating information security awareness, in short, establishing a live ISMS is an indispensable condition of having ISO27001 certificate. This study is thought to be important in terms of shedding light on the efficiency levels, ownership and technical competence of ISMS established by public institutions.

Keywords: *e-government, Informatıon Security, ISO27001.*

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 (Colwill, 2009). Bunun sebebi, kurumsal sistemlerde uygulanan birçok teknik veya teknik olmayan güvenlik önlemleri saldırganlar tarafından insanlar kullanılarak çeşitli yöntemlerle aşılabilmektedir (Arce, 2003).

Bilgi güvenliğinin sağlanabilmesi amacıyla, kurumların kendi ihtiyaçları ve süreçleri doğrultusunda bir dizi güvenlik politikalarını ve prosedürlerini belirlemesi ve uygulanması gerekmektedir (Asosheh, Hajinazari, & Khodkari, 2013). Bu politikalar, kurumsal faaliyetlerin gözden geçirilmesi, sistemlere erişimlerin izlenmesi, değişiklik kayıtlarının tutularak gerekli değerlendirmelerin yapılması, silme yetkisinin kısıtlanması gibi bazı kullanıcı işlemlerine indirgenebilmektedir (Canbek & Sağıroğlu, 2006).

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 (Asosheh et al., 2013).

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 (Gikas, 2010).

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 (Rhodes-Ousley, 2013).

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 (UDHB, 2017).

1.1. Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliğinin sağlanabilmesi için öncelikle bilgi kavramı ve bu bilginin güvenliğinin sağlanabilmesi ile doğrudan ilişkili olan temel unsurları göz önünde bulundurmak gerekmektedir.

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 olabilir. Bu noktada bilginin güvenilirliği, konu ile ne kadar ilgili olduğu, eksiksiz olması, erişim kolaylığı, ihtiyaçları karşılaması gibi ölçütler o bilgisinin kalitesini belirlemektedir (Demirtaş, 2013).

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 (Rhodes-Ousley, 2013). Bilgi güvenliği, kurumsal bilgi güvenliği risklerini tanımlamak ve bu risklerin etkilerinin kabul edilebilir seviyelere indirgenebilmesi amacıyla yürütülen süreçlerdir (Asosheh et al., 2013).

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.

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.

BGYS; 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 BGYS, kuruluşların güvenlik olaylarını bütüncül ve sistematik bir biçimde yönetmelerini sağlayan bir çerçevedir.

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 (Achmadi, Suryanto, & Ramli, 2018).

1.1.1. ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı

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 (ISO, 2019).

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.

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 (ISO, 2017).

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 (UHDB, 2016). 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 (UDHB, 2017). 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.

ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardı üzerine yapılmış çalışmalar şunlardır;

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.

King (2017) tarafından yayınlanan doktora tezinde kurumsal bilgi güvenliği yönetişimi ile bilgi güvenliği yönetim standartları arasında doğrusal bir ilişki olup olmadığının araştırılması amaçlanmıştır.

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.

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.

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.

Gürcan (2014) tarafından yapılan çalışmada, finans kurumlarının bilgi güvenliği ihtiyaçlarının ISO27001 çatısı altında incelenerek belirlenmesi üzerinde durulmuştur.

Ganbat (2013) tarafından, ISO27001 ve ISO27005 standartlarının uygulanması konulu çalışmasında ISO27001'in nasıl uygulanması gerektiği ve ISO27005 Risk Yönetimi standardı ile ilişkisi üzerinde durulmuştur.

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.

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.

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.

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.

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.

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.

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 (UDHB, 2017) 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.

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 BGYS'nin kamu kurumlarına uygulanabilirliğinin araştırılması amaçlanmıştır. Bu amaç kapsamında belirlenmiş olan alt amaçlar ise şunlardır.

ISO27001 BGYS 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?

2. YÖNTEM

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

2.1. 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.

2.2. 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. Resmi yollardan alınan izinler neticesinde Ankara ili genelinde 6 kamu kurumuna anket uygulanabilmiştir. Bu sebeple araştırmanın örneklemini Ankara'da bulunan 6 kamu kurumu ve bu kurumlarda görevli 539 kişi oluşturmaktadır.

2.3. Veri Toplama Araçları

Araştırmada Türkiye'de bulunan ISO27001 sertifika sahibi kurumların hâlihazırda çalışan dört farklı personel grubuna (Üst Yönetim, BGYS Ekibi, Teknik Ekip ve Personel) uygulanmak üzere hazırlanmış dört ayrı anketten oluşmaktadır. Anketlerde 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. 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.

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.

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.

2.4. Verilerin Toplanması

Hazırlanan anketler, hem ankete özel hazırlanmış web sitesi hem de alınan çıktılara altı adet kamu kurumuna uygulanmıştır. Toplam 573 adet anket cevaplanmış, cevaplanan bu anketlerden 34 tanesinin eksik cevaplanmış olması sebebiyle değerlendirmeye alınmamıştır.

Tablo 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**

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 Tablo 1'de verilmiştir. Kurum isimleri güvenlik nedeniyle ve kurumlardan alınan izinler doğrultusunda gizli tutulmuştur.

2.5. 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.

Bu kapsamda, ISO/IEC sertifikasyon sürecinin tamamlamış ve aktif BGYS'ye sahip olan kamu kurumlarında görevli yönetim kademesi, kurumsal BGYS'nin yönetiminden sorumlu olan BGYS ekip üyelerinin, kurumda görevli diğer teknik personelin ve teknik olmayan personel görüşlerinin belirlenmesi amacı için frekans ve yüzde dağılımları kullanılmıştır.

3. ARAŞTIRMA BULGULARI

Bu bölümde, yapılan araştırma 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.

3.1. 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 incelenmiştir. 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.

Tablo 2: Yönetim Kademesinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Görüşleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	N	$\overline{X}$
ISO27001 Standardının kurumlar için gerekliliği olduğunu düşünüyorum	3	3,8	4	5,1	1	1,3	23	29,5	47	60,3	78	4,37
ISO27001 Sertifika sahibi olmanın kazandırdığı ulusal ve uluslararası saygınlık kazandırdığını düşünüyorum	2	2,6	4	5,1	8	10,3	27	34,6	37	47,4	78	4,19
ISO27001 Bilgi Güvenliği alanındaki kurumsal hedeflerime de sağladığı kolaylık sağladığını düşünüyorum	6	7,7	1	1,3	4	5,1	32	41,0	35	44,9	78	4,14
ISO27001 Bilgi Güvenliği politikalarının kurumsal süreçlerin uygulanması konusunda kolaylık sağladığını düşünüyorum	1	1,3	7	9,0	3	3,8	31	39,7	36	46,2	78	4,21
ISO27001'in kurum yöneticilerinin Bilgi Güvenliği farkındalığına katkı sağladığını düşünüyorum	1	1,3	6	7,7	3	3,8	25	32,1	43	55,1	78	4,32
Bilgi Güvenliği Yönetim Sisteminin sürdürülebilir olmasına yönetim desteğinin katkısının önemli olduğunu düşünüyorum	3	3,8	3	3,8	4	5,1	11	14,1	57	73,1	78	4,49
ISO27001 Bilgi Güvenliği Yönetim Sisteminde yer alan, yönetimin üzerine düşen görevlerin uygulanabilir olduğunu düşünüyorum	4	5,1	3	3,8	9	11,5	36	46,2	26	33,3	78	3,99
ISO27001 standartlarının uygulanmasının kurumsal süreçlerin uygulanması sırasında ek iş yükü getirdiğini düşünüyorum	10	12,8	20	25,6	22	28,2	12	15,4	14	17,9	78	3,00
ISO27001 Bilgi Güvenliği ve Yönetim Sistemi üst yönetim olarak bu sistem içerisindeki ayrıcalıklı olmam gerektiğini düşünüyorum	13	16,7	16	20,5	15	19,2	20	25,6	14	17,9	78	3,08
ISO27001 in kurum dışı ve kurum içi güvenliğe katkı sağladığını düşünüyorum	1	1,3	6	7,7	9	11,5	47	60,3	15	19,2	78	3,88
ISO27001 kapsamında genelde veya yerelde gerçekleşecek kritik bir güvenlik probleminde sistemin bizi koruyacağını düşünüyorum.	1	1,3	8	10,3	9	11,5	49	62,8	11	14,1	78	3,78
ISO27001 sertifikasyonu sağlanmadan bilgi güvenliği yönetim sisteminin verimli olarak yönetilemeyeceğini düşünüyorum.	4	5,1	12	15,4	14	17,9	32	41,0	16	20,5	78	3,56

Tablo 2'den de anlaşılacağı üzere Kurum yöneticileri, ISO/IEC 27001 standardının kurumları için gerekli olduğu yönündeki ağırlıklı görüş bildirmektedir. Bununla birlikte kurum yönetiminin tamamına yakınının ISO/IEC 27001 sertifika sahibi olmanın kuruma saygınlık kazandırdığı ve kurumsal süreçlerin işletilmesine olumlu yönde katkı sağladığı noktasında görüş birliğinde oldukları görülmektedir. Kurum yönetim kademesinin ISO/IEC 27001 standardının bilgi güvenliği farkındalığına olumlu yönde katkı sağladığı ve standardın sürdürülebilir olması için üst yönetim desteğinin gerekliği olduğu görüşünün hâkim olduğu da verilen cevaplardan anlaşılmaktadır. Diğer taraftan ISO/IEC 27001 standardının kurumsal süreçlerin uygulanması esnasında ek iş yükü getirdiği noktasında bir görüş birliği olmadığı görülüyor. Ortalamanın 3.00 olarak görüldüğü bu soruda; katılımcıların %33,3'ünün standardın ek iş yükü getirdiği, %28,2'sinin bu konuda karasız

olduğu ve geri kalan %38,5'lik kısmının da ek iş yükü getirmediği yönünde görüş bildirdikleri görülmektedir. Aynı zamanda yönetim kademesinin sistem içerisinde ayrıcalıklı olup olmamaları yönünde sorulan soruya verilen cevaplarda da bu konuda bir görüş birliği sağlanamadığını görülmüştür. Yönetim kadrosunun %43,5'lik bir bölümünün ayrıcalıklı olmaları gerektiği yönünde görüş bildirdikleri, %19,2'lik bölümünün bu konuda kararsız oldukları, geri kalan %37,3'lük bölümün ise ayrıcalık tanınmaması gerektiği yönünde görüş bildirdikleri görülmektedir. Kurum yönetiminin %76,9 gibi yüksek bir bölümünün kurum tarafından yönetilen bilgi güvenliği yönetim sisteminin ISO/IEC27001 sertifikasyonu olmadan verimliği bir şekilde yönetilemeyeceği yönünde görüş bildirdikleri görülmektedir.

3.2. 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 incelenmiştir. Altı 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.

Tablo 3 incelendiğinde ekip üyelerinin BGYS süreçlerinin yönetimi ve ISO27001 süreçlerinin etkin bir şekilde yönetilebilmesi için kurulmuş olan ekibin, eğitim ihtiyacı olduğu, sayısal anlamda yeteriz kaldığı ve bu sebeple danışmanlık hizmetlerinin gerekli olduğu yönünde görüş bildirdikleri görülmektedir. Ekip üyelerinin %84,1'inin eğitime ihtiyaç duydukları yönünde görüş bildirdikleri görülmüştür. Süreçlerin yönetilmesi noktasında personel yeterli olup olmadığı konusunda %43,2'lik bir çoğunluğun kararsız kaldığı görülmektedir. Diğer taraftan kurum personeli ile uyumlu bir çalışma yürütülüp yürütülmediği konusunda %43,2'sinin olumlu görüş bildirdiği %34,1'lik bölümünün ise kararsız kaldığı görülmektedir. Diğer taraftan kurum personeli ile yürütülen risk çalışmalarında ise uyumlu bir çalışma yapılıp yapılamadığı yönünde %43,2'lik bölümünün olumsuz görüş bildirdiği görülmüştür. BGYS kapsamında yapılan çalışmaların ve kurumsal BGYS süreçlerinin sağlıklı bir şekilde uygulanıp uygulanamadığı yönündeki soruya ilişkin cevaplar incelendiğinde, katılımcıların %29,6'sinin olumsuz görüş bildirdiği, %38,6'lık bölümünün bu konuda kararsız kaldığı ve geri kalan %31,8'lik bölümünün ise kurumsal BGYS süreçlerinin sağlıklı bir şekilde işletilebildiği yönünde görüş bildirdikleri görülmektedir. Diğer taraftan kurum personelinin %65,9'luk bölümünün ise BGYS kapsamında alınan önlemler kapsamından yapılan değişiklikler ile birlikte alışkanlıklarını değiştirme konusunda zorlandıkları yönünde görüş bildirdikleri görülmüştür. Son olarak, ISO27001 sertifikasyon süreci tamamlanmış ve etkin bir şekilde BGYS süreçlerini kapsamında uygulanan politika ve prosedürlerin kurumsal süreçlere sağladığı katkılara ilişkin sorulan soruya katılımcıların toplam %27,3'lük bölümünün olumsuz görüş bildirdiği, %36,4'lük bölümünün kararsız kaldığı ve %36,9'unun olumlu yönde görüş bildirdikleri görülmüştür.

Tablo 3: BGYS Ekip Üyelerinin Bilgi Güvenliği Yönetim Sistemi Hakkındaki Düşünceleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	N	$\overline{X}$
Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilmesi amacıyla mutlaka danışmanlık hizmeti alınması gerektiğini düşünüyorum.	3	6,8	5	11,4	6	13,6	15	34,1	15	34,1	44	3,77
Bilgi Güvenliği Yönetim Sistemi süreçlerinin yönetilebilmesi için kurumumuz personelinin yeterli olduğunu düşünüyorum.	4	9,1	8	18,2	19	43,2	11	25,0	2	4,5	44	2,98
Bilgi Güvenliği yönetim Sistemi süreçlerinin yönetilmesi için ekip üyelerinin eğitim alması gerektiğini düşünüyorum.	3	6,8	2	4,5	2	4,5	9	20,5	28	63,6	44	4,30
Kurulacak olan ekibin bilişim personellerinden oluşması gerektiğini düşünüyorum.	3	6,8	11	25,0	11	25,0	13	29,5	6	13,6	44	3,18
Kurumumuz Bilgi Güvenliği yönetimi ekip üyelerinin sayısının ISO27001 süreçlerinin sağlıklı bir şekilde yönetilebilmesi için yeterli olduğunu düşünüyorum.	5	11,4	12	27,3	12	27,3	12	27,3	3	6,8	44	2,91
ISO/IEC 27001 süreçlerinin yönetimi esnasında kurum personeli ile sağlıklı bir çalışma yürütülebileceğini düşünüyorum.	2	4,5	8	18,2	15	34,1	15	34,1	4	9,1	44	3,25
Kurumsal risk çalışmaları sırasında kurum personelinden yeterince destek alınabileceğini düşünüyorum.	4	9,1	15	34,1	10	22,7	14	31,8	1	2,3	44	2,84
ISO/IEC 27001 süreçlerinin kurumumuzda sağlıklı bir şekilde uygulanabildiğini düşünüyorum.	5	11,4	8	18,2	17	38,6	10	22,7	4	9,1	44	3,00
ISO/IEC 27001 standardının kurumsal bilgi güvenliği açısından gerekli olduğunu düşünüyorum.	4	9,1	3	6,8	5	11,4	18	40,9	14	31,8	44	3,80
ISO27001 kurum dışı olduğu kadar kurum içi güvenliği de tam olarak sağladığını düşünüyorum	4	9,1	6	13,6	16	36,4	13	29,5	5	11,4	44	3,20
ISO27001 kapsamında alınan önlemlerin, kurum içinden veya dışından gelecek kritik bilgi güvenliği problemlerine karşı bizi koruyacağına inanıyorum.	3	6,8	8	18,2	9	20,5	21	47,7	3	6,8	44	3,30
ISO27001 sistemine geçiş sürecinde insanların alışkanlıklarını terk etmelerinin zor olduğunu düşünüyorum.	3	6,8	6	13,6	6	13,6	14	31,8	15	34,1	44	3,73
ISO/IEC 27001 sistemine geçişin ardından bilişim personeli üzerindeki iş yükünün azaldığını düşünüyorum.	15	34,1	13	29,5	8	18,2	5	11,4	3	6,8	44	2,27
ISO/IEC 27001 çerçevesinde belirlenen politika ve prosedürlerin tıkanan kurumsal süreçlerini açtığını düşünüyorum.	3	6,8	9	20,5	16	36,4	11	25,0	5	11,4	44	3,14

3.3. 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 incelenmiştir. Altı 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.

Tablo 4: Teknik Personelin Bilgi Güvenliği Yönetim Sistemi ve Yeterlilikler Hakkındaki Görüşleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	N	$\overline{X}$
Bilgi Güvenliği Yönetim Sistemi süreçlerinin sağlıklı bir şekilde yürütülmesi için teknik personelin yeterli olduğunu düşünüyorum.	8	8,9%	28	31,1%	8	8,9%	34	37,8%	12	13,3%	90	3,16
ISO/IEC 27001 standardının kurumsal bilişim süreçlerinde uygulanabilir olduğunu düşünüyorum.	2	2,2%	7	7,8%	18	20,0%	51	56,7%	12	13,3%	90	3,71
ISO/IEC 27001 ile ilgili eğitim/eğitimler almamız gerektiğini düşünüyorum.	4	4,4%	5	5,6%	5	5,6%	42	46,7%	34	37,8%	90	4,08
ISO/IEC 27001 görevimle ilgili süreçleri etkin ve zamanında yerine getirebilmemde fayda sağladığını düşünüyorum.	3	3,3%	9	10,0%	23	25,6%	42	46,7%	13	14,4%	90	3,59
ISO/IEC 27001 kapsamında alınan önlemler sayesinde Bilgi Güvenliği olaylarında azalma yaşandığını düşünüyorum.	3	3,3%	5	5,6%	15	16,7%	49	54,4%	18	20,0%	90	3,82
ISO/IEC 27001 Standardının, geliştirilen kurumsal uygulamaların güvenliğine olumlu katkı sağladığını düşünüyorum.	2	2,2%	5	5,6%	11	12,2%	53	58,9%	19	21,1%	90	3,91
ISO/IEC 27001 sayesinde, bilgi güvenliği ihlal olaylarının kontrol edilebilir noktaya geldiğini düşünüyorum.	2	2,2%	5	5,6%	20	22,2%	52	57,8%	11	12,2%	90	3,72
Bilişim sistemlerinde tespit edilen aksaklıklar üzerinde düzenleyici ve önleyici faaliyetler uygulanmasının faydalı olduğunu düşünüyorum.	2	2,2%	6	6,7%	2	2,2%	52	57,8%	28	31,1%	90	4,09
ISO/IEC 27001 kapsamında güvenlik açısından daha fazla önlem alınmış bir sistem üzerinde daha az problem yaşanacağını düşünüyorum.	1	1,1%	8	8,9%	13	14,4%	43	47,8%	25	27,8%	90	3,92
ISO/IEC 27001 standardının bütün süreçlerinin en iyi şekilde işletilmesi durumunda olası risklerin önceden tespit edilebileceğini düşünüyorum.	3	3,3%	4	4,4%	12	13,3%	50	55,6%	21	23,3%	90	3,91

Tablo 4 incelendiğinde kurum teknik ekiplerinin ISO27001 hakkındaki görüşlerinin genel anlamda olumlu yönde olduğu görülebilir. Diğer taraftan teknik personelin sayısal anlamda yeterli olup olmadığı sorusuna %40 oranında olumsuz cevap verildiği, %51,1 oranında ise olumlu cevap verildiği görülmüştür. ISO27001'in kurumsal süreçlere uyumluluğu konusunda %70'lik bir oranda olumlu görüşün hakim olduğu görülmüştür. Diğer taraftan teknik personelin %80'inden fazlasının eğitim ihtiyacı olduğu konusunda fikir birliğine vardığı görülmüştür. ISO27001'in süreçlerinin bilgi güvenliği olaylarının azalmasına katkı sağladığı yönünde olumlu görüş bildirenlerin oranı ise %74,4 olarak gözlemlenmiştir. ISO27001 ile birlikte kurumlar bünyesinde geliştirilen yazılımların bilgi güvenliği açısından incelenmesi konusunda bir farkındalık oluştuğu yönündeki görüşlerin oranı ise %80'dir. Aynı zamanda bilgi güvenliği olaylarının gerçekleşmeden önce tahmin edilebilmesi ve düzenleyici ve önleyici faaliyetlerin olumlu yönde katkı sağladığı görüşünün ağır bastığı görülmüştür. Teknik personelin ISO27001 kapsamında alınan önlemlerin daha fazla olması durumunda yaşanması muhtemel bilgi güvenliği olaylarında azalma yaşanacağı şeklinde görüş bildirdikleri görülmüştür.

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

Bu bölümde ISO27001 sahibi kamu kurumlarında görevli personelden elde edilen veriler incelenmiştir. 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. Altı kamu kurumunda görevli toplam 329 personel yapılan ankete katılım sağlamıştır. Katılımcıların anket sorularına vermiş oldukları cevaplar aşağıda soru bazlı olarak incelenmiştir.

Personele sorulan sorular ile personelin bilgi güvenliği yönetim sistemi çalışmaları kapsamında almış oldukları farkındalık eğitimleri ve sistem ile ilgili genel görüşleri hakkında bilgi sahibi olunmaya çalışılmıştır. Verilen cevaplar incelendiğinde, %65,3'lük bir oranın verilen eğitimlerin sürelerinin yeterli olduğunu düşündüğü görülmüştür. Diğer taraftan eğitimde kullanılan materyallerin ve eğitim içeriğinin yeterliliği konusunda yaklaşık %60'lık bir oranda olumlu görüş bildirildiği görülmüştür. Bununla birlikte alınan eğitimlerin bilgi güvenliği farkındalığı açısından faydalı olduğunu düşünenlerin oranı ise %73,3 seviyesinde. Eğitim içeriklerinden memnun olunmasına rağmen, eğitimlerin sadece slaytlar üzerinden yapılmasının yeterli olmadığını düşünenlerin oranı %44,4 olarak görülmektedir. BGYS kapsamında alınan önlemler ve kısıtlamaların kullanıcı yetkilerini kısıtlayıp kısıtlamadığı konusunda ise personel içerisinde bir görüş birliği olmadığı görülmektedir. Personelin %42,5'lik bir bölümünün yetkilerin kısıtlanmadığı yönünde, %27,4'ünün bu konuda kararsız olduğu ve geri kalan %30,1'lik kesiminin ise yetkilerin aşırı derecede kısıtlandığı yönünde görüş bildirdikleri görülmektedir.

4. SONUÇ VE ÖNERİLER

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.

Tablo 5: Kurum Personelinin BGYS ve Farkındalık Eğitimleri Hakkındaki Görüşleri

	Kesinlikle Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Kesinlikle Katılıyorum		N	Ort
	f	%	f	%	f	%	f	%	f	%		
ISO/IEC 27001 hakkında verilen bilgilendirme eğitimlerini süresinin yeterli olduğunu düşünüyorum.	13	4,0	40	12,2	61	18,5	181	55,0	34	10,3	329	3,56
ISO/IEC 27001 hakkında verilen bilgilendirme eğitimlerinin içeriklerinin yeterli olduğunu düşünüyorum.	8	2,4	43	13,1	78	23,7	162	49,2	38	11,6	329	3,54
ISO/IEC 27001 hakkında verilen Bilgi Güvenliği bilgilendirme eğitimleri esnasında verilen materyal ve örneklerin yeterli ve güncel olduğunu düşünüyorum.	12	3,6	30	9,1	99	30,1	159	48,3	29	8,8	329	3,50
Almış olduğum Bilgi Güvenliği Eğitimlerinin faydalı olduğunu düşünüyorum.	10	3,0	25	7,6	54	16,4	168	51,1	72	21,9	329	3,81
Bilgi Güvenliği Eğitimleri kapsamında verilen bilgilerin kurumsal süreçler açısından uygulanabilir olduğunu düşünüyorum.	4	1,2	27	8,2	80	24,3	170	51,7	48	14,6	329	3,70
Danışmanlık kapsamında verilen Bilgi Güvenliği Eğitimlerinin süresinden ziyade içeriklerinin dolu olması gerektiğini düşünüyorum.	10	3,0	11	3,3	44	13,4	143	43,5	121	36,8	329	4,08
Bilgi Güvenliği Eğitimlerinin sadece slaytlar üzerinden yapılmasının yeterli olduğunu düşünüyorum.	38	11,6	108	32,8	89	27,1	79	24,0	15	4,6	329	2,77
Bilgi Güvenliği Eğitimi veren firmanın diğer müşterilerinden elde ettiği tecrübeleri de bize aktardığını düşünüyorum.	15	4,6	37	11,2	102	31,0	148	45,0	27	8,2	329	3,41
Bilgi Güvenliği kapsamında alınan önlemlerin kullanıcı yetkilerini aşırı derecede kısıtladığını düşünüyorum.	31	9,4	109	33,1	90	27,4	82	24,9	17	5,2	329	2,83
Kurumumuzda yürütülen bilgi güvenliği yönetim sisteminin iyi bir şekilde yönetildiğini düşünüyorum.	8	2,4	19	5,8	89	27,1	159	48,3	54	16,4	329	3,71

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 çalışma kapsamında, 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.

4.1. 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.

KAYNAKÇA

Achmadi, D., Suryanto, Y., & Ramli, K. (2018, 12-13 May 2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. Paper presented at the 2018 International Workshop on Big Data and Information Security (IWBIS), Jakarta, Indonesia.

Akay, İ. G. (2014). Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları. Bilecik Şey Edebali Üniversitesi, Bilecik.

Arce, I. (2003). The weakest link revisited [information security]. IEEE Security & Privacy, 1(2), 72-76. doi:10.1109/msecp.2003.1193216

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. Paper presented at the 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, Kish Island, Iran. https://ieeexplore.ieee.org/ielx7/6552353/6556712/06556730.pdf?tp=&arnumber=6556730&isnumber=6556712

Aydoğmuş, E. (2010). Türkiye'deki organizasyonların bilgi güvenliği olgunluk seviyelerinin belirlenmesi ve ISO/IEC 27001:2005 standardına uyumluluklarının değerlendirilmesi. İstanbul.

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

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. doi:10.1016/j.istr.2010.04.004

Çek, E. (2017). Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi. İstanbul Bilgi Üniversitesi, İstanbul.

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

Ganbat, O. (2013). Bilgi güvenliği yönetim sistemi ISO/IEC 27001 ve bilgi güvenliği risk yönetimi ISO/IEC 27005 standartlarının uygulanması. (Yüksek Lisans Tezi), İzmir.

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

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. doi:10.1080/19393551003657019

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

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

Haklı, T. (2012). Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi. (Yüksek Lisans Tezi), Isparta.

ISO. (2017). Uluslararası Standart Organizasyonu 2017 İstatistik Raporu. Retrieved from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO. (2019). Uluslararası Standart Organizayonu Web Sayfası. Retrieved from https://www.iso.org/

King, K. E. (2017). Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management. (10256918 Ph.D.), Capella University, Minneapolis, USA. Retrieved from https://search.proquest.com/docview/1877918458?accountid=11054

http://JJ2EC6WC6Q.search.serialssolutions.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&rft.genre=dissertations+%26+theses&rft.jtitle=&rft.atitle=&rft.au=King%2C+Kenneth+E.&rft.aulast=King&rft.aufirst=Kenneth&rft.date=2017-01-01&rft.volume=&rft.issue=&rft.spage=&rft.isbn=9781369575507&rft.btitle=&rft.title=Examine+the+relationship+between+information+technology+governance%2C+control+objectives+for+information+and+related+technologies%2C+ISO+27001%2F27002%2C+and+risk+management&rft.issn=&rft_id=info:doi/ ProQuest Dissertations & Theses Global database.

Mete, H. (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin bilgi işlem merkezlerinde uygulanması. Sakarya.

Rhodes-Ousley, M. (Ed.) (2013). Information Security, Complete Reference. San Francisco: McGraw-Hill Education.

Shoraka, B. (2011). An Empirical Investigation of the Economic Value of Information Security Management System Standards. (3456209 Ph.D.), Nova Southeastern University, Florida, USA. Retrieved from https://search.proquest.com/docview/871586434?accountid=11054

http://JJ2EC6WC6Q.search.serialssolutions.com?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&rft.genre=dissertations+%26+theses&rft.jtitle=&rft.atitle=&rft.au=Shoraka%2C+Babak&rft.aulast=Shoraka&rft.aufirst=Babak&rft.date=2011-01-01&rft.volume=&rft.issue=&rft.spage=&rft.isbn=9781124655314&rft.btitle=&rft.title=An+Empirical+Investigation+of+the+Economic+Value+of+Information+Security+Management+System+Standards&rft.issn=&rft_id=info:doi/ ProQuest Dissertations & Theses Global database.

UDHB. (2017). KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ. Retrieved from http://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm

UHDB. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Retrieved from http://www.edevlet.gov.tr/wp-content/uploads/2016/07/2016-2019-Ulusal-e-Devlet-Stratejisi-ve-Eylem-Plani.pdf