T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ YÖNETİMİNİN GEREKLERİ VE BAŞARI DAYANAKLARI: BİR UYGULAMA ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Hasan DEMİRTAŞ

Enstitü Anabilim Dalı : İşletme
Enstitü Bilim Dalı : Yönetim ve Organizasyon

Tez Danışmanı: Prof. Dr. Mehmet BARCA

HAZİRAN – 2013

T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ YÖNETİMİNİN GEREKLERİ VE BAŞARI DAYANAKLARI: BİR UYGULAMA ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Hasan DEMİRTAŞ

Enstitü Anabilim Dalı : İşletme
Enstitü Bilim Dalı : Yönetim Organizasyon

"Bu tez 26 /06 /2013 tarihinde aşağıdaki jüri tarafından Oybirliği / Oyçokluğu ile kabul edilmiştir."

JÜRİ ÜYESİ	KANAATİ	İMZA
Prof. Dr. Mehmet Bozca	Başarılı	
Doç. Dr. Suayyip Garip	Başarılı	
Yrd. Doç. Dr. Mahmut Hüseyin Gülü	Başarılı	

BEYAN

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan ederim.

Hasan DEMİRTAŞ

26.06.2013

ÖNSÖZ

Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Organizasyon Bilim Dalında, Bilgi Güvenliği Yönetimin Gerekleri ve Başarı Dayanakları: (TS ISO/ IEC 27001) Bir Uygulama Örneği olarak isimlendirdiğim, bu sistemi uygulayan ve uygulamayı düşünen kuruluşlara katkı sağlayacağını umut ettiğim çalışmamda engin tecrübesi ile bana yol gösteren, destek olan ve yardımlarını esirgemeyen tez danışmanım değerli hocam Prof. Dr. Mehmet BARCA'ya sonsuz teşekkür ederim.

Çalışmam ile ilgili dokümanların temininde her türlü yardımı gördüğüm ve burada çalışmaktan gurur duyduğum TSE teşkilatı ve çalışma arkadaşlarıma teşekkür ederim.

Çalışmanın ortaya çıkmasında bana destek veren Prof. Dr. Ali GÜL'e, Dr. Hatice BEKTAŞ'a, Dr. Cemal YILDIZELİ'ne, Mehmet Ali DÖNMEZ'e, Aslı ERZURUMDAĞ'a ve Erdem KEKLİK'e teşekkür ederim.
Çalışma süresince bana destek olan eşim ve oğluma teşekkür ederim.

Tahsil hayatım ve tahsil hayatım sonrası hiçbir fedakarlıktan kaçınmayarak bana her türlü maddi ve manevi desteği sağlayan aileme minnet ve şükranlarımı sunarım.

Hasan DEMİRTAŞ
26.06.2013

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

Tezin Başlığı: Bilgi Güvenliği Yönetiminin Gerekleri ve Başarı Dayanakları: Bir Uygulama Örneği

Tezin Yazarı: Hasan DEMİRTAŞ **Danışman:** Prof. Dr. Mehmet BARCA

Kabul Tarihi: 26.06.2013 **Sayfa Sayısı:** viii (ön kısım) +75 (tez)+ 8(ek)

Anabilimdalı: İşletme **Bilimdalı:** Yönetim ve Organizasyon

Dünyada ve ülkemizde devlet kurumları ve özel sektör kuruluşları yaptıkları işlerin sürdürebilirliğini sağlamak için yoğun bir şekilde bilgi kullanımına yönelmişlerdir. Zaman geçtikçe bilginin değeri artmış, sadece depolanması değil güvenli bir şekilde saklanması, istendiğinde ulaşılması ve bu olgunun sürdürülebilir olması önemli hale gelmiştir. En küçük bir bilgi sızıntısı, bilgi kayıpları, bilinçli ya da bilinçsiz yapılan hataların sonuçları kuruluşlarca telafisi zor olmaktadır. Kendine özgü kullanılan hiç bir yöntem, bilginin, bilgi sistemlerinin, hizmetlerinin, ürün bilgilerinin, kuruluşlara özel bilgilerin ya da bilgisayar ağlarının tamamen korunmasını garanti edememektedir. Bu yöntemler uygulansa bile bilgi güvenliğini tam olarak sağlanamayabilir. Böylece, kuruluşların olası iş faaliyet alanlarında bilinçli yada bilinçsiz güvenlik ihlali olayları meydana gelebilir. Bu nedenle kuruluşlar elde ettikleri bilgi birikimini korumak için tüm dünyada kabul görmüş, uluslararası bir standard olan TS ISO/IEC 27001, Bilgi Güvenliği Yönetim Sistemini (BGYS'ni) kullanabilirler.

Bu çalışma, kamu ve özel sektör kuruluşlarında uygulanan bilgi güvenliği sisteminin başarı dayanakları değerlendirilerek, bilgi güvenliği yönetiminin performansını aşağı veya yukarı çeken faktörleri ortaya çıkarmak hedeflenmiş ve TS ISO/IEC 27001, Bilgi Güvenliği Yönetim Sistemini kurmak, uygulamak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model önerisinde bulunulmuştur. İki ana bölüm olarak tasarlanan çalışmanın Birinci bölümü "Bilgi, Bilgi yönetimi, Bilgi güvenliği, Bilgi güvenliği standartları ve Bilgi Güvenliği Yönetim Sistemi TS ISO/IEC 27001'in kuruluşlarda uygulama nedenleri, Bilgi güvenliği Standart maddeleri açıklanması ve Bilgi güvenliği yönetim sisteminin Kuruluşlara faydaları" başlıkları üzerine kurgulanmıştır. İkinci bölümde "Bilgi Güvenliği Yönetim Sistemi TS ISO/IEC 27001'in Başarı dayanakları oluşturulan anket ile sorgulanmıştır. Anket bulguları sonucunda Bilgi Güvenliği Yönetim Sistemi TS ISO/IEC 27001'in Kritik Başarı dayanakları irdelenmiştir. Sonuç ve Öneriler kısmında ise kuruluşların kendilerine özgü oluşturdukları yöntemlerin sürdürülebilir olmadığı, bilgi güvenliğinin bir sistem dahilinde yürütülmesi gerekliliği ve buna uygun yöntemin TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'ni uygulamaları olduğu vurgulanmıştır. Ayrıca kurulan bilgi güvenliği yönetim sisteminden uluslararası bir belge almanın kuruluşun marka ve imaj değerini attıracağına değinilmiştir.

Anahtar Kelimeler: Bilgi, Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001, BGYS uygulaması

Title of the Thesis: Information Security Management Requirements and Success Bases: A Case Study

Author: Hasan DEMİRTAŞ **Supervisor:** Professor. Dr. Mehmet BARCA

Date: 26.06.201 **Nu. of pages:** viii (pre text) +75 (main body)+8(annexes)

Department: Business Administration **Subfield:** Organisational Management

Governmental authorities and private sector organizations in the World and our country head towards using information intensely to achieve sustainability in their work. As time goes value of information has increased, not only storing but also storing safely, reaching when it has been needed and being sustainable have become important. Even a minimum information leakage, information lost, results of conscious or unconscious faults become unrecoverable for organisations. Any method of its own that is used can not guarantee the full protection of information, information systems, service and product information, and information special for the organization and computer network. Applying this methods also can not achieve information security fully. Thus, conscious or unconscious security infringement events in organisation's operation area can result in. For this reason, the organisations can apply for the Information Security Management System (ISMS) standard, TS ISO/IEC 27001, which is acknowledged all over the World to protect their knowledge that they have. This study aimed to obtain factors that bring down or up the performance of information security management with evaluating success bases of information security system which applied by governmental authorities and private sector organizations. The study is design as two parts, in the First Part has following headings; "Information, Information Management, Information Security, Information Security Standards, Reasons for Applying Information Security Management System- TS ISO/IEC 27001 in the organizations, Explanation of Information Security Management System Standard's Requirements and Benefits of Information Security Management System to the organizations". In the Second Part, success bases of Information Security Management System, TS ISO/IEC 27001 has been examined by a survey. As a result of the survey findings, critical success bases of Information Security Management System, TS ISO/IEC 27001 are explicated. In the Results and Suggestions Part, it is emphasized that methods of its own that is established by organisation are not sustainable, information security is needed to maintain systematic and suitable method for this is Information Security Management System, TS ISO/IEC 27001. In addition, it is mentioned having an international cerificate for Information Security Management System increases the brand mark and image value.

Keywords: Information, Information Security, Information Security Management System, TS ISO/IEC 27001, Implementation of ISMS.

GİRİŞ

Yaşamakta olduğumuz zamana damgasını vuran bilgi, dünyanın oluşumundan itibaren sürekli büyüyerek önem kazanmış, tarım toplumundan bilgi toplumuna geçişle birlikte üretime ve işletmelerin gelişmesine etki eden en önemli olgu olmuştur. Günümüzde bilgi, ekonomik yaşamın en önemli gerçeği haline gelmiştir. Bilginin bu denli önemli olması bilginin yönetilmesini doğurmuştur. Bununla beraber bilgi yönetiminin alanı genişlemekte, karmaşık ve sürekli değişime uğramaktadır. Bilgi yönetimi, yönetim, kuruluş uygulamaları, yönetim felsefesi, teknolojiler, stratejiler, insan davranışları olarak birçok alanı kapsamaktadır. Bilgi yönetiminin asıl amacı, kuruluşun hedeflerini gerçekleştirmesine yardımcı olmaktır. Bilgi yönetiminin başarısı için, kurum kültürü ve uzun dönemli stratejik planlar büyük önem taşımaktadır. Yeni ekonomide, entelektüel sermaye işletmenin önemli varlıklarından birisidir. Bilgiye dayalı ekonomide entelektüel sermaye, bir kuruluşun en önemli rekabet argümanı olmuştur.

Yeni ekonomide kuruluşların katma değer yaratması tüm çalışanlar, müşteriler, tedarikçiler, hissedarlar ile ilişkiler ve bu ilişkilerden sağladığı bilgi birikimine bağlıdır. Günümüz rekabetçi ortamında, fazla bilgi ve beceri biriktiren ya da bu bilgileri muhafaza etmeyi başaran kuruluşlar marka ve pazar değerlerini artırmaktadırlar. Kuruluşların rekabet etme yeteneğini sürdürebilir hale getirmek için ihtiyaç duydukları şey yeni ürün yaratabilen temel yetenekleridir. Bu temel yeteneklerin özünü de bilgi ve bilgi yönetimi oluşturmaktadır.

1990'ların başından itibaren belirginleşen yeni ekonomi dönemi, bilgi yönetimi yöneticilerin ilgisini çekmeye başlamış ve son zamanda bilgi ve iletişim teknolojilerinin kuruluşlarda iletişim ve işbirliğini son derece kolaylaştırıcı etkisi ile de bilgi ve bilgi yönetimi olağanüstü önem kazanmıştır.

İnternet teknolojileri ile beraber hızla değişen iş dünyası ve ekonomi birçok değişik olgu ve uygulamaların olmasına neden olmuştur. Yöneticiler hem bilgilerinin değerini, hem de bu bilgilerden en yüksek katma değer sağlamak için bilgiyi nasıl yönetmeleri gerektiğinin önemli olduğunun farkına varmışlardır. Bilginin kaybolmaması, boşa harcanmaması, doğru kullanılması ve katma değer yaratması için bilgi yönetimi olgusu ortaya çıkmıştır.

Bilgi yönetimi, kuruluşlarda rekabet üstünlüğü yaratmakta ve pazar değerini artırmaktadır. Dış çevrede oluşan fırsatları rakiplerden daha önce görebilmek ve ilk olmak, daha sonra elde edilen bu fırsatı uzun dönem sürdürebilmek için bilgi yönetimi etkileyici değil belirleyici bir rol oynayacaktır.

Kuruluşların başarmak istediği, rekabet üstünlüğü elde etmek ve uzun dönemde bunu sürdürebilmektir. Rekabet üstünlüğünün temel dayanaklarının ne olduğunu ortaya çıkarmak stratejik yönetim düşünce ve araştırmalarının temel sorununu oluşturur. Bir kuruluşun rekabet üstünlüğü elde etmesi ve bu rekabeti sürdürebilmesi o kuruluşun bilgilerinin kolayca taklit edilememesi ve bu bilgilerin işletme dışına çıkarılmasını engelleyen bir sisteme sahip olacak şekilde bir strateji yaratmalıdır.

Bilginin üretim ve gelişmede en önemli kaynak olması ve rekabet avantajı sağlaması nedeniyle bu olgunun korunması büyük önem taşımaktadır. Kuruluşlar stratejik bilgilerininin (üretim ve hizmet bilgileri, müşteri bilgileri, çalışan bilgileri ve işletmeye dışına çıkartılması istenmeyen bilgiler) güvenli bir ortamda saklanması, elektronik ortamda ve arşivlerde saklanan bilgilerin saldırılara ve işletme dışına habersiz bir şekilde çıkmasını engellemeye yönelik olarak çaba göstermek zorundadırlar. Devletlerin, kuruluşların ve bireylerin bilgilerinin korunması ile ilgili hukuki düzenlemeler bulunmakta olup bu hukuki düzenlemelere bağlı kalmak şartıyla kuruluşlar kendi bilgi güvenliği sistemlerini kurabilirler.

Kuruluşlar kendilerine özgü her türlü bilgilerini korumak için uluslararası bir standart olan ISO 27001 Bilgi Güvenliği Yönetim Standardı uygulayabilirler. Uygulayacakları bu sistem sayesinde rekabet etme becerilerini daha da arttırabilir ve pazar da kalıcılığı sağlayabilirler. Bu nedenle bilgi güvenliği yönetim sistemlerinin günümüz gelişmelerine paralel olarak düzenli bir şekilde araştırılması uygulama ve yönetim problemlerinin tespit edilerek çözüm önerilerinin ortaya çıkarılması gerekmektedir.

Bilgi güvenliği yönetim sistemi ile ilgili araştırıcılar tarafından yapılmış çeşitli çalışmalar bulunmaktadır. Bu araştırmalardan bazıları aşağıda verilmiştir.

Vural (2007), bilgi güvenliğini genel olarak incelemiş, kurumsal bilgi güvenliği ve standartlarını değerlendirmiş, bilgi güvenliğini zaafa uğratan tehditleri belirlemeye

çalışmıştır. Çalışmada ülkemiz bilişim hukuku incelenmiş ve ağırlıklı olarak yüksek tehdit altında olan web uygulamaları üzerinde durulmuştur.

Erkan (2006), bilgi güvenliği yönetim sistemi süreçlerinin otomasyonunu incelemiş, ISO/IEC 27001:2005 ve ISO/IEC 17799:2005 standartlarına uygun olarak dokümante edilmiş bir bilgi güvenliği yönetim sistemi için gerekli faaliyetlerin mümkün olduğunca otomatikleştirilmesi hususunda önerilerde bulunmuştur.

Kandemirli (2012), ABC A.Ş.'de yaptığı çalışmada bilgi teknolojileri güvenlik yönetimi konusunda dünyada en yaygın uygulama alanı bulan ISO 27001, CobIT ve ITIL Güvenlik Yönetimi süreçlerini incelemiştir.

Yıldız (2007), Ülkemizde uygulaması yeni başlayan E-Devlet kapsamında kurumların bilgi teknolojileri konusundaki durumlarını irdelemiş, ISO/IEC 17799:2005 ve ISO/IEC 27001:2005 standartlarının kurumlarda bilgi güvenliği yönetim sistemini hangi aşamalarda ve alt başlıklar altında oluşturulduğunu belirterek bu doğrultuda önerilerde bulunmuştur.

Aydoğmuş (2010), kurumların bilgi güvenliği olgunluk düzeylerini ve ISO/IEC 27001:2005 standardı ile uyumluluklarını değerlendirmiştir.

Mete (2010), BGYS Standardını kurmak ve yönetmek isteyen bilgi işlem merkezi yöneticilerine kuruluşlarında bilgi güvenliği kültürünü oluşturmak, ISO/IEC 27001uygulanması için Türkçe bir rehber hazırlanması üzerine bir çalıma yürütmüştür.

Çetinkaya (2008), kurumların bilgi güvenliğini hangi başarılılıkta uyguladıklarını saptamak ve ISO/IEC 27001:2007 bilgi güvenliği yönetim sistemi prensiplerinin kullanıldığı web tabanlı bir test aracı geliştirmek üzerine çalışmıştır.

Kahraman (2006) tarafından yapılan çalışmada, işletmelerin TS ISO/IEC 17799 ve TS ISO/IEC 27001 standartlarında bilgi güvenlik yönetim sistemi kurmak için gereken bilgi risklerini belirleme yöntemleri vurgulanmakta ve bu risklerin giderilmesi için ihtiyaç duyulan temel safhalara ait teknoloji, politika ve prosedürler açıklanmaktadır.

Bingöl (2010), bilgi güvenliği yönetim sistemi faaliyetini tamamen açık kaynak kodlu yazılımlar halinde düzenleyerek sürecin yönetiminin çok düşük maliyetle

sağlanabileceğini, bilgi güvenliği yönetim sistemi kurmak ve yönetmek isteyen bir işletmenin sürecin yönetimi esnasında ne tür bir sisteme ihtiyaç duyulabileceği hususunda çalışmasını yürütmüştür.

Bu çalışmada ise; ülkemiz kamu ve özel sektör kuruluşlarının bilgi güvenliği yönetiminin gerekleri ve başarı dayanakları incelenmiş olup, çalışma bilgi güvenliğinin başarılı olması için hangi şartların oluşması gerektiği üzerine odaklanmıştır. Bu çerçevede çalışmanın yukarıda belirtilen tüm çalışmalardan farklı bir boyutu vardır. Ayrıca konunun bilgi güvenliği olması sebebiyle işletmelerin verilerini paylaşmak istememesi ve ülkemizde yeni bir alan olması çalışmayı zorlaştırmaktadır. Bu çalışma görgül bir yöntem ile bilgi üretimi ve model önerisi ile litaratüre katkı sağlamayı hedeflemektedir.

Bu çalışmada; kuruluşlardaki özel bilgilerin (üretim ve hizmet bilgileri, müşteri bilgileri, çalışan bilgileri gibi işletme dışına çıkartılması istenmeyen bilgilerin) güvenli bir ortamda saklanması ve elektronik ortamda saklanan bilgilerin saldırılara ve işletme dışına habersiz bir şekilde çıkmasını engellemeye yönelik olarak kurulan sistemin yönetilmesinde başarı dayanaklarının ne olduğunun ortaya çıkarılması amaçlanmıştır. Bu çerçevede cevabı aranacak temel soru, bilgi güvenliği sisteminin yönetiminde başarıyı artıran ve azaltan ana faktörler nelerdir? Bu soru ile kamu ve özel sektör kuruluşlarında uygulanan bilgi güvenliği sisteminin başarı dayanakları değerlendirilerek, bilgi güvenliği yönetiminin performansını aşağı veya yukarı çeken faktörleri ortaya çıkarmak hedeflenmiştir.

Bu amaçla araştırmada aşağıdaki soruların cevapları aranmıştır.

1) Bilgi Güvenliği ihtiyacını doğuran nedenler nelerdir?
2) Bilgi Güvenliği uygulama yaygınlığı nedir (hangi sektör)?
3) Bilgi Güvenliği Yönetiminde yaşanan sorunlar nelerdir?
4) Bilgi Güvenliği Yönetimini uygulayan kuruluşların kazanımları nelerdir?
5) Bilgi Güvenliği Yönetiminin eksiklikleri nelerdir?
6) Bilgi Güvenliği yönetimi İK gelişimine katkı sağlar mı?
7) Bilgi güvenliğine ilişkin kararların stratejik önemi ve kuruluşun genel stratejisi içerisindeki yeri nedir veya ne olmalıdır?

Araştırmanın Önemi

Bilginin öneminin her gecen gün arttığı dünyamızda, bilginin güvenliği de o kadar önem kazanmıştır. En küçük bilgi güvenliği açıklarının kuruluşlara büyük miktarda maddi ve manevi zararlara yol açtığı bir ortamda kuruluşların bilgi güvenliği yönetim sistemini uygulamaları, bu sistemi geliştirmeleri ve işletmelerde farkındalık yaratması önemini arttırmaktadır.

15.10.2010 tarihli Resmi Gazetede yayınlanan "Elektronik Haberleşme Güvenliği Yönetmeliği" sonucunda Telekomünikasyon Kurumu tarafından yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten sermaye şirketlerinin, bir yıllık süre içerisinde TS ISO/IEC 27001 veya ISO/IEC 27001 standartlarına uyumluluğu yükümlülük haline gelmiştir (R.G., 2009). Bu yönetmeliğin ilerleyen dönemlerde kapsamının genişleyeceği, bilgi işleyen tüm işletmeleri kapsayacağı ve özel sektöründe bu standardı uygulayacağı öngörülmektedir. Ayrıca Ülkemizde "E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları" kılavuzu içerisinde yer alan 4.1.1 Bilgi Güvenliği Yönetim Sistemi (BGYS) maddesine göre kurumlara Bilgi Güvenliği Yönetim Sistemi kurması tavsiye edilmekte ve ihtiyaç sahibi kurumların kendi bünyelerinde BGYS'ye sahip olmaları ve BGYS'yi tamamlayan kurumlara, sertifika belgelendirme çalışmaları yapmaları önerilmektedir (DPT, 2004: 27). Bu gelişmeler ışığında çalışma ayrı bir önem kazanmaktadır.

Uygulanan sistemlerin kuruluşun insan kaynakları, teknolojisi ve süreçlerine katkı sağlaması beklenir. Bu üç olgu üzerine değerlendirmeler yapılması ve bu sistemin irdelenerek kuruluşlara katkı sağlanması acısından bu çalışma oldukça önemlidir.

Araştırmanın Amacı

Günümüzde enformasyon, teknoloji ve iletişim alanındaki büyük gelişmeler toplumları kıyasıya bir rekabete yöneltmiştir. Her geçen gün yeni teknolojik gelişmelerin yaşandığı ekonomik bir yarış söz konusudur. Bu yarış da işletmelerin her türlü bilgilerinin önemli olduğunu ve bu bilgilerin kazanılmasının çok zor süreçler gerektirdiği düşünüldüğünde bu bilgilerin korunması ve devamlılığının sağlanması büyük önem arz etmektedir.

Gelişen teknolojiler sonucunda bilgiye erişimin giderek kolaylaşmasıyla birlikte, bilginin güvenliğinin sağlanması da oldukça zorlaşmıştır. Artan risklere yönelik, daha ciddi ve daha çeşitli önlemlerin alınması gereklilik haline gelmiştir.

Bu çalışma Bilgi Güvenliği Yönetim Sistemini uygulayan kuruluşların bu sistemden maksimum faydalanmalarını, eksik kalan yönlerini geliştirmelerini ve başarı dayanaklarının ortaya konmasını amaçlamaktadır. Çalışmanın diğer amacı da kuruluşlarda bilgi güvenliği farkındalığı yaratarak bu sitemi uygulamayan kuruluşlara bilgi güvenliğinin önemli olduğu, her gecen gün bu önemin arttığını ve bilgilerini güvenli ortamlarda saklamaları gerektiğini dikkate almaları olacaktır.

Araştırmanın Yöntemi

Kuruluşlarda Bilgi güvenliği yönetiminin (TS ISO/ IEC 27001) gerekleri ve başarı dayanaklarının araştırıldığı bu çalışmada anket tekniği yöntemleri kullanılmıştır.

Bu yöntem; yazışma, yazılı iletişim yoluyla veri toplama tekniği olarak tanımlanmaktadır. Mektup, anket, yazılı testler vb'leri, bu tür veri toplamada yaygın olarak kullanılan araçlardır. Anket, belli bir amaç ve plana göre düzenlenmiş "soru listesi" dir. Anketteki soruların kapsamı konunun özelliğine göre değişebilmektedir. Genellikle anketler geniş kitlelere uygulanırlar ve elde edilen sonuçlar üzerinde istatistiksel değerlendirmeler yapılır (Karasar, 2003: 174).

Bu yöntem betimleme teknikleri arasında çok kullanılan bir yöntemdir. Bunun sebebi, kolay, ucuz ve doğrudan doğruya veri toplama tekniği oluşudur. Ayrıca fikirler, inanışlar, tavsiye ve bireysel yaşantılarla ilgili bilgilerin elde edilmesi için de uygun bir yöntemdir (Kaptan, 1973: 235).

Çalışmanın Bilgi Güvenliği Yönetim Sistemi olması sebebiyle bu sistemi uygulayan kuruluşların verilerini paylaşmamaları veri toplama açısından çalışmanın boyutlarını kısıtlamıştır. Bu durum çalışmanın sınırlılığını oluşturmaktadır. Bununla birlikte, Türk Standartları Enstitüsü'nden Bilgi Yönetimi Belgesi alan özel ve kamu sektör kuruluşları ile sınırlı bir anket çalışması yapılabilmiştir.

Bu çalışmada Türk Standartları Enstitüsü'nden Bilgi Güvenliği Yönetim Sistemi (TS ISO /IEC 27001) Belgesine sahip 35 kuruluşa (bkz. Ek 1) Nisan 2013 ayı içerisinde veri toplamak üzere anket gönderilmiştir. Anket örneği Ek 2'de verilmiştir. Önceden hazırlanan bir plan çerçevesinde Bilgi güvenliği yönetim sisteminin başarı dayanaklarının ölçülmesini hedefleyen toplam 9 ana sorudan oluşan ankete 24 kuruluş geri dönüş yaparak bu çalışmaya katılmıştır. Anketten elde edilen veriler ile ilgili yönetim sistemi denetçilerinin sektör denetim tecrübeleri birlikte değerlendirilmiştir.

Araştırma 2 bölümden oluşmaktadır. Birinci bölümde Bilgi ve Bilgi Güvenliği başlığı altında bilginin ve bilgi güvenliğinin tarihsel gelişimi ve önemi ele alınmıştır. Ayrıca kuruluşların bilgi kazanımları, bu kazanımlarını nasıl korumaları gerektiği irdelenmiştir. Bu bölümde Bilgi Güvenliği Yönetim Sistemi (TS ISO/ IEC 27001) standardının yorumlanması ve Bilgi Güvenliği Yönetim Sisteminin (TS ISO/ IEC 27001) kuruluşlara faydaları da açıklanmaktadır. İkinci Bölüm de Bilgi Güvenliği Yönetim Sisteminin (TS ISO/ IEC 27001) başarı dayanakları uygulanan anket ile sorgulanmış ve elde edilen veriler istatistiksel değerleriyle birlikte tablo ve grafikler şeklinde sunulmuştur.

BÖLÜM 1: BİLGİ, BİLGİ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

Bu bölümde, bilgi, bilgi yönetimi, bilgi güvenliği ve bilgi güvenliği standartları ile ilgili kuramsal bir çerçeve sunulacaktır. Bununla, çalışmanın kuramsal arkaplanı oluşturulmaya çalışılacaktır. Arkaplan oluşturulurken bir yandan bu kavramların uygulamadaki karşılıkları, diğer yandan tarihsel gelişimleri değerlendirilecektir. Böylece, tezin katkı sunmayı hedeflediği ülkemizdeki özel ve kamu kuruluşlarının bilgi güvenliği yönetimi bakımından araştırılmasına zemin oluşturulmuş olacaktır.

1.1.Bilgi Kavramı

Bilgi (information) kelimesinin menşei, Latince'deki herhangi bir şeye şekil vermek anlamına 'informare' kelimesinden gelmektedir (Vural, 2007:18).

Bilgi "bilme" eyleminin insan belleğinde oluşan bir çıktısıdır ve bu hali ile insanla ilgili ve insanla sınırlıdır. Bilgisayar dünyasında, günlük dildeki kullanımımızla bilgiyi, veri (data), enformasyon (information) ve fikri mülkiyetin konusu olan bilgi (knowledge) olmak üzere üçşekilde görürüz. (http://www.tse.org.tr/eoq2010).

Bilgi (Information), belli bir formda işlenmiş ve alan için anlamlı olan, halihazırdaki ve gelecekteki kararlar için anlam ifade eden, algılanan veya gerçek değeri olan veri (data) demektir. Kısaca, veri davranışları etkilediği zaman bilgi olmaktadır. Bazen bilgi kesin bir anlam ifade etmeyebilir. Bir karar için anlamlı olan bilgi, başka bir değerlendirme için ham veri demektir. Bu yüzden, kullanılacak olan kişiye bağlı olarak bilgi ve veri birbirinin yerini alacak şekilde kullanılabilir. Herhangi bir uzman için bilgi olan bir değer, kurumun üst yöneticisi için ham veri anlamına gelebilir (Çoban, 1996:123).

Türk Dil Kurumu güncel Türkçe sözlük anlamında ise; insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bilim, malumat, Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat, vukuf, insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf. Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler olarak tanımlanmaktadır (http://www.tdk.gov.tr).

Bilgiyi örgütsel olarak ele alırsak 'Bir örgütün bütün olarak yeni bir bilgiyi yaratması, onu işletme içinde yayması, ürün, hizmet ve sistemlere dönüştürmesidir (Özcan ve Barca, 2008:149).

Bilgiyi daha geniş tanımlayacak olursak "Bilgi belli bir düzen içindeki tecrübelerin, değerlerin, amaca yönelik enformasyonun ve uzmanlık görüşünün, yeni tecrübelerin ve enformasyonun bir araya getirilip değerlendirilmesi için bir çerçeve oluşturan esnek bir bileşimdir. Bilgi bilenlerin beyinlerinde ortaya çıkar ve orada uygulamaya geçirilir. Kuruluşlarda yalnızca belgelerde ya da dolaplarda değil rutin çalışmalarda, süreçlerde, uygulamalarda ve normlarda da kendisini gösterir" (Davenport ve Prusak, 2001: 27).

Bilgi, enformasyonun bir biçimidir ve sadece bireylerin zihinlerinde vardır. Bilgi, öznel (subjektif) bir oluşumdur; bir kişiden diğerine doğrudan doğruya transfer olunamaz veya iletilemez; ama ilk enformasyona dönüştürülebilir. Enformasyon ise, bilginin iletilebilir ve kaydedilebilir şeklidir. Bu durumda enformasyona, bilgiye yönelik bir amaç [aynı zamanda bilgiye de enformasyonun oluşumuna yönelik bir amaç ve araç] gözüyle bakılmalıdır". Nitekim Davenport ve Prusak "bilgi ve enformasyon arasındaki ilişkiyi, nasıl enformasyon veriden doğuyorsa, bilgi de enformasyondan doğar" şeklinde açıklamışlardır. Bilgi, enformasyon ve veri arasındaki ilişkiyi ve bilginin özelliğini şu şekilde açıklamaktadır:

a) Bilginin temelini veri ve enformasyon oluşturur.

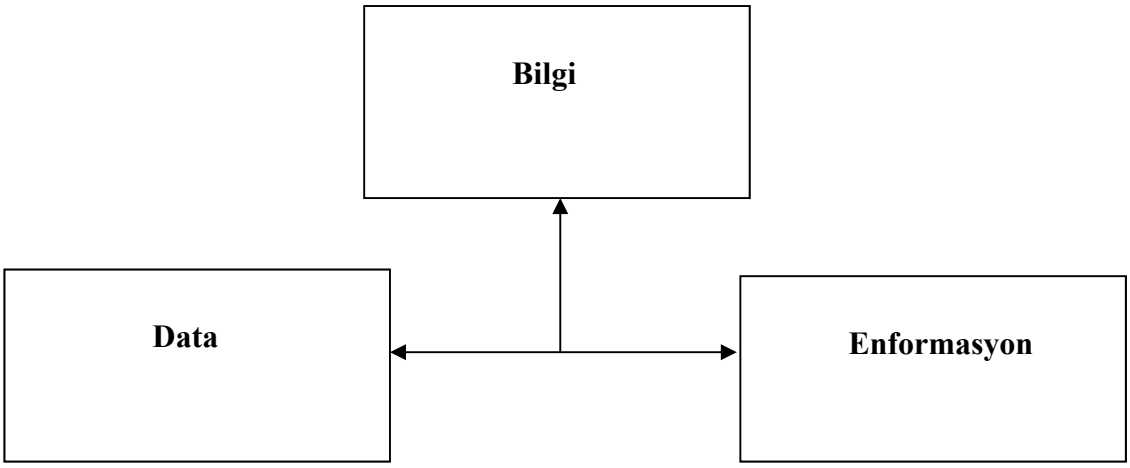
b) Bilgi, enformasyonun rasyonel bir biçimde akıl süzgecinden geçmesi, yorumlanması ve kullanımıyla ortaya çıkar.

c) Bilgi, karar verme, planlama, karşılaştırma, değerlendirme, analiz, tahmin, tanı vb. gibi yaşamın her alanına dayanak oluşturacak eylemlerin ve uygulamaların temelini oluşturur.

Davenport ve Prusak "Bilgi yaratmaya yönelik eylemler insanlarca yürütülmektedir. Veriler, kayıtlarda ve işlemlerde; enformasyon da mesajlarda bulunmaktadır. Buna karşılık, bilgi bireylerden ya da bilenler grubundan veya bazı zamanlarda da kurumun rutin çalışmalarından elde edilmekte ve bilgi, kitaplar ve belgeler gibi belli biçimlere sahip araçlarla [basılı ve elektronik enformasyon kaynaklarıyla] ve sohbetlerle, ustalık

çıraklık ilişkilerine kadar uzanan kişisel ilişkilerle aktarılmaktadır" açıklamasını getirmişlerdir. Yukarıda da değinildiği gibi bu kavramlar birbirleriyle doğrudan ilişkilidir. Bu ilişkiden ötürü doğal olarak bu kavramlar arasında kimi zaman karışıklıklar baş gösterebilmektedir; fakat bu karmaşık ilişkileri birbirinden ayırarak, kavramların sahip oldukları kendilerine özgü anlamlarını ve sınırlarını belirlemek, kavramsal kargaşayı ortadan kaldırmak ve doğru kullanımlarını sağlamak adına önemlidir (Yılmaz, 2009:100-110).

Bilgi, veri ve enformasyon ile ilgili Türkçe'mizde aynı anlamda kullanılmasından dolayı aradaki farkı da belirtmekte yarar vardır. Genelde veri (data) işlenmiş (ham) enformasyon parçacıkları, enformasyon (information) organize edilmiş bir veri seti, ve bilgi (knowledge) anlamlı (anlaşılabilir) enformasyonlardır. Bilgi organize edilmiş iken enformasyon organize değildir. Veri ve enformasyon beyin dışından transfer edilen, alınan ve kaydedilen formlardır. Bilgi ise sadece kişisel olarak insanların beyinlerinde bulunmaktadır. Enformasyon sensörler (alıcılar) vasıtasıyla insan beynine ulaşmakta ve burada enformasyon işleyicisi tarafından öncelikli bilgiler kullanılmak suretiyle yeni bilgiye dönüştürülmekte ve hafızadaki yerini almaktadır. Enformasyon işlemesi yoluyla çok ve yeni enformasyon elde edildiğinden ve işlendiğinden yeni bilgiler elde edilebilmekte ve gelecekteki kullanım için üretilmektedir (Keskin, 2003:176-177). Bahsedilen ilişki alttaki şekilde:1'de görünmektedir.



Şekil 1: Data, Enformasyon ve Bilgi Arasındaki İlişki (Bhatt, 2001:68-75).

1.2.Bilgi Yönetimi

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

Bilgi yönetimi bilginin verimli bir şekilde teknolojik uygulamalara dökülmesindeki süreçlerin tanımlamalarını, modellenmesini ve organizasyonun amaçları doğrultusunda bilginin kullanılması için yapılması gereken hareket planını kapsar.

Bilgi yönetimi, üretken (değer yaratıcı) bilginin elde edilmesi, paylaşılması, geliştirilmesi ve kullanılması ile ilgilidir.

Bilgi yönetimi; Entellektüel sermayeye ilişkin süreçler, ölçümler, değerlendirmeler ve yatırımların dönüşümü gibi konulara odaklanır. Entellektüel sermaye daha önce açıklandığı gibi şirketin sahip olduğu insan, yapısal ve müşteri sermayesidir. Bilgi yönetimi ile bilginin yedeklenmesi kayıp bilgi kontrolü ve sistemdeki bilginin homojen yayılışı amaçlanmaktadır. Bilgi yönetimi adından da anlaşılacağı gibi bir yönetim aracıdır. Şirketin sahip olduğu entellektüel sermayeyi kontrol edilebilir ve yönetilebilir bir varlık olarak görür. Bilgi yönetiminde örgütün kurumsal dinamikleri, süreç analizleri ve bilişim teknolojileri kullanılan temel araçlardır. Bu araçlar, bir örgütteki veri ve bilgi akışını güçlendirir ve bu bilgileri çeşitli görevleri yürütmekle sorumlu bireylere ve gruplara sunar. Özellikle de bilişim teknolojileri bilgi yönetiminin ortaya çıkışının yönetim biliminin gelişmesi yönetim biliminin de teknolojik ve gelişimlerle paralel gelişmesi bilgi yönetiminin uygulamada bilişim teknolojilerinin kullanımı olarak düşünülmesine neden olmuştur. Uygulamadaki diğer bir başka düşünce de bilgi yönetiminin somut bilgi dokümanları olduğudur. Oysa bilgi yönetimi şekilde şirket içinde oluşumundan daha önce bahsedilen her türlü bilginin, entellektüel sermayenin oluşturduğu her şeyin bilgisayarda bir veri tabanına aktarılması veya bunların büyük bir bilgi bankasında depolanması değildir. Bilgi yönetimi, teknoloji, somut dokümanlar değildir. Bunlar bilgi yönetiminin araçlarıdır. Bilgi yönetimi tamamen şirketin yönetim yapısıyla ilgilidir. Bilgi yönetimini merak eden, uygulamak isteyen şirketlerin

dokümantasyon, teknoloji kullanımları yerine yönetim yapılarını gözden geçirmeleri gerekir.

Firmanın sadece üretim, pazarlama vs. konularında gelişme göstermesi, değişime ayak uydurması başarılı olması için yeterli değildir. Çünkü pazar koşullarıyla birlikte yönetim anlayışı da gelişmekte bilgi yönetimi gibi yeni bileşenlerini doğurmaktadır.

Günümüzün rekabetçi ortamında, başarı ile başarısızlık arasındaki fark, işletmenin bilgi yönetimin de ne kadar başarılı olduğunun yani yönetim yapısının nedenli gelişime açık olduğunun altında yatmaktadır.

1.3. Bilgi Güvenliği Kavramı

Bilgi fiziki bir varlık bile değilken, enformasyon veri vb. kavramlar arasındaki yerini tam olarak bulamamışken, patent-faydalı bilgi vb. yeterince tanımadığımız kullanmadığımız yeni kavramlarla mevcut tanımı daha da karmaşıklaştırılmışken, şimdi karşımızda 'bilgi güvenliği' kavramı var. Buna rağmen şunu da fark etmeliyiz ki dünya, uzun süreden bu yana 'bilgi güvenliği'ni tartışıyor (Özkan, 2010:71).

Bilgi, bir organizasyonun diğer önemli ticari varlıkları gibi önemli bir varlığıdır, dolayısıyla is ihtiyaçlarına uygun korunmuş olması gerekmektedir. Globalleşen dünyada, bilişim sektörünün artan gücünün bir sonucu olarak bilgiler, giderek artan sayıda ve çeşitlilikte tehditlere maruz kalmaktadır.

Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmeli ve uygulanmalıdır. Bu politikalar, faaliyetlerin sorgulanması, erişimlerin izlenmesi, değişikliklerin kayıtlarının tutulup değerlendirilmesi, silme işlemlerinin sınırlandırılması gibi bazı kullanım şekillerine indirgenebilmektedir. Bilgi güvenliği daha genel anlamda, güvenlik konularını detaylı olarak ele alan güvenlik mühendisliğinin bir alt alanı olarak görülmektedir. Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler

tarafından elde edilmesini önleme olarak" tanımlanır. Bilgisayar teknolojilerinde güvenliğin amacı ise "kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınmasıdır". Özellikle ülkemizde, ne yazık ki, birçok kurum ve kuruluşun ve her seviyeden bilgisayar kullanıcısının çoğunlukla bilgi ve bilgisayar sistemlerine ve bilgi güvenliğine bakış açısının yeterli seviyede olmadığı tespit edilmiştir. Bilgi güvenliği yönetimi, diğer yönetim sistemleri gibi, bir süreklilik gerektirir. Bu nedenle güvenlik yönetimi bir program yönetimi yaklaşımıyla gerçekleştirilmelidir. Program yönetiminden kasıt planlama, gerçekleştirme ve kontrol etme aktivitelerini içeren ve bu aktiviteleri periyodik olarak gerçekleştirmeyi öngören bir yönetim anlayışıdır. Yeni kurulan bir yönetim sistemi bir proje dahilinde kurulabilir. Proje, tanımı gereği bir başı ve bir sonu olan, bir kereye mahsus gerçekleştirilen, yani rutin operasyonları içermeyen bir çalışmadır. Yönetim sisteminin temel yapı tasları bir proje ile geliştirilebilir ancak sistemin devamlılığı ancak program yönetimiyle gerçekleştirilebilir (http://wwwcagataycebi.com/security/bilgi_gunebligi.pdf).

Bilgi koruma, kuruluşun sahip olduğu özel bilgilerini yasal olmayan ve uygun görülmeyen kullanımdan korumayı amaçlamaktadır. Kuruluş rakipleri ile rekabet edebilmek ve bu rekabette avantajı sağlamak için bilgiyi korumalı ve bunu sürdürebilir hale getirmelidir. Teknolojinin gelişmesi ve insanların istediği bilgilere ulaşmasın kolaylaştığı dünyada bilginin korunması da o ölçüde zorlaşmıştır.

Bu nedenle kuruluşlar çalışanlara yönelik davranış kuralları, iş tanımları ve talimatları gibi uygulamalarla bilgiyi korumak için önlemler almaktadır. Kuruluşlar işletme için gizli ve hayati önem taşıyan bilgiye ulaşmayı sınırlayan teknolojiler, yazılım programları ve sistemler geliştirilmektedir.

Kuruluş kullandığı, elde ettiği ya da kullanmaya hazırlandığı bilgiyi korumalıdır. Aksi halde kuruluş hem rekabet avantajını kaybeder, hem de bilgi yönetimi için geliştirilen kültürel ve yapısal unsurlar etkin bilgi yönetiminin oluşumunu sağlamakta yetersiz kalır. Bilgiyi koruma konusunda başarısız olan kuruluşlar elde edilen bilgi ile verimli sonuç alabilir ancak bu bilgi başka kuruluş tarafından kullanılacağından rekabet avantajı sağlama özelliğini kaybedebilir (Çakar ve Yılmaz, 2010: 77). Bu bilgileri korumanın en

önemli yollarından biri TS ISO EN 27001 Bilgi Güvenliği Yönetim Sistemi oluşturmaktır.

1.4.Bilgi Yönetimi ile Bilgi Güvenliği Yönetim Sistemi Arasındaki İlişkisi

Bilgi yönetimi denildiğinde akla gelen şey yönetsel açıdan dört uygulama alanıdır. Birincisi bilgi ile ilgili faaliyetlerin tepeden aşağı izlenmesi ve sağlanmasıdır. İkincisi, bilgi altyapısının oluşturulması ve sürdürülmesidir. Üçüncüsü bilgi sermayesinin yenilenmesi, örgütlenmesi ve dönüştürülmesidir. Son olarak bilgilerin kullanılmasıdır (Özcan ve Barca, 2008:179). Organizasyonlar için gerekli bir uygulama olan bilgi yönetimi, üç ayaklı bir tabureye benzetilebilir. Üç ayaklı bir taburenin bir ayağı ayrılsa, ayakta durması imkânsız hale gelecektir. Bu üç ayak; insanlar, süreçler ve teknolojiden oluşmaktadır. Çünkü, bilginin bir bireyden diğer bireye aktarılabilmesi için insanlara ve bilginin kullanımını sağlamak için ya da onu işte kullanabilmek için süreçlere gereksinim duyulmaktadır. Teknoloji ise, depolama, tekrar ele geçirme ve geniş enformasyonların insanlar tarafından kullanılabilmesini düzenlemek için zorunludur (Doğan ve Kılıç, 2009:90-91). İşletmelere bilgi yönetimin başarılı olması için Bilgi güvenliğinin amaçları olan bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletilmesi gerekmektedir. Tamamıyla bilginin güvenliğine odaklana ve bunu sürdürebilir hale dönüştürülmesini sağlayan bir sistem olan bilgi güvenliği işletmelerde bilgi yönetimini destekleyen bir olgudur. Bu yönüyle bilgi yönetimine pozitif katkı sağlamaktadır. Bilgi güvenliği yönetimin önemsenmemesi veya olmaması bilgi yönetimini olumsuz bir şekilde etki edecektir.

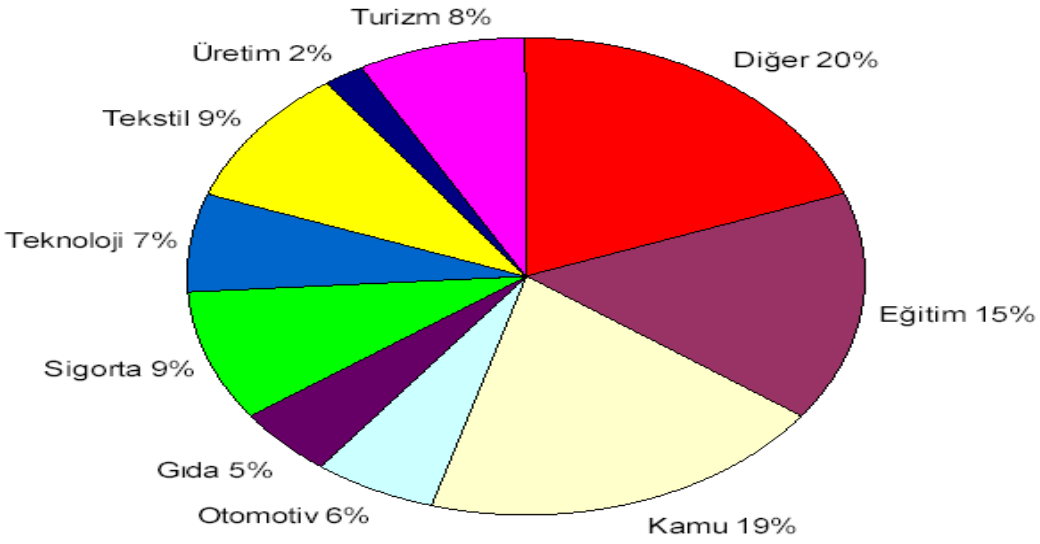
1.5. Bilgi Güvenliği Yönetiminin Gerekleri

"Bilgi ve destek süreçleri, sistemler ve ağlar gibi önemli iş süreçleridir. Bilginin güvenliği rekabet avantajı, nakit akışı, karlılık, yasal uyum ve ticari imaj için gereklidir. Kritik altyapıları korumak için bilgi güvenliği hem kamu sektörü hem de özel sektör için çok önemlidir. Bilgi ve bilgisayar güvenliğinde, karsı taraf, kötü niyetli olarak nitelendirilen kişiler (korsanlar veya saldırganlar) ve yaptıkları saldırılardır. Var olan

bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler saldırı veya atak olarak adlandırılmaktadır. Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi, bilgi güvenliği için büyük bir önem arz etmektedir. (http://www.cagataycebi.com/security/bilgi_guvenligi.pdf)

Ülkenizde özellikle internet ile ilgili ciddi güvenlik acıkları olduğu yapılan araştırmalarda ortaya cıkmıştır. Bu konuda Koç.net şirketini yapmış olduğu ilgili çalışmalar örnek verilebilir. 1025 ADSL kullanıcısı ve 850 şirketin kapsandığı Rizikometre 2005 Türkiye Internet Güvenliği Araştırması Sonuçları'na göre; ADSL eri şimlerinin %65'inin güvenlik duvarı (İng. firewall) kullanmadığı saptanmıştır. Web sunucularının %43'ünün bilgileri kolaylıkla çalınabilir, ana sayfaları değiştirilebilir veya bir başka adrese yönlendirilebilir durumda risk altındadır.Şirketler ve ADSL kullanıcılarının sadece %30'u casus yazılımlara (İng.spyware) karşı korunmaktadır.Alan adı hizmeti (İng. DNS) sunucularının %22'sindeki açıklardan dolayı şirket e-postaları ele geçirilebilir veya çalışanların internet üzerinden eriştiği bankacılık vb. işlemlerde kullanılan şifreler çalınabilir durumdadır.

Kritik güvenlik açıklarının oranı tüm açıkların tamamının %19'u, orta düzey açıkların oranı da tüm açıkların %28'idir; başka bir deyişle araştırmaya katılanların yaklaşık yarısı internet' ten gelecek güvenlik tehditlerine karşı kayda değer düzeyde risk altındadır. Kamu, Eğitim, Turizm, Tekstil ve Sigorta sektörleri risk altındadır.



Şekil 2: Yüksek Düzeydeki Güvenlik Açıklarının Sektör Bazında Dağılımları (Koç.net, 2005).

Bu araştırmada altı çizilmesi gereken bir başka nokta da, ilgili çalışmanın sadece Internet üzerinden ve dışarıdan yapılabilecek tehdit ve saldırıları kapsamış olmasıdır. Bir başka deyişle, kurumlardaki diğer sistemlerin ve içeriden olabilecek saldırılar ve risklerin de kapsama alınması durumunda elde edilecek sonuçların çok daha kötümser bir tablo ortaya koyması beklenebilir. Türkiye'nin de kapsama alındığı diğer bir başka uluslararası araştırmaya göre genel amaçlı bilgi sistemlerinin kurulumunda bilgi güvenliği birimleri süreçlere büyük oranda katılırken insan kaynakları sistemlerinin kurulumunda katılımın yarı yarıya azaldığı görülmektedir. (Bu oran dünyada %69 iken Türkiye'de %53 seviyesinde bulunmaktadır.) Ayrıca, Türkiye'deki kurumların sadece %31'inin iş sürekliliğine yönelik planları olduğu ve bilgi sistemlerinin krizlere, felaketlere hazırlıklı olduğu, dünya genelinde de bu oranın %40 civarında olduğu bulgulanmıştır (Ağaoğlu ve Gökşen, 2009:7)

Dünyada ve Ülkemizde özellikle bilgi işleyen kuruluşlara yönelik yapılan sayısız bilgi güvenliği ihlalleri örnekleri mevcuttur. Bunlara birkaç örnek verecek olursak;

a) **İlk bilgisayar solucanı;** Cornell Üniversitesi Bilgisayar Mühendisliği yüksek lisans öğrencisi olan Robert Morris Jr. tarafından 1988 yılında yazılmıştır. İlk deneysel kendi kendine çoğalan ve yayılan kod parçasıdır ve "worm" adını

almıştır. Fakat tahmin ettiğinden çok daha hızlı sürede çoğalmış ve bilgisayarları tekrar tekrar etkilemiştir. (Bug) Worm çalıştığında İnternetin yaklaşık onda birini oluşturan 6000 bilgisayar çalışamaz hale gelmiştir.

b) **Citibank hesaplarının ele geçirilmesi;** 1995'de Vladimir Levin tarafından gerçekleştirildi. Londra'da laptop (taşınabilir bilgisayar) kullanarak Citibank'ın müşteri isimlerine ve parolalarına ulaştı. Elde ettiği bilgilerle 10 milyon doları farklı hesaplara aktardı. Londra'da tutuklandı ve mahkeme için Amerika'ya gönderildi. 3 yıl hapis cezası ve tazminat ödemeye mahkum edildi.

c) **Conficker (Downadup, Kido) Solucanı;** Microsoft'un 23 Ekim 2008 tarihinde çok acil olduğunu bildirdiği bir güncelleme yayınlamasından 1 ay kadar sonra bu açıklığı kullanan Conficker solucanı ortaya çıktı. İlk başlarda çok fazla dikkat çekmeyen bu solucan, yeni sürümünün çıkmasıyla, 3 milyonun üzerinde bilgisayara bulaştı. Conficker solucanının, 2009 yılının son yarısında 15 milyon bilgisayara bulaşmış olduğu tahmin edilmektedir. Bu bir solucan için çok büyük bir başarıdır. Bu solucanın bir başka özelliği de, bulaştığı bilgisayara da heyecan olsun diye bulaşmaması, o bilgisayarı Bot (robot) bilgisayara çevirmesidir. Conficker solucanı bir bilgisayara bulaştığı zaman tespit edilmesini zorlaştıran ve yayılmasını kolaylaştıran birçok değişiklik yapmaktadır. Hatta Conficker bulaştığı bilgisayardaki anti-virüs programlarının kendilerini güncellemek için bağlanmaları gereken etki alanlarına ulaşmasını da engellemektedir. Yani anti-virüs programınız kendini güncelleyemiyorsa Conficker size çoktan bulaşmış olabilir(http://www.bilgimikoruyorum.org.tr/?b111_bilgi-guvenligi-neden-bu-kadar-onemli).

d) **İnternet Hesabı Hırsızlığı;** Rusya'dan 3 "hacker"ın Türkiye'de internet hesabı bulunan kişilerin adreslerine virüslü mail göndererek hesap bilgilerini elde etmesi ve bu bilgileri Türkiye'deki şebeke elemanlarına iletmesi suretiyle yaklaşık bin kişinin hesabından yüz binlerce dolar çektiği tespit edilendi. Yapılan araştırma sonucunda, mağdurların hesaplarındaki paraların internet şifreleri kullanmak suretiyle başka hesaplara transfer yapılarak çekildiği tespit edildi(http://www.habervitrini.com/haber/1-milyon-kisinin-banka-sifreleri-hackerlerin-elinde-261976/).

e) **Kimlik Bilgileri Çalınası;** Türkiye'deki Kamu kurum ve kuruluşlarının veri tabanlarına girerek 70 milyon vatandaşa ait adres, telefon ve kimlik bilgilerini çalan çetenin bu bilgileri hukuk bürolarına paket programlar halinde sattığı belirlendi. Paketler arasında Telefon Sorgu Programı, Plaka Sorgu Programı gibi başlıklar var. Zanlıların bu bilgileri para karşılığı sattığı açıklandı. Bu bilgiler resmi kurumların dataları, Sigorta bilgileri, adres bilgileri veya araç bilgileri. Bu bilgilere hackelemek veya bir takım programlarla ulaşılmış (http://www.turkhukuksitesi.com/showthread.php?t=52705).

f) **Kredi Kartı Bilgileri Hırsızlığı;** ABD, bugüne kadar gerçekleşen en büyük mali bilgi hırsızlığını konuşuyor. Bankalar ve şirketler için hesap nakli yapan Arizona merkezli 'CardSystems Solutions' adlı şirketin güvenlik sistemini virüs yardımıyla delen hırsız veya hırsızlar, 40 milyon kişiye ait kredi kartı bilgilerini ele geçirdi. Durum, 'MasterCard International'ın güvenlik biriminin uyarısı üzerine anlaşıldı. Kredi kartlarıyla yapılan dolandırıcılıkları belirleyen uzmanların uyarısı üzerine başlatılan araştırmada 40 milyon kredi kartının risk altında olduğu, bu kartlardan 13.9 milyonunun MasterCard müşterilerine ait olduğu ortaya çıkarıldı (http://www.radikal.com.tr/haber.php?haberno=156182, 09.01.2006).

Kuruluşlar bu tip olaylarla karşılaşmak istemiyorlarsa mutlaka bilgi güvenliğini önemsemeleri gerekmektedir. Yukardaki örnekler haricinde kurumsal olarak bakıldığında bilgi güvenliği yönetim sistemine şu somut nedenlerden dolayı da ihtiyaç vardır;

- Kurumsal yönetim
- Bilgi güvenliğinin geliştirilmiş etkinliği
- Piyasada farklılaşma
- Üst yönetim ve müşteri gereksinimlerinin karşılanması
- Küresel kabul görmüş tek standart
- Sigorta pirimlerinde potansiyel olarak daha düşük oranlar

- Odaklanmış çalışan sorumlulukları
- Yasalar ve yasal zorunluluklara uyum
- İletişimin artması sonuçunda bilginin çok fazla sayıda tehdit ve açıklığa maruz kalması
- Personelin, müşterilerin ve yükleyicilerin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanımlarını engellemesi (Ersoy, 2012:9)
- Personel, başkaları tarafından yapılabilecek olan saldırılar nedeniyle suçlanmasının önüne geçilmesi (yetkisiz erişimin engellenmesi ve loglama) (Ersoy, 2012:9)
- Tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması(Ersoy, 2012:9)

Ülkemizdeki kamu ve özel sektör temsilcilerinin bilgi güvenliği yönetim sistemini oluşturulmasının diğer bir nedeni de aşağıda belirtilen Başbakanlık genelgesidir.

2003/48 sayılı Başbakanlık Genelgesi ile yürürlüğe giren e-Dönüşüm Türkiye Projesinin 4.1.1.' inci maddesinde Bilgi Güvenliği Yönetim Sisteminin (BGYS) tüm kurumlarda kurulmasının hedeflendiği belirtilmektedir.

05/08/2005 tarihli ve 25897 sayılı Resmi Gazete'de yayımlanan, 2005/20 sayılı Başbakanlık Genelgesi ile çıkarılan Birlikte Çalışabilirlik Esasları Rehberinde elektronik ortamda sunulan hizmetlerde başarı, güven ortamının sağlanmasına bağlı olduğu vurgulanmıştır. Bu da, güvenlikle ilgili politika ve düzenlemelerin geliştirilmesini gerektirir.

2006/38 sayılı Yüksek Planlama Kurulu Kararı'yla onaylanan ve 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete'de yayımlanan Bilgi Toplumu Stratejisi Belgesinde stratejik öncelikler arasında yer alan bilgi güvenliğinin ülke genelinde ve kamu kurumlarında bilgi sistemleri ile elektronik iletişim ve ağ bağlantılarında güvenliğin sağlanması ve sürdürülmesi için gerekli organizasyonel düzenlemelerin gerçekleştirileceğinden

bahsedilmektedir. Ayrıca, bilgi güvenliğinin sağlanması için yasal düzenlemelerin yapılacağı da vurgulanmaktadır *(*TSE, 2013: 14).

Kuruluşların bilgi varlıklarını korumayı amaçlayan bilgi güvenliği yönetimi Kuruluşlar şu bilgi varlılarını;

Elektronik Veri: SAP ERP verileri, CBS verileri, Active directory verileri, E-posta, Doküman Yönetim Sistemi -Arşiv verileri, Proje verileri, Santral ve IVR verileri, Araç Takip Verileri, Dosya Sunucusu Verileri

Fiziksel Veri: Müşteri sözleşmeleri, Personel sözleşmeleri, Tedarikçi sözleşmeleri, Gizlilik sözleşmeleri, Sistem prosedürleri, Tedarikçi faturaları, Tahsilat Makbuz ve Faturaları, Gelen Giden Evraklar, Kurum içi Dokümanlar, Bilgi Güvenliği Yönetim Sistem Dokümanları, Kıymetli evrak, Personel özlük dosyaları, İş başvuru formları, SSK, İş Kur, vb. evrak

Yazılım: SAP ERP Yazılımları, İşletim sistemleri, MS Office yazılımları, Antivirüs Yazılımları, Geçiş Kontrol Sistemi, Santral ve Çağrı Merkezi Yazılımları, Grafik Tasarım yazılımları, Adobe Acrobat Yazılımları, Araç Takip, Yedekleme Yazılımları, Veritabanı ve programlama, MS Office Sharepoint, MS Exchange Server 2007

Donanım: Kişisel bilgisayar, Sunucu, Masa telefonu, Faks, Aktif Cihaz, Yedekleme Ünitesi, TV, Projeksiyon Cihazı, POS Makinesi, Tarayıcı

Mobil Cihaz: Dizüstü bilgisayar, Cep telefonu, Telsiz, El terminali, Telsiz telefon, Fotoğraf Makinesi ve kamera, Araç takip sistemleri, Seyyar Diskler, GPRS Data Kartı

Hizmetler: Telefon santrali, Çağrı merkezi, Yangın algılama, Yangın söndürme, Kablolama, Güvenlik kamerası, Isıtma/soğutma, Kapalı devre TV, Q-Matic (Sıramatik), UPS, Jeneratör, Elektrik ve Aydınlatma,

Personel: Üst yönetim ekibi, Orta kademe yöneticiler, Uzman personel, Diğer Personel

Müşteri: Abone, Potansiyel abone

Kurumsal Değerler: Marka, İmaj

Bilgi Güvenliği Yönetim Sistemi içerisinde bulunan risk değerlendirme modelini uygulayarak kuruluşlara ait özel bilgileri korur ve sürekliliğini sağlarlar.

Risk Değerlendirmeyi şöyle bir örnek ile açıklayacak olursak;

Bilgi varlıkları, risk analizinde işe etki seviyesi dikkate alınarak aşağıdaki tabloda belirtildiği gibi değerlendirilebilir.

Tablo 1: Risklerin İşe Etki Tablosu

İşe Etki Seviyesi		**Açıklama**
Yüksek	3	100.000 TL. üzeri maddi zarar
Orta	2	10.001 - 10.000 TL. aralığında maddi zarar
Düşük	1	10.000 TL.' nin altında maddi zarar

Not: Bu değerlendirme kuruluşlar arası farlılık gösterebilir.

A. Tehditler:

Bilgi varlıklarının risk analizinde, aşağıda belirtilen tehditler dikkate alınır:

1. Kişilerin kasıtlı ve yetkisiz eylemleri:
2. Mücbir Sebepler
3. Kişilerin hataları
4. Ekipman/yazılım/hat arızası
5. Diğer

Tehditler risk analizinde 3 seviyede değerlendirilir:

Tablo 2: Tehdit Seviyesi Tablosu

Tehdit Seviyesi	
Yüksek	3
Orta	2
Düşük	1

Risk analizinde dikkate alınan tehditlerin detayı ilgili kategorilerde belirtilmiştir.

Kişilerin kasıtlı ve yetkisiz eylemleri:

1. Kundakçılık ve vandalizim
2. Bombalı saldırı
3. İletişime sızma / hacking
4. Gizlice dinleme
5. Endüstriyel eylem
6. Kötü niyetli yazılım (örnek: virüs, solucan, turuva atları)
7. Sahte kullanıcı kimliği kullanımı
8. Yetkisiz kişilerin ağa erişimi
9. Sabotaj
10. Terörist saldırı
11. Hırsızlık
12. Depo ortamlarının yetkisiz kullanılması
13. Ağ araçlarının yetkisiz şekilde kullanılması
14. Yazılımların yetkisiz kişilerce kullanılması
15. Yazılımların yetkisiz şekilde kullanılması (lisansız yazılım)
16. Personelin kasıtlı zarar vermesi
17. Eski personelin kasıtlı zarar vermesi

Mücbir Sebepler:

18. Tozlanma
19. İletişim hatlarına/kablolara zarar gelmesi

20. Çevresel felaket
21. Aşırı sıcaklık ve nem
22. Güç kaynağı kesintileri
23. Güç seviyesinde dalgalanmalar
24. Su kesintileri
25. Yangın
26. Deprem
27. Sel
28. İklimsel hasar (fırtına, kasırga, vb.)
29. Yıldırım çarpması

Kişilerin Hataları:

30. Kullanıcı hatası
31. Bakım hataları
32. İşletme/destek personeli hatası

Ekipman/yazılım/hat arızası:

33. Havalandırma arızası
34. Depolama ortamının bozulması
35. Ağ bileşenlerinde arıza
36. Donanım arızası
37. Ortamın okunamaması

38. Düşük kaliteli yazılım ve donanım işletilebilirliği

39. Yazılım arızası

40. Aşırı trafik

Diğer:

41. Kilit personelin istifa etmesi veya yetersizliği

B. Açıklıklar:

Açıklıklar risk analizinde 3 seviyede değerlendirilir:

Tablo 3: Açıklık Seviyesi Tablosu

Açıklık Seviyesi	
Yüksek	3
Orta	2
Düşük	1

C. Olasılık:

Risklerin meydana gelme olasılığı için aşağıdaki tabloda belirtilen olasılık seviyeleri dikkate alınır:

Tablo 4: Olasılık Seviyesi Tablosu

Olasılık Seviyesi		**Açıklama**
Yüksek	3	Her ay birden fazla
Orta	2	6 ayda 1 kez
Düşük	1	Yılda 1 kez veya hiç

D. Risk Değeri: Bu tehditlerin çarpımından oluşan risk değerlendirme tablosu aşağıda belirtilmektedir.

Tablo 5: Risk Değeri Tablosu

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

Oluşan riskler kırmızı ise yüksek, sarı ise orta ve yeşil ise düşük olarak değerlendirilir ve buna göre gerekli tedbirler alınır. Kurulan bu sistem sayesinde kuruluşlarda olabilecek bilgi güvenliği ihlallerinin önüne geçilmiş ve tüm varlıların korunması sağlanmış olur.

1.6. Bilgi Güvenliği Yönetim Sistemi (TS ISO/IEC 27001)

1.6.1. Bilgi Güvenliği Yönetim Standardının Tarihçesi

Bilgi ve iletişimin büyük bir önem kazandığı dünyada şirketlerin verimliliklerini artırabilmeleri, pazarda etkin rol oynamaları, müşteri ve Pazar paylarını artırmaları ve rekabet üstünlüğü sağlayabilmeleri için bilgi edinme ve bilgileri işleme konusunda gerekli teknolojileri kullanmaları, süreçlerini bilgi yönetimine göre şekillendirmeleri ve insan kaynaklarını bu yönde yetiştirmeleri gerekmektedir. Geleneksel is dünyasında bilişim sistemlerine gittikçe artan bağımlılık, bilişim dünyasının sunduğu olanaklar ve tüm bunların getirdiği iş fırsatları ve riskler ister istemez "bilgi" kavramının da yönetimsel bir yaklaşımla stratejik seviyede ele alınmasına ve kurumları bu alanda sistem yaklaşımları kurmaya zorlamıştır (Sunay, 2006:28). Bu gelişmeler ve doğrultusunda İngiltere de bazı sektörlerin talebi doğrultusunda adı duyulmaya başlamıştır.

Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından yayınlanan bir diğer standart BS 7799-1 ise bilgi güvenliğinin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Bu da yine ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıştır. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu (Dinçer ve Dinçkan, 2007:7).

Bilgi güvenliği yönetimi sisteminde en çok "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardı kullanılmaktadır. Kuruluşlara bilgi güvenliği yönetimini uygulamak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar bir nevi kılavuz standarttır. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, dokümante edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir. Bu iki standardın Türkçe halini TSE tarafından TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Bu standartların belgelendirmesi konusunda TSE TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu standardını yayınlanmıştır. ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart da doğrudan bilgi güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir. Standardın Tarihsel gelişimi aşağıdaki tabloda belirtilmektedir.

Tablo 6: Standardın Tarihsel Gelişimi

1	Endüstri çalışma grubunun kurulması	1993
2	Kural rehberi olarak yayınlanması(BS-7799-1)	1993
3	İngiliz Standardı olarak kabulü	1995
4	BS 7799-2'nin oluşturulması	Şubat 1998
5	BS- 7799-1 ve BS 7799-2 bölümlerinin gözden geçirilmesi	Mayıs 1999
6	BS- ISO/IEC17799(BS 7799-1: 2000) Geçiş Versiyonu	Ocak-Ağustos 2000
7	ISO tarafından yayınlanması	Aralık 2000
8	İngiltere'de BS- ISO/IEC 17799:2000/BS 7799-1: 2000 olarak adlandırılması	2000
9	BS 7799-2: 2002'nin yayınlanması	5 Eylül 2002
10	TS ISO/IEC 17799'un TSE Teknik Kurulu tarafından kabulü	11 Kasım 2002
11	TS 17799-2'nin TSE Teknik Kurulu tarafından kabulü	17 Şubat 2005
12	TS 17799-2'nin TSE Teknik Kurulu tarafından iptali	2 Mart 2006
13	TS ISO/IEC 27001:2005'in TSE Teknik Kurulu tarafından kabulü	2 Mart 2006

1.6.2. Bilgi Güvenliği Yönetim Sistemi İlgilendiren Standardlar

Bilgi güvenliği yönetim sistemi ile ilgili yürürlükte olan standardlara ait bilgiler Tablo 7-17 aralığında verilmiştir.

Tablo 7: TSE GUIDE 13268-1 (TSE GUIDE 13268-1, 2007)

Doküman No	TSE GUIDE 13268-1
Türkçe Adı	TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) belgelendirmesi için gereksinimler ve hazırlık kılavuzu
İngilizce Adı	Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001
Türkçe Kapsamı	Bu standard, standardların uygun şekilde kullanılmasını desteklemek amacıyla, BGYS (Bilgi güvenliği yönetim sistemi) TS ISO/IEC 27001 standardında belirtilen gereksinimler ile TS ISO/IEC 17799'da belirtilen en iyi uygulama hakkında kılavuzu kapsar.
İngilizce Kapsamı	This document provides guidance on the requirements specified in the ISMS(Information security management system) standard ISO/IEC 27001:2005 and the best practice described in ISO/IEC 17799:2005 to support the appropriate use of these standards.
Kabul Tarihi	13.03.2007

Tablo 8: TSE GUIDE 13268-2 (TSE GUIDE 13268-2, 2007)

Doküman No	TSE GUIDE 13268-2
Türkçe Adı	TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) gerçekleştirmelerinin etkinliğinin ölçülmesi kılavuzu
İngilizce Adı	Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001
Türkçe Kapsamı	Bu kılavuz BGYS standardı olan TS ISO/IEC 27001'in gerektirdiği şekilde BGYS gerçekleştirmelerinin etkinliğinin ölçülmesi hakkında bilgi verir ve BGYS gerçekleştirmesinin etkinliğinin ölçülmesine yardımcı olur.
İngilizce Kapsamı	This guide provides information and help on measuring the effectiveness of ISMS (Information Security Management System) implementations, as required by the ISMS standard, ISO IEC 27001:2005.
Kabul Tarihi	22.05.2007

Tablo 9: TSE GUIDE 13268-3(TSE GUIDE 13268-3, 2007)

Doküman No	TSE GUIDE 13268-3
Türkçe Adı	TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) denetimine hazırlık kılavuzu
İngilizce Adı	Are you ready for an ISMS audit based on ISO/IEC 27001?
Türkçe Kapsamı	Bu kılavuz aşağıdaki başvuru dokümanlarıyla birlikte TS ISO/IEC 27001 standardında belirtilen gereksinimlere göre kuruluşun kendi BGYS'sinin durumunun belirlenmesine yardımcı olacak prosedürleri kapsar
İngilizce Kapsamı	This guide provides a means to help organizations assess their ISMS with respect to the requirements specified in ISO IEC 27001:2005.
Kabul Tarihi	22.05.2007

Tablo 10: TSE GUIDE 13268-4 (TSE GUIDE 13268-4, 2009)

Doküman No	TSE GUIDE 13268-4
Türkçe Adı	TS ISO/IEC 27001'i esas alan bilgi güvenliği yönetim sistemi (BGYS) kontrollerinin gerçekleştirilmesi ve denetlenmesi kılavuzu
İngilizce Adı	Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001

Tablo 10'un devamı

Türkçe Kapsamı	Bu standard, TS ISO/IEC 27001 Bilgi güvenliği yönetim sistemleri - Gereksinimler standardına uygun belgelendirme için kuruluşların hazırlık yapmalarına yardımcı olmak üzere mevcut kontrol gereksinimlerinin denetlenmesi maksadıyla BGYS kontrol gereksinimlerinin gerçekleştirilmesi konusunda yol gösterir. Bu standardın içeriği, TS ISO/IEC 27001'e göre belgelendirmeyi düşünen kuruluşlar tarafından çözümlenmesi gereken BGYS kontrol gereksinimlerini kapsar. Bu standardın 2'nci maddesi TS ISO/IEC 27001'in Ek-A'sındaki kontrollerin her birini iki farklı açıdan ele alır.
İngilizce Kapsamı	This guide provides guidance on the implementation of ISMS control requirements for auditing existing control implementation to help organizations preparing for certification in accordance with ISO/IEC 27001:2005, Information Security Management Systems - Requirements.
Kabul Tarihi	26.03.2009

Tablo 11: TS ISO/IEC TR 18044 (TS ISO/IEC TR 18044, 2007)

Doküman No	TS ISO/IEC TR 18044
Türkçe Adı	Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği ihlal olayı yönetimi
İngilizce Adı	Information technology - Security techniques - Information security incident management
Türkçe Kapsamı	Bu standard; bilgi güvenliği yöneticileri ile bilgi sistemi, hizmeti ve bilgisayar ağları yöneticilerine bilgi güvenliği ihlal olayı yönetimi konusundaki tavsiyeleri kapsar.
İngilizce Kapsamı	This standart provides advice and guidance on information security incident management for information security managers, and information system, service and network managers.
Kabul Tarihi	13.03.2007

Tablo 12: TS ISO/IEC 27001(TS ISO/IEC 27001, 2006)

Doküman No	TS ISO/IEC 27001
Türkçe Adı	Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – Gereksinimler
İngilizce Adı	Information technology — Security techniques — Information security management systems — Requirements
Türkçe Kapsamı	Bu standard, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kar amaçlı olmayan kuruluşlar) kapsar. Bu standard, dokümante edilmiş bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir.
İngilizce Kapsamı	This standard covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
Kabul Tarihi	02.03.2006

Tablo 13: TS ISO/IEC 17799 (TS ISO/IEC 17799, 2006)

Doküman No	TS ISO/IEC 17799
Türkçe Adı	Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri
İngilizce Adı	Information technology - Security techniques - Code of practice for information security management
Türkçe Kapsamı	Bu Standard bir kuruluşta bilgi güvenliği yönetimini gerçekleştirmek, uygulamak ve sürdürmek için kılavuzu ve genel prensipleri kapsar. Bu standardda belirtilen amaçlar bilgi güvenliği yönetiminin genel kabul görmüş gayeleri üzerinde genel kılavuzluk sağlar. Bu doküman kuruluşun güvenlik standardlarını ve etkin güvenlik yönetim uygulamalarını geliştirmek için pratik bir kılavuzluk ve güvenli kuruluş içi iletişim sağlar.
İngilizce Kapsamı	This International Standard establishes guidelines and general principles for initiating, implementing and maintaining information security management in an organization. The objectives outlined in this standard provide general guidance on the commonly accepted goals of information security management. This document may serve as a practical guideline for developing organizational security standards and effective security management practices, and to provide confidence in inter-organizational dealings.
Kabul Tarihi	21.12.2006

Tablo 14: TS ISO/IEC 27006 (TS ISO/IEC 27006, 2010)

Doküman No	TS ISO/IEC 27006
Türkçe Adı	Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemlerinin denetimini ve belgelendirmesini yapan kuruluşlar için gereksinimler
İngilizce Adı	Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
Türkçe Kapsamı	Bu standarda, ISO/IEC 17021 ve ISO/IEC 27001'de bulunan gereksinimlere ilaveten bilgi güvenliği yönetim sisteminin (BGYS) denetimini ve belgelendirmesini yapan kuruluşlar için gerekler ve açıklayıcı bilgiler verilmiştir. Bu standardın temel amacı, BGYS belgelendirmesini yapan kuruluşların akreditasyonunu sağlamaktır. Bu standardda bulunan gereksinimlerin, BGYS belgelendirmesini yapan kuruluşlar tarafından yeterlilik ve güvenilirliğin gösterilmesi gerekir ve bu standardda bulunan kılavuz bilgiler, BGYS belgelendirmesini yapan kuruluşların herhangi biri için bu gereksinimlerin ilave yorumlanmasını sağlar.
İngilizce Kapsamı	ISO/IEC 27006:2007 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in ISO/IEC 27006:2007 need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in ISO/IEC 27006:2007 provides additional interpretation of these requirements for any body providing ISMS certification.
Kabul Tarihi	29.04.2010

Tablo 15: TS EN ISO 27799 (TS EN ISO 27799, 2009)

Doküman No	TS EN ISO 27799
Türkçe Adı	Sağlık bilişim - Sağlık Bilgi güvenliği yönetimi kullanarak ISO / IEC 27002
İngilizce Adı	Health informatics - Information security management in health using ISO/IEC 27002
Türkçe Kapsamı	Bu standard, sağlık bilişiminde ISO/IEC 27002 standardının uygulanması ve yorumlanması konusunda bir kılavuzu kapsar
İngilizce Kapsamı	ISO 27799:2008 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard.
Kabul Tarihi	09.04.2009

Tablo 16: TS ISO/IEC 27000 (TS ISO/IEC 27000, 2012)

Doküman No	TS ISO/IEC 27000
Türkçe Adı	Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Genel bakış ve sözlük
İngilizce Adı	Information technology - Security techniques -- Information security management systems - Overview and vocabulary
Türkçe Kapsamı	Bu standard, a) BGYS standardları ailesine genel bir bakışı; b) bilgi güvenliği yönetim sistemlerine (BGYS) bir girişi; c) Planla-Uygula-Kontrol et-Önlem al (PUKÖ) sürecinin kısa bir açıklamasını ve d) BGYS standardları ailesinde kullanılan terimler ve tariflerini kapsar.
İngilizce Kapsamı	This standard provides: a) an overview of the ISMS family of standards; b) an introduction to information security management systems (ISMS); c) a brief description of the Plan-Do-Check-Act (PDCA) process; and d) terms and definitions for use in the ISMS family of standards.
Kabul Tarihi	19.07.2012

Tablo 17: TS ISO/IEC 27011 (TS ISO/IEC 27011, 2011)

Doküman No	TS ISO/IEC 27011
Türkçe Adı	Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği yönetim sistemleri – Telekomünikasyon kuruluşları için ISO/IEC 27002 standardını temel alan bilgi güvenliği yönetimi kılavuzu
İngilizce Adı	Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
Türkçe Kapsamı	Bu standard, telekomünikasyon kuruluşlarında Bilgi Güvenliği Yönetiminin gerçekleştirilmesini destekleyen kılavuzların tanımlanmasını kapsar.
İngilizce Kapsamı	The scope of this standard is to define guidelines supporting the implementation of Information Security Management in telecommunications organizations.
Kabul Tarihi	22.03.2011

1.6.3. Bilgi Güvenliği Yönetim Sistemi Terminolojisi

Bilgi: Bilgi bir kurumun en önemli değerlerinden birisidir ve sürekli korunması gerekir (TS ISO IEC 17799, 2006:2).

Güvenlik: İç veya dış kaynaklı, kasıtlı veya kasıtsız olabilecek tehditleri katlanılabilir seviyeye çekmek.

Bilgi Güvenliği: Bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletilmesi (Tekerlek, 2008:132).

Yönetim: Belirli bir amaç doğrultusunda sistem elemanlarını koordineli olarak çalıştırmak(TSE, TS EN ISO 9000 :2004).

Başka bir tanım yapacak olursak 'Başkaları vasıtası ile iş görmek' de diyebiliriz (Koçel, 2007:13).

Sistem: Birbiriyle ilişkili veya etkileşimli elemanlar takımı (TSE, TS EN ISO 9000 :2004.7).

Diğer bir tanımlamada ise 'belli parçalardan (alt birimlerden ve alt sistemlerden) oluşan, bu parçalar arasında belirli ilişkiler olan, bu parçaların aynı zamanda dış çevre ile ilişkisi olan, bir bütün olarak tanımlama mümkündür' (Koçel,2007:177-178).

Yönetim Sistemi: Politika ve hedefleri oluşturma ve bu hedefleri başarma sistemi (TSE, TS EN ISO 9000: 2004:7).

Bilgi Güvenliği Yönetim Sistemi: Bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak tanımlanmaktadır (Vural, 2007:81).

Diğer bir tanımda şöyledir; Bilgi Güvenliği Yönetim Sistemi BGYS, kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri sistemlerini kapsar (Dinçer ve Diçkan, 2007:7).

1.7. Bilgi Güvenliği Yönetimini Hangi İşletmeler Uygulayabilir

Bilgi güvenliği TS ISO EN 27001 standardını tüm kamu kuruluşları, özel sektör, organizasyonu ve kısacası bilgilerinin önemli olduğunu düşünen bütün işletmeler uygulayabilir. Bu standard uluslararası bir standard olup ISO üyesi olan tüm ülkelerde

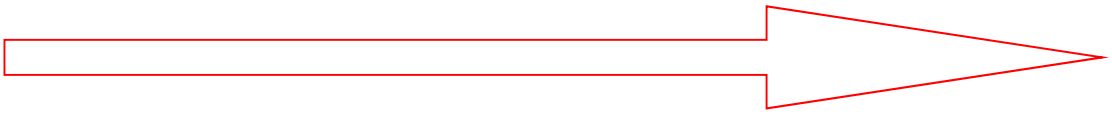
aynı amaç doğrultusunda kullanılmaktadır. Bilgi güvenliği yönetim standardının şirketlerin büyüklüğüne ve birincil öncelik durumlarına göre hangi bölümlerini kullanılması gerektiği aşağıda Tablo 18'de gösterilmektedir.

Tablo 18: Standard Kullanımı (Martin ve Pehlivanlı, 2009: 52)

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

Sektörel olarak firmaların risk durumlarına bakıldığında tarım, inşaat, gıda gibi alanlarda çalışan firmaların düşük ölçekli; otomotiv, kimya enerji gibi alanda çalışan firmaların orta ölçekli; kamu kurumları, savunma sanayi, biyomedikal, elektronik gibi çalışma alanlarındaki firmaların yüksek ölçekli olduğu ((Martin ve Pehlivanlı, 2009:52) aşağıdaki tablo 14 de belirtilmektedir.

Tablo 19: Sektörel Risk Gurupları(Martin ve Pehlivanlı, 2009: 52)



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

Tablo 19'de görüleceği üzere hizmet sektörü olarak adlandırılan ve tüm iş süreçlerini elektronik ortamda yürüten özellikle kamu kuruluşları, finansal hizmetler en yüksek risk altında olan işletmelerdir. Bu nedenle hizmet üreten kuruluşlar aynı zaman da en fazla bilgi güvenliği ihlallerine maruz kalan kuruluşlar olmaktadır.

1.8. Standard Kuruluşları

ISO(International Organization for Standardization-Uluslararası Standardizasyon Teşkilatı) : 23/02/1947 tarihinde kurulmuştur. ISO halen 135 (her ülkeden bir üye) ülkeden ulusal standard kuruluşların katılımı ile faaliyetlerini yürüten bağımsız bir kuruluş olarak; dünyadaki standardizasyon ve benzeri aktivitelerin gelişiminin; uluslar arası ticaret transferi, bilimsel çalışmalar ve ekonomik faaliyetleri kolaylaştıracak şekilde desteklenmesi amacı ile kurulmuştur (Yıldırım, 2000:17). ISO'nun temel amacı; uluslar arası Standardlar konusunda tüm ülkelerin kabulünün sağlanmasıdır

CEN: European Committee for Standardization, Avrupa Standartlarının kısaltmasıdır. EN (Europen Normalisation) Avrupa Birliği'nde Standartlar arasında harmonizasyonu sağlamak için oluşturulmuştur (https://www.cen.eu/cen/pages/default.aspx).

IEC: International Electrotechnical Commission 1906 yılında elektrik, elektronik ve ilgili teknolojiler konusunda uluslararası standard hazırlama çalışmalarına başlayan ve halen 51 üyesi bulunan IEC'ye TSE 1956 yılında üye olmuştur. IEC'nin hedefleri Global pazar gerekliliklerini karşılamak, ürünlerin ve hizmetlerin kalitesini arttırmak, insan sağlığı ve güvenliğine katkıda bulunmak, çevrenin korunmasına katkı sağlamaktır (www.iec.ch).

Bilindiği gibi, uluslararası standartların dünya ekonomisinde ve ticaretinde yeri çok fazla önem taşımakta, bu açıdan IEC üyesi ülkeler bu standartların yapımında gayret sarf etmekte ve bunu, görevi uluslararası standartları geliştirmek ve sistematik kontrollerini yapmak olan teknik ve alt komitelere üye olarak sağlamaktadır (http://www.iso-belgesi.info).

Türk Standardları Enstitüsü(TSE); Her türlü madde ve mamüller ile usul ve hizmet standardlarını yapmak amacıyla 18.11.1960 tarih ve 132 sayılı kanunla kurulmuştur.

Enstitünün ilgili olduğu bakanlık Sanayi ve Ticaret Bakanlığıdır. Enstitü, tüzel kişiliği haiz, özel hukuk hükümlerine göre yönetilen bir kamu kurumu olup, kısa adı ve markası TSE'dir. Bu marka çeşitli şekillerde gösterilir. Türk Standardları Enstitüsü'nün izni olmadan bu marka hiçbir şekil ve şart altında kullanılamaz. Yalnız Türk Standardları Enstitüsü tarafından kabul edilen standardlar Türk Standardı adını alır. Bu standardlar ihtiyari olup, standardın ilgili olduğu bakanlığın onayı ile mecburi kılınabilir. Bir standardın mecburi kılınabilmesi için Türk Standardı olması şarttır. Mecburi kılınan standardlar Resmi Gazete'de yayımlanır (http://www.tse.org.tr/tse-hakkinda/kurulus-ve-gorevleri).

Türk Akreditasyon Kurumu(TÜRKAK): Uygunluk değerlendirme kuruluşlarını akredite etmek, bu kuruluşların ulusal ve uluslararası standartlara göre faaliyette bulunmalarını ve bu suretle uygunluk değerlendirme kuruluşlarınca düzenlenen belgelerin ulusal ve uluslararası alanda kabulünü temin etmek amacıyla tüzel kişiliği haiz, kâr amacı gütmeyen Avrupa Birliği Bakanlığının ilgili kuruluşudur (http://www.turkak.org.tr).

1.9. Ülkemizde Bilgi Güvenliği Yönetim Sistemi Belgelendirmesi Yapan Kuruluşlar

Ülkemizde uluslararası geçerliliği olan ve TÜRKAK tarafından Akredite edilen, Bilgi Güvenliği Yönetim Sistemi Belgesi veren belgelendirme kuruluşları aşağıda Tablo 20'de belirtilmektedir.

Tablo 20: TÜRKAK Onaylı Belgelendirme Kuruluşları.

Belgelendirme Kuruluşu Adı		Belge No	Şehir	Geçerliliği
1	TSE Sistem Belgelendirme Merkezi Başkanlığı	AB-002-YS	Ankara	Aktif
2	Standart BM Trada Belgelendirme A. Ş.	AB-0013-YS	İstanbul	Aktif
3	KALİTEST Belgelendirme ve Eğitim Hizmetleri Ltd. Şti.	AB-0017-YS	İstanbul	Aktif
4	ALBERK QA Uluslararası Teknik Kontrol ve Belgelendirme Ltd. Şti.	AB-0022-YS	İstanbul	Aktif

Tablo 20'nin devamı

5	DENETİK ULUSLARARASI Belgelendirme ve Gözetim Hizmetleri Ltd. Şti.	AB-0079-YS	İstanbul	Aktif

http://www.turkak.org.tr/online/search/akredite.asp?action=searc

Ülkemizin milli belgelendirme kuruluşu olan TSE tarafından belgelendirilen firmaların sayısı ve kapsamı çalışma içerisinde Ek'1 de belirtilmektedir. Diğer belgelendirme kuruluşları ilgili firma isimleri ve kapsamını ticari kaygılar nedeniyle üçüncü şahıslarla paylaşmamaktadır.

Bilgi Güvenliği Yönetim Sistemi için gereklilikleri belirten standart olan TS EN ISO/IEC 27001'in temelindeki düşünce, kurumun hassas bilgilerinin yönetilmesini sağlamak ve etkili bir bilgi güvenliği elde etmek için yönetim sistem süreçlerinin oluşturulması, gerçekleştirilmesi ve sürdürülmesidir. Ayrıca çeşitli büyüklüklerdeki kurumlara uygulanabilecek şekilde planlanmıştır. Söz konusu standart, kurumun sahip olduğu teknolojik imkanlar ve bunların güvenliğiyle ilgilenmez. Bu yönüyle de TS EN ISO/IEC 27001 teknik ve teknoloji bağımlı bir standart değil, asıl olarak bilginin güvenliği ile ilgili bir standarttır (Bingöl, 2010:13).

1.10. Standard Maddelerinin Yorumlanması

TS EN ISO/IEC 27001 Standardı uygulaması aşağıda belirtildiği gibi 8 bölüm ve ilgili EK A Kontrollerinden oluşmaktadır.

0.Giriş

1.Kapsam

2.Atıf yapılan standartlar ve/veya dokümanlar

3. Terimler ve Tarifler

4. Bilgi Güvenliği Yönetim Sistemi

5.Yönetim Sorumluluğu

6.BGYS İç Denetimleri

7.Yönetimin Gözden Geçirmesi

8.BGYS İyileştirme

Ek A - Kontrol amaçları ve kontroller

A5- Güvenlik Politikası

A6- Bilgi Güvenliği Organizasyonu

A7- Varlık Yönetimi

A8- İnsan Kaynakları Güvenliği

A9- Fiziksel ve Çevresel Güvenlik

A10- Haberleşme ve İşletim Yönetimi

A11 Erişim Kontrolü

A12- Bilgi Sistemleri Edinim, Geliştirme ve Bakım

A13- Bilgi Güvenliği İhlal Olayı Yönetimi

A14- İş Sürekliliği

A15- Uyum

Aşağıda bulunan Bilgi Güvenliği Yönetim Sistemi TS EN ISO/IEC 27001 Standardı maddeleri tez çalışması içerisinde uygulanan numaralandırma sistemine göre düzenlenmiş.

1.10.1. Giriş

Standardın bu maddesi sistemi uygulayacak kuruluş hakkında detay bilgilerin yer alması için oluşturulmuştur. (kuruluşun tarihçesi, tanıtımı, adresi, telefonu çalışan sayısı vb. bilgileri)

1.10.2. Kapsam

Standardın bu maddesi kuruluş faaliyetleri hakkında bilgiler içermeli. (sektörü ve faaliyetleri hakkında detaylı bilgiler verilmeli)

1.10.3. Atıf Yapılan Standardlar ve/veya Dokümanlar

Bilgi güvenliği sağlamak etkili bir sistem oluşturmak için kuruluşunu yaptığımız ISO 27001 standardının bilgi güvenliği uygulama prensipleri esas olarak alınmıştır.

1.10.4. Terimler ve Tarifler

Kuruluşumuzda ISO 27001 standardının istediği terimler ve tariflere ilaveten bilgi işlem dünyasında kullanılan tarif ve kavramlarda kullanılmaktadır. Donanımsal ve yazılımsal birçok kavram ve terim Türkçe tanımlamaları ile kullanılmaya çalışılacaktır.

Varlık: Kuruluş için değeri olan ve korunması gereken her şeydir. En somut varlık somut varlık donanımdan en soyut varlık bilgiye kadar tüm unsurlar belirtilmelidir (Mete, 2010: 37). İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi bir organizasyonda her yerde bulunabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Kurum çalışanlarının zihinlerinde, konuşmalarında bulunur (Koç, 2008:6).

Kullanılabilirlik: Yetkili kullanıcıların gerektiğinde bilgiye ve ilişkili varlıklara erişim sağlamasını temin etme, Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği. Kuruluş çalışanları görev talimatlarına göre tanımlanan bilgiye erişim hakları ve gizli şifre bilgileri tanımlanarak kendilerine verilmiştir. Erişim hakkının korunması ve gizliğinin sağlanmasından erişim hakkı verilen yönetici veya personel sorumludur.

Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (örneğin; şifreli e-posta gönderimi ile epostanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir (Çetinkaya, 2008: 16).

Bilgi Güvenliği: Bilginin gizliliğini bütünlüğünü kullanılabilirliğini koruma güvenliği, Bilginin gizliliği, bütünlüğü ve kullanılabilirliğinin korunması. Ek olarak, doğruluk, açıklanabilirlik, inkâr edememe ve güvenilirlik gibi diğer özellikleri de kapsar. Kuruluşumuz bilgi bütünlüğü ve bu bütünlüğü korumak için gerekli donanımsal yapıyı oluşturmuş ve bu konudaki alt yapıyı oluşturarak kuruluş çalışanlarının kullanımına açmıştır. Serverdeki bilgiler sürekli olarak yedeklenerek koruma altına alınmıştır.

Bilgi Güvenliği Olayı: Olası bir bilgi güvenliği politikası açığı, koruyucuların başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun tanımlanan bir ortaya çıkışı.

Bilgi Güvenliği İhlal Olayı: İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayı.

Bilgi Güvenliği Yönetim Sistemi: BGYS Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası. kuruluşumuz bilgi güvenliğini sağlamak etkin kılmak üzere bilgi güvenliği yönetim sistemi uygulamaya karar vermiş bu konuda standardın istekleri doğrultusunda proses haritalarını çıkararak uygulama için gerekli prosedürleri oluşturmuş ve yazılı olarak oluşturduğu dokümanları kayıt altına almıştır. Proseslerin etkin uygulanması için gerekli kayıtları tutmuştur. Kuruluşumuzda elde edilen kayıtlardan veri analizleri yapılarak etkin önleyici faaliyetler oluşturulacaktır. Kuruluşumuzda görev tanımları yapılarak görev tanımına uygun proses haritaları ve bilgi erişim kotları oluşturulmuştur.

Bütünlük: Bilgi ve işleme yöntemlerinin doğruluğunu ve tamlığını koruma Kuruluşumuzun el kitabı BGYS ISO 27001 standardı temel alınarak hazırlanmıştır. Bu kitapta anlatılan Bilgi güvenliği yönetim sistemi tüm kuruluş çalışanları için uygulama sorumluluğu getirir. Bilgi güvenliği yönetim sistemi bilgi güvenliği kurulu tarafından oluşturulur ve tüm kuruluş içerisinde uygulanarak sürekliliği sağlanır ve etkinliği sürekli olarak iyileştirilir. Bilgi Güvenliği yönetim sistemi standardında istenenler ve Kuruluşumuz prosesleri de bilgi kaynaklarını kullanan donanımlar göz önüne alınarak yazılı hale getirilmiştir.

Kuruluşumuzda Bilgi Güvenliği Yönetim Sistemi için ihtiyaç duyulan prosesler, etkileşimleri, birbirine olan etkisi, sırası ve operasyonların etkinliği, izlenmesi, ölçülmesi, analiz edilmesi, sürekli iyileştirilmesi ve risk'ler ve analizleri bunların tamamı kuruluşdaki uygulamaları belirlenmiştir. Ayrıca bu proseslerin çalıştırılmasını ve izlenmesini desteklemek için gereken kaynak ve bilginin hazır bulundurulması üst yönetim tarafından sağlanmıştır. Belirlenen prosesler standardın şartlarına uygun olarak yönetilmektedir. Kuruluşumuzda bilgi güvenliği şartlarına uygunluğunu etkileyecek testlerin yapıldığı Bununla ilgili yazılı dökümanlar oluşturulduğu gibi kayıtların tutulması bütün kuruluş elemanlarının uygulamasıdır.

Artık Risk: Uygulanan kontroller var olan riski tamamen ortadan kaldırmak zorunda değildir. Risk işleme sonrası kalan riske artık risk adı verilir. Uygulanan kontroller sonrası artık risk belirlenmelidir. Eğer bulunan risk seviyesi kabul edilebilir risk seviyesinin üzerinde ise risk analizi ve risk işleme tekrar yapılmalıdır, eğer bulunan artık risk seviyesi kabul edilebilir riskin altında ise artık risk dokümante edilmeli ve varlığı yönetim tarafından onaylanıp kabul edilmelidir (Kandemirli,2102: 95).

Risk Kabulü: Bir riski kabul etme kararı Kuruluşumuzda bilgi güvenliğinin sağlanması için risk kabulü esastır. Bu riskler donanımsal olarak oluşabildiği gibi yazılım nedeni ilerde olaşabilir. Ayrıca kötü niyetli bilgisayar korsanları amatör bilgisayarcılar ve bilgisayar kullanımında yeni olan sistemi ve özelliklerini bilmeyen kullanıcılarda bilgi güvenliği için risk oluşturmaktadırlar. Kuruluşumuz üst yönetimi bütün bu risklerin farkında olup her zaman var olan riskleri kabul eder.

Risk Analizi: Kaynakları tanımlamak ve riski hesaplamak için bilginin sistematik kullanımı Kuruluşumuz kabul edilen riskler ve bu risklere ait risk analiz haritalarını çıkararak gerekli donanım ve yazılım önlemlerini alır risk analizi sonucunda riskin ortaya çıkma ihtimalleri değerlendirilerek riski ortadan kaldırmaya yönelik çalışmalar yapılır.

Risk Değerlendirme: Tüm risk analizi ve risk ölçme prosesi Kuruluşumuzda bilgi güvenliğine yönelik riskler tanımlanıp analiz edilince Risk analizi ve risk ölçme prosesine göre uygulama yapılır. Teknolojinin belirlediği risk ölçme metotları kullanılır

bununla ilgili prosedürlerde risk ölçümleri gösterilip kayıtları tutulur. Risk değerlendirme tabloları oluşturularak riskin oluşma olasılıkları tanımlanır.

Risk Derecelendirme: Riskin önemini belirlemek için hesaplanan riske karşılık verilen risk kriterlerini karşılaştırma prosesi.

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçekleşmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir (Kandemirli,2102: 84)

Risk Yönetimi: Kuruluşumuzda risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetlerin tamamı risk yönetimini oluşturur.

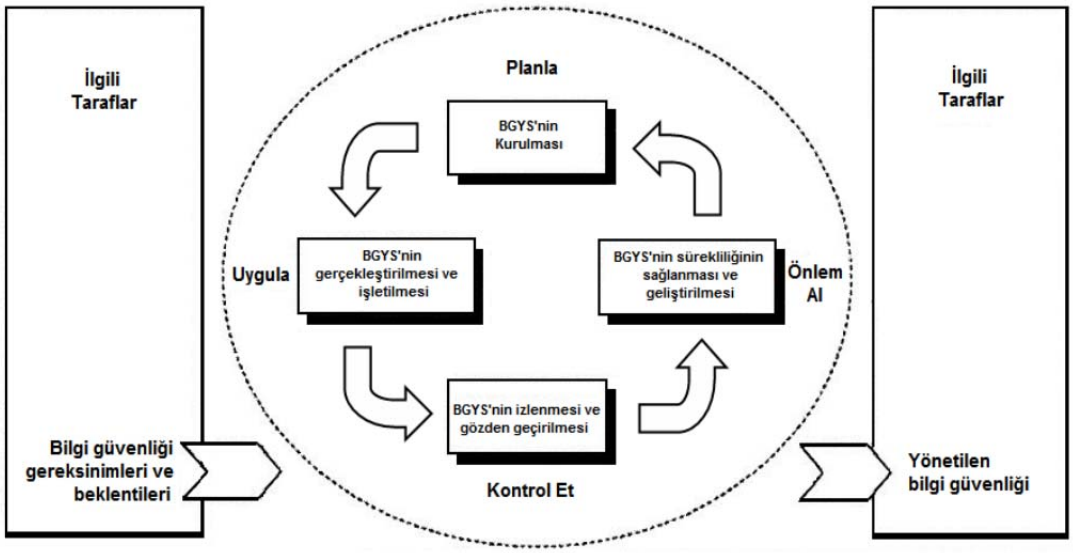
Risk İşleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması prosedür. Kuruluşumuzda risk işleme etkin olarak uygulanmaya çalışılmaktadır.

Uygulanabilirlik Bildirgesi: Kuruluşumuz BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşumuzun bilgi güvenliği için iş gereksinimlerini temel alır.

Bilgi Güvenliği Yönetim Sistemi: Kuruluşumuz bilgi güvenliği el kitabı diğer tüm dokümanlardan bağımsız olarak ve tüm doküman sistemimize referans teşkil edecek şekilde bir şemsiye oluşturacak doküman olarak bilgi güvenliği kurulu başkanı tarafından hazırlanır ve Genel Müdür tarafından onaylanarak yürürlüğe girer. Bilgi güvenliği el kitabında prosedür ve talimat, form gibi dokümanlara atıf yapılır. Bilgi güvenliği el kitabı kuruluşumuzun tüm faaliyetleri hakkında bilgi verecek şekilde hazırlanır. Her hangi bir kuruluş faaliyetimiz bilgi güvenliği Yönetim Sistemi dışında tutulmamaktadır. Bilgi güvenliği el kitabı tüm 27001 bilgi güvenliği yönetim sisteminin anlatılması için bir referans teşkil eder.

1.10.5. Genel Gereksinimler

Kuruluşumuz dokümante edilmiş bir BGYS'yi, kuruluşun tüm ticari faaliyetleri ve karşılaştığı riskleri bağlamında,kurup gerçekleştirmiş, işletmiş , izlemiş, gözden geçirerek , etkinliğini sürdürerek geliştirmiştir.. Bu standardın bir gereği olarak, kullanılan proses, Şekil 4'de gösterilen PUKÖ modeline dayanır.



Şekil 3: BGYS Proseslerine Uygulanan PUKÖ Modeli(TSE, TS ISO/IEC 27001 2006:2)

Tablo 21: PUKÖ Modeli Açıklaması (TS ISO/IEC 27001, 2006)

Planla (BGYS'nin kurulması)	BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi
Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi)	BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi
Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi)	BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi
Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)	Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir.

PUKÖ modelinde gösterildiği gibi (Planla – Uygula – Kontrol et – Önlem al) faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir. PUKÖ modeli özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır. BGYS kurulumu PUKÖ modelinin ilk adımını (Planla) teşkil etmektedir. Yerleşik bir sistemden bahsedebilmek için diğer adımların da uygulanması ve bunların bir döngü içinde yaşaması gerekir. Bilgi güvenliği yönetim sistemlerinin uygulanmasından sorumlu olan bilgi güvenlik yöneticilerinin karşılaştıkları en büyük problem, bilgi güvenliğinin sağlanması amacıyla alınan önlemlerin kesin hatlarıyla uygulanmaya dökülmemesidir (Tekerlek, 2008:132)

Bilgi güvenliği yönetim sistem dokümantasyonu aşağıda başlıklar halinde belirtilmektedir;

Bilgi Güvenliği Politikası

Bilgi güvenliği Hedefleri

Bilgi Güvenliği El Kitabı

Bilgi erişim ve organizasyon

BGYS Prosedürleri

Proses Haritaları

Risk analiz ve haritaları

Talimatlar

Planlar

Formlardan

Listelerden, oluşmalıdır.

Bilgi güvenliği Yönetim Sistemi içerisinde yer alan dokümanlar yeterlilik açısından onaylanmaktadır. Dokümanların gözden geçirilmesi, gerektiğinde güncelleştirilmesi

durumunda onay işlemi tekrarlanmaktadır. Doküman değişikliklerinin ve güncel revizyon durumunun belirlenmesi, yürürlükteki dokümanların ilgili baskılarının kullanım noktalarında bulunabilir olması, dokümanların okunabilir kalmasının, kolaylıkla belirlenebilmesi, dış kaynaklı dokümanların belirlenmesinin ve kontrol edilmesinin, güncelliğini yitirmiş dokümanların herhangi bir amaçla saklanmaları durumunda istenmeyen kullanımının önlenmesi için uygun bir işaretleme uygulanması sağlanmıştır.

1.10.6. Bilgi Güvenliği Yönetim Sisteminin Kurulması Yönetilmesi

İşin, Kuruluşumuz, yerleşim yerinin, varlıklarının ve teknolojisinin özelliklerine göre ve kapsamdan herhangi bir dışarıda bırakmanın ayrıntıları ve açıklamasını da ekleyerek, BGYS kapsamını ve sınırlarını tanımlaması yapılarak BGYS politikası tanımlanmıştır.

Amaçlarını ortaya koymak için bir çerçeve içeren ve bilgi güvenliğine ilişkin bir eylem için kapsamlı bir yön kavramı ve prensipleri kuran, İş ve yasal ya da düzenleyici gereksinimleri ve sözleşmeye ilişkin güvenlik yükümlülüklerini dikkate alan, BGYS kurulumu ve sürdürülmesinin yer alacağı stratejik kurumsal ve risk yönetimi bağlamını düzenleyen, Riskin değerlendirileceği kriterleri kuran ve Yönetim tarafından onaylanmış olan. Politika yayınlanmıştır. iş bilgisi güvenliğine, yasal ve düzenleyici gereksinimlere uygun bir risk değerlendirme metodolojisi tanımlanarak, Riskleri kabul etmek için kriterler geliştirme ve kabul edilebilir risk seviyelerini tanımlama, Seçilen risk değerlendirme metodolojisi, risk değerlendirmelerinin karşılaştırılabilir ve yeniden üretilebilir sonuçlar üretmesini sağlanmıştır.

1.10.7. Dokümantasyon Gereksinimleri

1.10.7.1. Dokümantasyon

Kayıtlar Kuruluşumuzun bilgi güvenliği yönetim sisteminin çalışmasında ispat unsuru taşıyan ve geçmişte yapılan uygulamaları izlenmesine yarayan özel dokümanlardır. Kayıtlar saklanma öncelikleri göz önüne alınarak belirlenir. Kayıtların saklanma süreleri ile saklama sorumlulukları belirlenir. Kuruluşumuzda kayıtların okunabilir olarak kalması, kolaylıkla ayırt edilmesi ve tekrar elde edilebilmesi kayıtlara kolaylıkla ulaşılabilme sağlanır. Kayıtların belirlenmesi, muhafazası, korunması, tekrar elde

edilebilir olması, saklama süreleri ve elden çıkarılması için gereken kontroller belirlenmiş ve aşağıda atıf yapılan prosedürde detaylı olarak Belirtilmiştir

1.10.7.2. Dokümanların Kontrolü

BGYS tarafından gerek duyulan dokümanlar korunarak kontrol edilmiştir. Dokümante edilmiş bir prosedür, oluşturulmuştur: Yayınlanmadan önce dokümanları uygunluk açısından onaylama, gerektiğinde dokümanları gözden geçirme, güncelleme ve tekrar onaylama, Doküman değişikliklerinin ve mevcut revizyon durumunun tanınmasını sağlama, Uygulanabilir dokümanların ilgili sürümlerinin kullanım noktalarında kullanılabilir olmasını sağlama, Dokümanların okunaklı ve hazır olarak tanınabilir olmasını sağlama, Dokümanların ihtiyaç duyanlar için kullanılabilir olmasını, aktarılmasını, saklanmasını ve sınıflandırılmalarına uygun prosedürlerle tamamen yok edilmelerini sağlama, Dış kaynaklı dokümanların tanınmasını sağlama, Doküman dağıtımının kontrol edilmesini sağlama, gerçekleştirilmiştir.

1.10.8. Kayıtların Kontrolü

Kayıtlar, gereksinimlere uygun ve BGYS'nin etkin işlediğine dair kanıtları sağlayacak şekilde oluşturulmuştur. Kayıtlar kontrol edilerek. BGYS, ilgili her yasal ve düzenleyici gereksinimi dikkate alınmıştır. Kayıtlar, okunabilir, hemen tanınabilir ve geri alınabilir şekilde dökümante edilmiştir Kayıtlar, proses performansına ve BGYS ile ilgili tüm güvenlik ihlal olaylarının oluşumlarına ilişkin tutulmaktadır. Ziyaretçi defteri, denetim kayıtları ve tamamlanmış erişim yetkilendirme formları, test kayıtları erişim kayıtları tutulmaktadır

1.10.9. Yönetim Sorumluluğu Genel

1.10.9.1. Yönetimin Sorumluluğu

Kuruluşumuz yönetimi bilgi güvenliği yönetim sisteminin sürekliliğinin sağlanmasının Kuruluş çalışmaları ve bundan sonraki gelişme planları açısından son derece önemli olduğunu kabul ve teyit eder. Kuruluş çalışanlarının bilgi yönetim sistemini uygulama zorunluluğu belirlenmiştir. Kuruluşumuz üst yönetimi yasal ve mevzuat şartları da dahil olmak üzere müşteri şartlarının da yerine getirilmesinin önemini tüm çalışanlarına aktararak gerekli bilincin oluşmasını sağlar. Bilgi yönetim sisteminin tüm yönleri ile ve sürekli gelişme gereği göz önüne alınarak uygulanması gerekmektedir. Kuruluşumuz

üst yönetimi bilgi güvenliği Politikasını oluşturur, bilgi güvenliği sistemimizin uygulanması için gerekli hedefleri belirler ve kuruluş çalışanlarının sorumlulukları arasına alır. Bilgi yönetim sistemi sabırla ve emek ile uygulanmaktadır. Bilgi güvenliği sisteminden beklenilen kurumsallaşma faydası bu çalışma ile sağlanacaktır. Kuruluş yönetimi bilgi güvenliği sistem çalışmaları için gerekli zaman, eğitim, insan, makine ve çalışma çevresi kaynaklarını sağlayacağını taahhüt eder. Bilgi güvenliği kurulu çalışmalarına seçilen başkan kanalı ile ve yönetim sisteminde yer alan (el kitabı, prosedür vb.) dokümanlarda verilen sorumlulukları yerine getirerek bilgi güvenliği yönetim sisteminin geliştirilmesi ve uygulaması kararlılığındadır.

1.10.9.2. Kaynak Yönetimi

Kuruluş kaynak ihtiyacı bölüm müdürleri tarafından belirlenir ve Yönetimin gözden geçirme toplantılarında gündeme alınır. Belirlenen kaynak ihtiyacının karşılanması ve bu amaçla planlar yapılması sorumluluğu bilgi güvenliği komitesindedir ve Kuruluş üst yönetimindedir. Kuruluş insan kaynakları ihtiyaç duyan bölüm yöneticisi tarafından Genel Müdür ile görüşülerek giderilir. Bilgi güvenliği yönetim sisteminin etkin uygulanmasını gerçekleştirmek amacı ile gerekli teknik eğitimi almış personel arasından seçilmesi sağlanır. Ayrıca bilgi güvenliği yönetim sistemini uygulama, sürdürme ve etkinliğinin sürekli iyileştirilmesi için ortaya çıkabilecek kaynak ihtiyaçları belirlenerek üst yönetim tarafından sağlanır.

1.10.10. Eğitim Yeterlilik

Kuruluş personeli bilgi, eğitim ve tecrübelerine göre görevlendirilir. Kuruluş içerisinde uzun süreler çalışmış olan personel zaman içerisinde yönetim ve karar mekanizmalarında yetki sahibi yapılır. Eğitim Talebinin Belirlenmesi Uygun Olmayan hizmetler, İç Tetkikler, Müşteri şikayetleri ve İstekleri, Personel İstek ve Önerileri ile belirlenebilir. Eğitim ihtiyacı varlık sahibi tarafından belirlenir ve Eğitim Talep Formu ile bilgi güvenliği kurulu başkanına' verilir. Belirlenen eğitimler Eğitim Planı'na kaydedilerek Genel Müdür'ün onayına sunulur. Onaylanan Yıllık Eğitim Planı tüm varlık sahiplerine duyurulur. Plan yıl içerisinde gerekirse revize edilir. Plan doğrultusunda Eğitmen, katılımcılar ve eğitim yeri belirlenir. Tüm eğitimlerin sonunda Eğitim Katılım Listesi düzenlenir. Personelin aldıkları eğitimlerin takibi Personel

Eğitim Takip Formu ile takip edilir. Yeni iş başı yapan personele uyum eğitimleri uygulanır.

1.10.11. Bilgi Güvenliği Yönetim Sistemi İç Denetim

BYGS sisteminin uygulamasını ve etkinliğini tespit amacı ile iç denetimleri uygulanır. Her yılbaşında iç kalite denetim planı hazırlanır. İç kalite denetim planları hazırlanırken denetlenecek bölüm, kalite sisteminin tüm elemanları, denetim zamanı ve denetçiler belirlenir.

Denetimlerde BYGS sisteminin standarda uygunluğu ve bütünlüğünün yanı sıra denetimlerin etkinliği de değerlendirilir. Denetimlerde elde edilen sonuçlar ve bulunan uygunsuzluklar kayıt altına alınır. Denetim sonuçları yönetimin BGYS sistemini gözden geçirme toplantılarının gündem maddelerinden birisini oluşturur.

1.10.12. Yönetim Gözden Geçirmesi

1.10.12.1. Genel

Kuruluş üst yönetimi BGYS yönetim sistemin, uygulamanın etkinliğini, hedeflerini, alt yapı isteklerini ve buradaki değişiklikleri ve sürekli gelişme gereğinin yakalanıp yakalanmadığını yılda en az 2 kez yapılacak BGY Sistemini gözden geçirme toplantılarında değerlendirir. Yapılan toplantıların 1 Ocak diğeri de Temmuz ayı içerisinde yapılır. Gözden Geçirme Toplantılarına Genel Müdür, Bilgi Güvenliği Kurulu Üyeleri, Başkanı, ve tüm Varlık sahipleri katılır. BGYS Gözden Geçirme Toplantılarından önce BYG Kurul Başkanı tarafından toplantı gündemi belirlenir ve toplantıya katılacaklara geçen dönemdeki BYG sistem uygulamaları ile ilgili rapor hazırlanarak sunulur. BGY Kurul Başkanı toplantıdan 1 hafta önce toplantı katılımcılarına toplantı detayları ve gündemi ile ilgili bilgi verir.

BGY sistemini gözden geçirme toplantılarının gündemi toplantıdan 1 hafta önce BGK Başkanı tarafından belirlenir ve toplantının diğer katılımcılarına duyurulur. Toplantı gündeminde esas olarak aşağıda belirtilen konular bulunur.

Bir önceki toplantıda alınan kararların takibi

İç denetim sonuçları

Uygulanan düzeltici ve önleyici faaliyet sonuçları şikayetleri

BGYS Politikası

BGYS Hedefleri

Kaynak ihtiyacı ve BGY sisteminin genel durumu

Öneri ve İstekler

Yönetim gözden geçirmesinde alınan kararlar Toplantı Raporuna BGK Başkanı tarafından kaydedilir ve toplantı sonunda bu kayıtları toplantıya katılanlara dağıtır. Alınan kararlar ilgili yöneticiler tarafından uygulama planlarına geçirilir. Bu planlarda uygulama sorumluları, terminler ve gerekli kaynak ihtiyacı belirlenir. Toplantılarda konuşulan her türlü konuyu Toplantı sonucunda alınan kararların uygulanıp uygulanmadığı Yönetim temsilcisi tarafından takip edilir ve bir sonra yapılacak toplantı gündem maddelerinden birisini oluşturur.

1.10.13. Bilgi Güvenliği Yönetim Sistemi İyileştirme Genel

1.10.13.1. Sürekli İyileşme

Uygulanan BGY sistemi sürekli iyileşme mantığı ile kurulmuştur. Sürekli iyileşme hedeflerinin belirlenmesi ve sürekli izlenmesi sonucunda ulaşılacak sonuçlara göre proseslerin iyileştirilmesi sonucunda ortaya sağlanır. BGY hedefleri, tetkik sonuçları, verilerin analizi, düzeltici-önleyici faaliyetler, yönetimin gözden geçirmesi kullanılarak sistem sürekli iyileştirilir.

1.10.13.2. Düzeltici Faaliyet

Bilgi güvenliği yönetim sistemi iç Denetiminde belirlenen uygunsuzluklar Sonucunda düzeltici faaliyet uygulaması yapılır. Düzeltici faaliyet uygulamaları BGK Başkanı tarafından takip edilir ve izlenir. Uygulama etkinlikleri yönetimin BGYS sistemini gözden geçirme toplantılarında değerlendirilir.

1.10.13.3. Önleyici Faaliyet

İç Kalite Denetimleri

Muayene ve Testler

İstatistik analizler

Sonucunda elde edilen veriler ve gelecekte uygunsuzluğa neden olma ihtimali olan konularda önleyici faaliyet uygulaması yapılır. Önleyici faaliyet uygulamaları aynı düzeltici faaliyet uygulaması gibi gerçekleştirilir.

1.11. Bilgi Güvenliği Yönetim Sisteminin İşletmelere Faydaları

Bilgi güvenliği yönetim sistemi kuruluşlarda birçok fayda sağlamaktadır, bu katkıların bazıları aşağıda belirtilmektedir;

Bilgi sistemlerini ve ağlarını; bilgisayar destekli sahtekârlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi kaynaklardan gelen tehdit ve tehlikelerden korur.

Bilginin gizliliğini, güvenilirliğini ve kullanılabilirliğini; rekabet gücünün, karlılığın, yasal yükümlülüklerin ve ticari imajın korunması ve sürdürülmesini sağlar.

Farklı ve değişik ölçekli kurumlara uygulanabilir

Belirli bir Üretici, Ürün veya Servis tavsiye edilmemiştir. Kontrolleri sağlayan her üretici, ürün, servis kullanılabilir.

Kurumlara Yönetsel, Fiziksel ve Teknik geniş bir güvenlik görüşü sunar.

Uluslararası kabul görmüş standarttır.

Güvenlik ve Kalite ile ilgili kanun, düzenleme ve standartlarla uyumludur.

İşin devamlılığını sağlar.

Müşterinin güveni kazanılır.

Rekabet avantajı kazandırır.

Yasal mevzuatlara uyumu garantiler.

Kurumsal yönetim.

Bilgi güvenliğinin geliştirilmiş etkinliği.

Piyasada farklılaşma.

Üst yönetim ve müşteri gereksinimlerinin karşılanması.

Küresel kabul görmüş tek standart.

Sigorta pirimlerinde potansiyel olarak daha düşük oranlar.

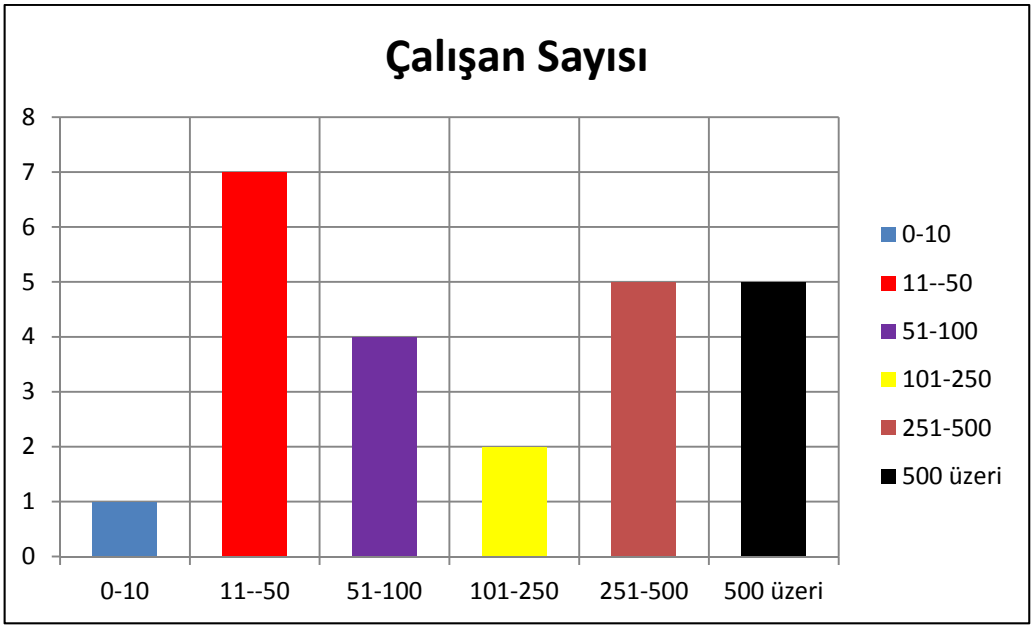
Odaklanmış çalışan sorumlulukları.

BÖLÜM 2: BİLGİ GÜVENLİĞİ YÖNETİMİNİN BAŞARI DAYANAKLARI

Bu bölüm de Türk Standardları Enstitüsünden Bilgi Güvenliği Yönetim Sistemi belgesi alan ve Bilgi Güvenliği Yönetim Standardını uygulayan çalışma içerisinde Ek 1'deki listede belirtilen kuruluşlara uygulanan Bilgi Güvenliği Yönetim Sisteminin gerekleri ve başarı dayanaklarının ölçülmesi üzerine oluşturulan ve çalışmada Ek 2'de verilen anket sonuçlarının değerlendirilmesi yapılmıştır. Anket Türk Standardları Enstitüsünden Bilgi Güvenliği Belgesi bulunan 35 firmaya gönderilmiştir. Ankete 24 firma geri dönüş yapmıştır. Değerlendirme bu sayı üzerinden yapılmıştır.

2.1. Kuruluşların Çalışan Sayısı Analizi

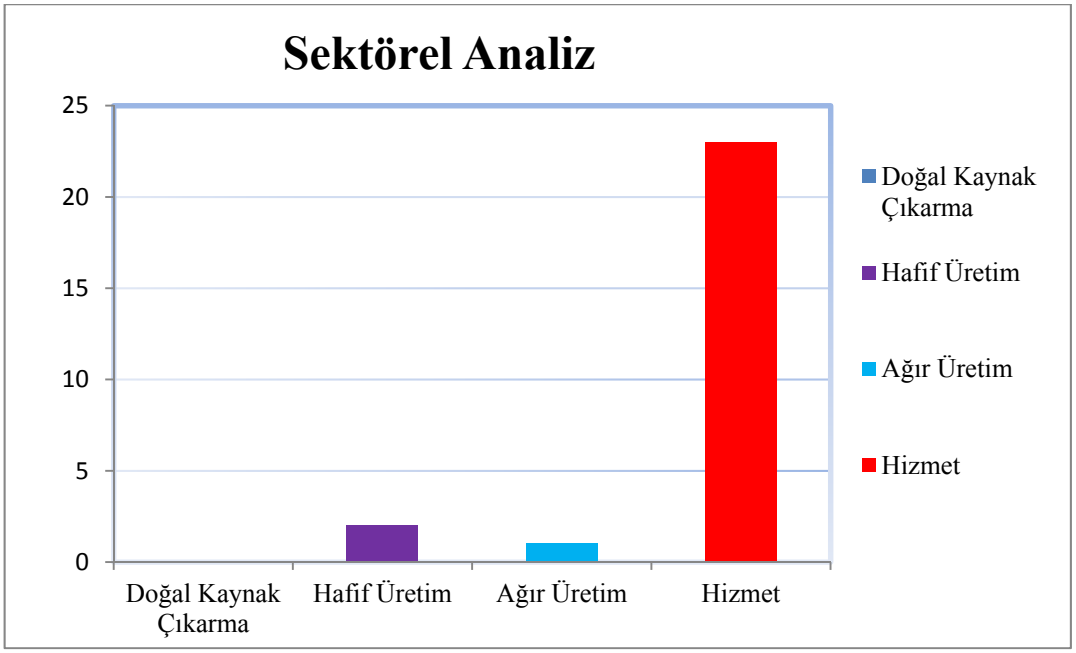
Ankete katılan kuruluşların çalışan sayıları analizi Şekil 4'de detaylandırılmıştır. Şekil 4'de görüleceği üzere Bu sitemi uygulayan kuruluşlar genellikle Mikro ve orta boylu işletmelerdir. Ülkemizin işletme yapıları genellikle mikro ve orta boylu işletmeler olduğu düşünüldüğünde anket sonuçununda bunu desteklediği görünmektedir.



Şekil 4: Kuruluşların Çalışan Sayısı Analizi

2.2. Kuruluşların Sektör Analizi

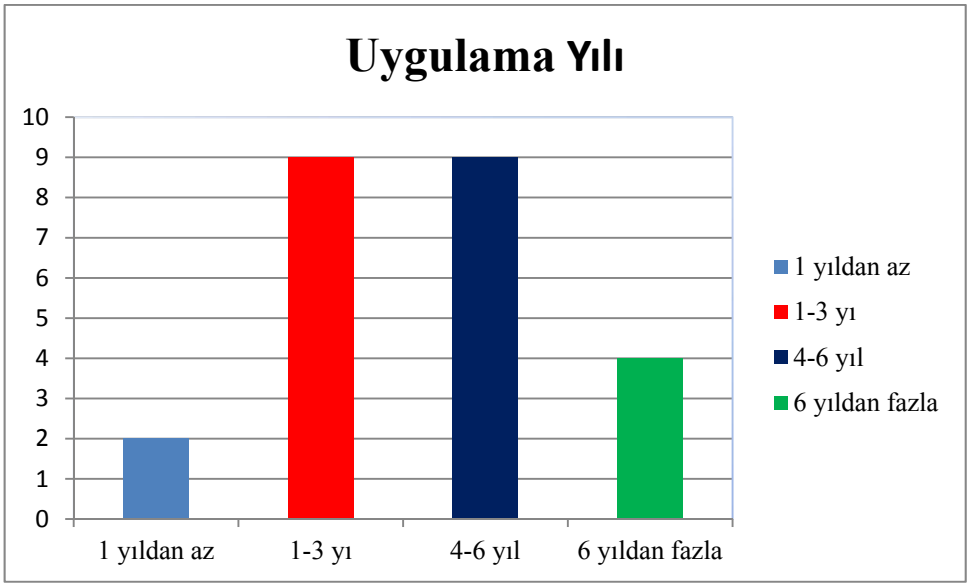
Ankete katılan kuruluşların sektör analizi aşağıda Şekil 5'de verilmiştir. Sistemi uygulayan kuruluşların tamamına yakını hizmet sektöründen yer almaktadır. Bu hizmet sektöründe olan kuruluşların bir tanesi hizmet sektörü ile birlikte ağır üretim diğeri ise hafif üretim yapmaktadır. Bir kuruluş ise hafif üretim sektöründe faaliyet göstermektedir. Bunun nedeni ; Hizmet sektörünün bu sitemi üretim sektörüne göre daha fazla uygulaması hizmet sektörünün üretim sektörüneden daha fazla bilgi işleyen ve bilgiye dayalı faaliyetleri ve süreçleri olması ile açıklanabilir.



Şekil 5: Kuruluşların Sektörel Analizi

2.3. Kuruluşların Bilgi Güvenliği Yönetim Sistemini Uygulama Yılı Analizi

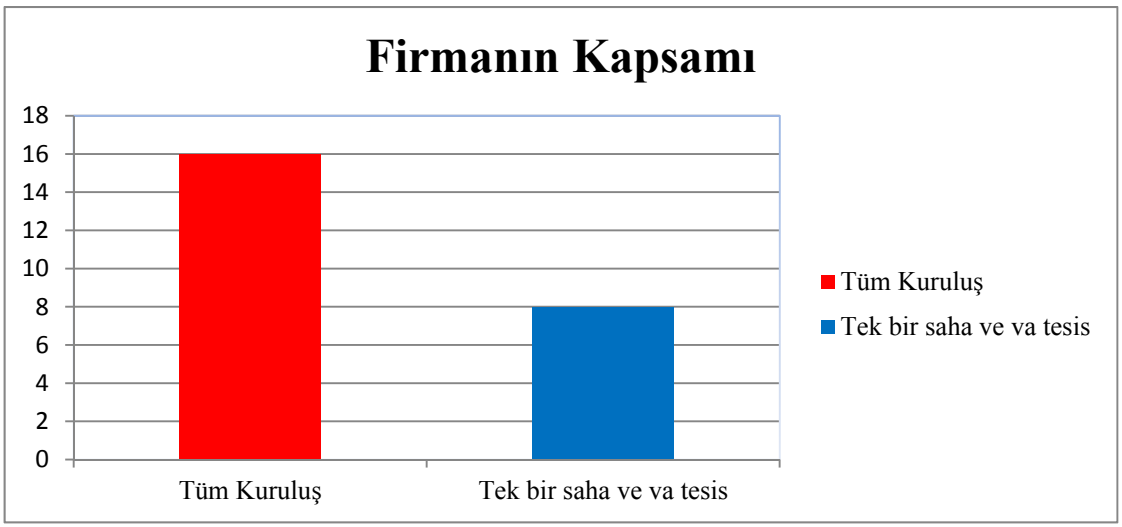
Ankete katılan kuruluşların sistemi uygulama yılı Şekil 6'de verilmiştir. Bilgi güvenliği yönetim sistemi ilk olarak ingiltere 2000'li yıllarda uygulanmaya başlanmıştır. Ülkemizde ise ilk belgelendirme 2005 yılında yapılmıştır. uygulamanın ülkemizde yeni olduğu göz önüne alındığında kuruluşların uygulama yılı açısından önemli adımlar attığından söz edilebilir.



Şekil 6: Kuruluşların Bilgi Güvenliğini Uygulama Yılı Analizi

2.4. Kuruluşların Bilgi Güvenliği Yönetim Sistemi Kapsamı Analizi

Bilgi Güvenliği Yönetim Sistemini uygulayan kuruluşların kapsamı Şekil 7'de belirtilmektedir. Yapılan değerlendirmede çoğu kuruluş bu sistemi tüm faaliyetlerinde uygulandığı sonucuna çıkarmakla birlikte bazı büyük organizasyonların sadece bir biriminde veya bilgi işlem bölümlerinde bu sistemi uyguladıkları belirlenmiştir. Küçük kuruluşların her faaliyetlerinin işletme içerisinde yaptığı, büyük organizasyonların ise faaliyetlerinin parçalayarak birimler bazında yönettiği için bilgi güvenliği ilgili birimler veya bilgi işlem merkezlerinde bu sistemi uygulama yoluna gittikleri görünmektedir.



Şekil 7: Kuruluşların Bilgi Güvenliği Yönetim Sistemi Kapsam Analizi

2.5. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Ürün ve Hizmet Kalitesine Etkisi

Tablo 22 bilgi güvenliği yönetim sisteminin kuruluşlarda ürün ve hizmet kalitesine etkilerinin yüzdelerini belirtmektedir.

Tablo 22: Ürün ve Hizmet Kalitesine Etkisi Analizi

Ürün ve Hizmet Kalitesine Etkisi (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	-	8.33	58.33	29.16

Tablo 22 detaylı bir şekilde incelendiğinde; katılımcıların tamamının bu sistemin ürün ve hizmet kalitesine değer sağladığını belirtmektedir. Katılımcıların % 58.33'ü bu sistemin firmalarının ürün ve hizmet kalitelerine yüksek değer sağladığını, % 29.16'nın çok yüksek değer sağladığını, % 8.33'ünde orta değer sağladığını ifade etmektedir. Bu verilerle dayanarak bilgi güvenliği yönetim sisteminin kuruluşlarda ürün ve hizmet kalitesinin arttırdığına ilişkin güçlü bir kanaatin olduğu sonuçuna varılmıştır.

2.6. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Paydaş İhtiyaçlarının Karşılanması Analizi

Tablo 23 Bilgi güvenliği yönetim sisteminin kuruluşlarda paydaş ihtiyaçlarının karşılama yüzdelerini belirtmektedir.

Tablo 23: Paydaş İhtiyaçlarının Karşılaması Analizi

Paydaş İhtiyaçlarının Karşılaması (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	-	25	50	20.83

Tablo 23 incelendiğinde; Bilgi güvenliği yönetim sisteminin paydaş ihtiyaçlarını karşılamasında da kuruluşlara katkı sağladığı görünmektedir. Orta değer sağlayanların oranı % 25'dir. Yüksek değer sağlayanlar % 50, çok yüksek değer sağlayanların oranı ise % 20.83'dür. Bu soruya 1 kuruluşu da bu sistemi paydaş ihtiyaçlarını karşılaması ile

ilişkilendirememiştir bu oranda % 4.16'ya tekabül etmekte olup ilgili kuruluşun kamu sektöründe yer aldığı görünmektedir.

2.7. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Stratejik Hedeflere Ulaşma Analizi

Tablo 24 Bilgi güvenliği yönetim sisteminin kuruluşlarda stratejik hedeflere ulaşma yüzdelerini belirtmektedir.

Tablo 24: Stratejik Hedeflere Ulaşma Analizi

Stratejik Hedeflere Ulaşma (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	4.16	4.16	62.25	25

Tablo 24 incelendiğinde; Bilgi Güvenliği Yönetim Sisteminin kuruluşlarda stratejik hedeflere ulaşmasında % 4.16 oranında düşük değer, % 4.16 oranında orta değer, % 62.25 oranında yüksek değer ve % 25 oranında çok yüksek değer sonucuna varılmıştır. Çalışmaya katılan bir kuruluş ise, bu sistemi stratejik hedeflere ulaşma ile ilişkilendirememiştir. Ortaya çıkan verilerle bu sistemin kuruluşların stratejik hedeflere ulaşmasında büyük katkı sağladığı sonucunu işaret etmektedir.

2.8. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Rekabet Avantajı Sağlama Analizi

Tablo 25 Bilgi güvenliği yönetim sisteminin kuruluşlarda rekabet avantajı sağlama yüzdelerini belirtmektedir.

Tablo 25: Rekabet Avantajı Sağlama Analizi

Rekabet Avantajı Sağlama (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	8.33	25	25	29.16

Tablo 25 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşlara rekabet avantajı sağlamada % 8.33'ü düşük değer, % 25'i orta değer, % 25'i yüksek değer, % 29.16'sı ise çok yüksek değer sağladığını belirtmektedir. Çalışmaya katılan üç kuruluş

ise bu sistemi rekabet avantajı sağlama ile ilişkilendirmemiştir. Bu oran ise % 12.5'dir. Ortaya çıkan verilerle bu sistemin kuruluşlarda rekabet etme özelliğini arttırdığına ilişkin güçlü bir algı oluştuğu sonucuna varılmıştır.

2.9. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Genel İmajı İyileştirme Analizi

Tablo 26 Bilgi güvenliği yönetim sisteminin kuruluşlarda genel imajının iyleştirmesine olan etkisi yüzdelerini belirtmektedir.

Tablo 26: Genel İmajı İyileştirme Analizi

Genel İmajı İyileştirme (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	-	4.16	54.16	41.66

Tablo 26 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun genel imajını iyileştirmesinde % 4.16'sının orta değer, % 54.16'sının yüksek değer ve % 41.66'sının çok yüksek değer sağladığını ifade etmektedir. Bu verilere göre bilgi güvenliği yönetim sistemi kuruluşların genel imajının artmasına büyük katkı sağladığına ilişkin izlenimden söz edilebilir.

2.10. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin İş Yönetim Sistemleri ile Entegrasyon Sağlama Analizi

Tablo 27 Bilgi güvenliği yönetim sisteminin kuruluşlarda iş yönetim sistemleri ile entegrasyon sağlama yüzdelerini belirtmektedir.

Tablo 27: İş Yönetim Sistemleri ile Entegrasyon Sağlama Analizi

İş Yönetim Sistemlerine Entegrasyon (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	4.16	16.16	66.66	12.5

Tablo 27 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşlarda iş yönetim sistemleri ile entegrasyonunda % 4.16'sı düşük değer, % 16.16'sı orta değer, % 66.66'sı yüksek değer ve % 12.5'i ise çok yüksek değer elde etmiştir. Bu veriler bilgi

güvenliği yönetim sisteminin kuruluşların iş sistemleri ile entegre olmasında bir sakınca olmadığını bu sistemlerle birlikte yürütülebileceği görünmektedir.

2.11. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Finansal Fayda Sağlama Analizi

Tablo 28 Bilgi güvenliği yönetim sisteminin kuruluşlarda finansal fayda sağlama yüzdelerinin belirtmektedir.

Tablo 28: Finansal Fayda Sağlama Analizi

Finansal Fayda Sağlama (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	20.83	29.16	33.33	4.16

Tablo 28 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşlara finansal değer sağlamada % 20.83'ü düşük değer, % 29.16'sı orta değer, % 33.33'ü yüksek değer ve % 4.16'sı ile çok yüksek değer sağladığını belirtmektedir. Çalışmaya katılan bir kuruluş bu sistemin işletmelerine finansal fayda sağlamadığını belirtmiştir. Bu oran % 4.16'dır. İki kuruluş ise bu sistemi finansal fayda sağlama ile ilişkilendirememiş olup bunun oranı ise % 8.33'dür. Ortaya çıkan değerler sonucunda bilgi güvenliğinin kuruluşlara finansal fayda sağlama oranını çok yüksek olmadığı söylenebilir.

2.12. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Teknolojik Gelişime Katkı Sağlama Analizi

Tablo 29 Bilgi güvenliği yönetim sisteminin kuruluşlarda teknolojij gelişime katkı sağlama yüzdelerini belirtmektedir.

Tablo 29: Teknolojik Gelişime Katkı Sağlama Analizi

Teknolojik Gelişime Katkı (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	4.16	16.66	45.83	33.33

Tablo 29 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşların teknolojik gelişimine % 4.16 düşük değer, % 16.16 orta değer, % 45.83'ün yüksek değer ve % 33.33'ün ise çok yüksek değer sağladığı belirtilmektedir. Bilgi güvenliğin yönetim

sisteminin teknolojik bir boyutunun da olması ve kuruluşları son teknoloji kullanmaya yönlendirmesi nedeniyle bu sistemi uygulayan kuruluşların teknolojik gelişimini pozitif yönde etkilediği kanaati belirgin olarak görünmektedir.

2.13. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin İnsan Kaynakları Gelişimine Katkısı Analizi

Tablo 30 Bilgi güvenliği yönetim sisteminin kuruluşlarda insan kaynaklarının gelişimine olan katkısını belirtmektedir.

Tablo 30: İnsan Kaynakları Gelişimine Katkı Analizi

İnsan Kaynakları Gelişimi (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	4.16	20.83	45.83	29.16

Tablo 30 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun insan kaynaklarının gelişimine etkisinin % 4.16'sının düşük değer, % 20.83'ün orta değer, % 45.83'ün yüksek değer ve % 29.16'sının çok yüksek değer sağladığı görünmektedir. Bilgi güvenliği yönetim sistemi tamamen çalışan odaklı yürümektedir. Çalışan personelin sürekli eğitimlerle bilgilendirilmesi insan kaynaklarının kalitesini arttırmaktadır.

2.14. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Çalışanların Bilgi Güvenliği Yönetimine Katılımı Analizi

Tablo 31 Bilgi güvenliği yönetim sisteminin kuruluşlarda çalışanların bilgi güvenliği yönetimine katılımına olan katkısını belirtmektedir.

Tablo 31: Çalışanların Bilgi Güvenliği Yönetimine Katılımı Analizi

Çalışanların Bilgi Güvenliği Yönetimine Katılımı (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	4.16	12.5	45.83	37.5

Tablo 31 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşta uygulamasına çalışanların katılımı % 4.16 ile düşük değer, % 12.5 ile orta değer, % 45.83 ile yüksek değer ve % 37.5 ile de çok yüksek değer elde edilmiştir. Sistemi uygulayan kuruluşlarda bir farkındalık oluştuğu ve çalışanların bu sistemi katkı ve katılım sağladığı ile ilgili güçlü bir sonuç algı söz konusudur.

2.15. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Kuruluşa Özel Bilgilerin Korunması Analizi

Tablo 32 Bilgi güvenliği yönetim sisteminin kuruluşlarda özel bilgilerinin korunmasına olan katkısını belirtmektedir.

Tablo 32: Özel Bilgilerin Korunması Analizi

Özel Bilgilerin Korunması (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	-	4.16	33.33	62.5

Tablo 32 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun özel bilgilerinin korunmasına % 4.16 ile düşük değer, % 33.33 ile yüksek değer ve % 62.5 ile çok yüksek değer sağladığı görünmektedir. Bilgi güvenliği yönetim sisteminin ana amacının bu olgu olduğu kuruluşların özel bilgilerin korunmasına çok yüksek bir değer sağladığı ve bu yönde güçlü bir algı net bir şekilde görünmektedir.

2.16. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Paydaşlar ile İletişim ve Paydaş Memnuniyeti Analizi

Tablo 33 Bilgi güvenliği yönetim sisteminin kuruluşlarda paydaşlar ile iletişim ve paydaş memumiyetine olan katkısını belirtmektedir.

Tablo 33: Paydaşlar ile İletişim ve Paydaş Memnuniyeti Analizi

Paydaşlar ile İletişim ve Paydaş Memnuniyeti (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	4.16	12.5	58.33	16.66

Tablo 33 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun Paydaş ile iletişim ve paydaş memuniyetine % 4.16 ile düşük değer, % 12.5 ile 0rta değer, % 58.33 ile yüksek değer ve % 16.66 ile çok yüksek değer sağlamıştır. Çalışmaya katılan Bir kuruluş bu sistemi Paydaş ile iletişim ve paydaş memuniyeti ile ilişkilendirememiştir. Bu ilişkilendirilmeyen oran % 8.33'dür. Bu bilgiler ışığında sistemin paydaşlar tarafından kabul gördüğü sonucuna varılabilir.

2.17. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Yasal Şartları Yerine Getirme Yeteneği Analizi

Tablo 34 Bilgi güvenliği yönetim sisteminin kuruluşlarda yasal şartları yerine getirme yeteneğine olan katkısını belirtmektedir.

Tablo 34: Yasal Şartları Yerine Getirme Yeteneği Analizi

Yasal Şartları Yerine Getirme (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	-	-	50	50

Tablo 34 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun yasal şartları yerine getirme yeteneğine % 50 yüksek değer ve % 50 çok yüksek değer katkı sağladığı anlaşılmaktadır. Bilgi güvenliği yönetim sisteminin içerisinde belirtilen yasal şartlara yerine getirme maddesi kuruluşların yasal şartlara en kısa sürede adepte olmalarını sağlamaktadır. Bu nedenle kuruluşların yasal şartlara uyumu yetenek üste seviyelerdedir.

2.18. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Kuruluşun Bilgi Güvenliği Yönetimi Performansının İyileşmesi Analizi

Tablo 35 Bilgi güvenliği yönetim sisteminin kuruluşlarda bilgi güvenliği yönetimi performansının iyleştirmesine olan etkisini belirtmektedir.

Tablo 35: Bilgi Güvenliği Yönetimi Performansının İyileşmesi Analizi

Kuruluşun Bilgi Güvenliği Yönetimi Performansının İyileşmesi (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	-	8.33	25	66.66

Tablo 35 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun bilgi güvenliği performansının arttırmasına % 8.33 orta değer, % 25 yüksek değer ve % 66.66 çok yüksek değer sağlamıştır. Bu veriler sistemin bilgi güvenliği performansını yükselttiğini göstermektedir.

2.19. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Tedarikçilerin Bilgi Güvenliği Yönetimi Performansında İyileştirme Analizi

Tablo 36 Bilgi güvenliği yönetim sisteminin kuruluşlarda tedarikçilerin bilgi güvenliği yönetimi performansının iyleşmesine olan etkisini belirtmektedir.

Tablo 36: Tedarikçilerin Bilgi Güvenliği Performansında İyileştirme Analizi

Tedarikçilerin Bilgi Ğüvenliği Performansında iyleştirme (N=24)	Düşük Değer (%)	Orta Değer (%)	Yüksek Değer (%)	Çok Yüksek Değer (%)
	12.5	29.16	33.33	20.83

Tablo 36 incelendiğinde; Bilgi güvenliği yönetim sisteminin kuruluşun Tederikçilerinin performansının arttırmasına % 12.5 düşük değer, % 29.16 orta değer, % 33.33 yüksek değer ve % 20.33 çok yüksek değer sağlamıştır. Çalışmaya katılan bir kuruluş bu sistemi tedarikçilerin bilgi güvenliği performansının iyleştirmesi ile ilişkilendirememiştir. Bu oran da % 4.16'dır. Bu veriler ışığında tedarikçilerinde sistemi uygulayan kuruluşları örnek aldığı ve bilgi güvenliği yönetim sistemi performanslarının arttığı sonucuna varabiliriz.

2.20. Kuruluşların Bilgi Güvenliği Yönetim Sistemini Uygulanma Nedenleri Analizi

Kuruluşların bilgi güvenliği yönetim sistemi uygulamasının nedenlerinin sorgulandığı bu sorunun sonuçunda aşağıdaki bulgulara ulaşılmış olup bu bulgular Tablo 37'de görüleceği üzere önem sırasına göre üzere sıralanmıştır.

Tablo 37: Bilgi Güvenliği Yönetim Sistemin Uygulanması Nedenleri Analizi

1	Bilgilerin Korunması ve Muhafaza Taahhüdü
2	Olumsuz Bilgi Güvenliği İhlali Riskin Azaltılması
3	Genel imaj
4	Devlet/Düzenleyici Kuruluş Şartı
5	Kuruluşun Uyguladığı Diğer Yönetim Sistemleri İle Entegrasyon Fırsatı
6	Müşteri Şartı
7	Maliyet Azaltma/Finansal Fayda

2.21. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Başarısını Düşüren Faktörlerin Analizi

Kuruluşların bilgi güvenliği yönetim sisteminin başarısını düşüren faktörlerin sorgulandığı bu sorunun sonuçunda aşağıdaki bulgulara ulaşılmıştır. Sonuçlar önem sırasına gore Tablo 38'de sıralanmıştır.

Tablo 38: Bilgi Güvenliği Yönetim Sistemin Başarısını Düşüren Faktörlerin Analizi

1	Çalışanların Katılımının Eksikliği
2	Üst Yönetimin Desteğinin Yetersizliği
3	Çalışanların Eğitim ve Bilinç Eksikliği
4	Dokümantasyon Sistemini Eksikliği
5	Teknolojik Eksiklik
6	Finansal Desteğin Yetersizliği
7	Müşteri Beklentilerinin Karşılanamaması

2.22. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Başarısını Yükselten Faktörlerin Analizi

Kuruluşların bilgi güvenliği yönetim sisteminin başarısını yükselten faktörlerin sorgulandığı bu sorunun sonuçunda aşağıdaki bulgulara ulaşılmıştır. Sonuçlar önem sırasına göre Tablo 39'da sıralanmıştır.

Tablo 39: Bilgi Güvenliği Yönetim Sistemin Başarısını Yükselten Faktörlerin Analizi

1	Üst Yönetimin Desteği
2	Çalışanların Katılımı
3	Çalışanların Yeterliliği ve Bilinci
4	Uygun Dokümantasyon Sistemini
5	Son Teknoloji Uygulanması
6	Finansal Destek
7	Müşteri Beklentilerinin Karşılanması

2.23. Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Kritik Başarı Faktörlerin Analizi

Kuruluşların bilgi güvenliği yönetim sisteminin kritik başarı faktörlerinin sorgulandığı bu sorunun sonuçunda aşağıdaki bulgulara ulaşılmıştır. Sonuçlar önem sırasına göre Tablo 40'de sıralanmıştır.

Tablo 40: Bilgi Güvenliği Yönetim Sisteminin Kritik Başarı Faktörlerin Analizi

1	Bilgi Güvenliği Yönetim Sistemine Üst Yönetimin Tam Desteği
2	Bilgi Güvenliği Yönetim Sisteminin Stratejik Hedeflerle Uyumu
3	Bilgi Güvenliği Yönetim Sisteminin Kuruluşun Misyon/Vizyonuna Uyumu
4	Bilgi Güvenliği Yönetim Sisteminin Kuruluşun Politikasını Karşılaması
5	Bilgi Güvenliği Yönetim Sisteminin Kurum Kültürü ile Tutarlı Olması
6	Ektin Bir Şekilde Oluşturulan Risk Değerlendirmeleri
7	Bilgi Güvenliği Yönetim Sisteminin Kaynak İhtiyacının karşılanması

2.24. Genel Değerlendirme

Dünyada artık bilgi gerçeği vardır. Özellikle iş dünyasında bilgi daha büyük önem kazanmıştır. Kuruluşlar bilgi tabanlı işletmeler haline dönüşmektedir. Bilgi tabanlı işletmelerde bilginin saklanması, korunması ve istenmeyen kişilerin eline geçmesi büyük sorunlara neden olmaktadır. Özel bilginin saklanması ve korunması sistematik ve sürdürülebilir yöntemler ile yapılmalıdır. Kuruluşların bilgi güvenliğine ilişkin; tehdit ve risklerden haberdar olması ve bu tehditlere ve risklere nasıl karşı koyabileceği konusunda hızlı adımlar atmaları gerekmektedir. Bu çalışmaya katılan ve sistematik bir şekilde bilgilerini uluslararası bir standard olan Bilgi Güvenliği Yönetim Standardı (TSISO/IEC 27001) uygulayarak korumaya çalışan kuruluşların fikirleri ve tecrübeleri değerlendirilmiştir. Bilgi güvenliği yönetim sistemi uygulayan kuruluşların genellikle küçük ve orta boylu işletmeler olduğu, tamamına yakınının hizmet sektöründe faaliyet gösterdiği büyük çoğunluğunun kuruluşa özel bilgilerini korumak, olumsuz riskleri kontrol altına almak ve genel imajlarını arttırmak için bu sistemi tercih ettiği görünmektedir. Bilgi Güvenliği Yönetim Sisteminin işletmenin Süreçlerine etkisi, Teknolojik gelişme etkisi ve İnsan kaynaklara etkisi olarak üç ana başlık halinde değerlendirilecek olursak;

A) İş süreçlerine;

Bilgi güvenliği yönetim sistemi İş süreçlerini olumlu katkılar sağladığı ürün ve hizmet kalitesini arttırdığı, kuruluşlara rekabet avantajı sağladığı, finansal fayda sağladığı, kuruluşun genel imajını yükselttiği, stratejik hedeflere ulaşmada ve diğer iş sistemleri ile entegrasyonunda başarılı olduğu sonucuna varılmaktadır.

B) Teknoloji Gelişimine;

Bilgi güvenliği yönetim sistemi kuruluşların teknolojisinin gelişmesine büyük katkı sağladığı özellikle bilgi işleyen kuruluşların son teknolojiyi kullandığını ve gelişen bu teknolojinin ürün ve hizmet kalitesini arttırdığı bunlarla birlikte müşteri ve paydaş ilişkilerinin de yükseldiği görünmektedir.

C) İnsan Kaynakları Gelişimine;

Bilgi güvenliği yönetim sistemi kuruluşlarda çalışan personelin gelişimine katkı sağladığı, sisteme katılma ve çalışan memnuniyetini arttırdığı görünmektedir.

Bilgi güvenliği yönetim sistemi uygulayan kuruluşların yasal şartları yerine getirmede daha hızlı hareket ettiği ve bilgilerinin en üst seviyede korunduğu sonucu çıkmaktadır.

Bilgi güvenliği yönetiminin kurumlarda başarılı olabilmesi için; üst yönetimin bilgi güvenliği ve buna bağlı süreçlerine maddi ve manevi destek vermesi, bu sisteme inanması ve tüm çalışanların benimsemesi gerekmektedir. Kurum içerisinde bilgi güvenliğinin sadece teknoloji veya bilgisayar güvenliği olmadığı bunun bir yönetim modeli olduğu süreçleri, görev tanımları ve iş akışları ile yönetilmesi gerektiği bilinmelidir. Bilgi güvenliği, kurumun ticari stratejileri ve iş geliştirme vizyonu kadar önemli ve belirleyici bir yerde konumlanmalı, bir kurum kültürü haline getirilmelidir.

Bilgi güvenliğin diğer kritik başarı faktörü de kurumlarda çalışanlardır. Başarılı ve uzun soluklu bir bilgi güvenliği; çalışanların bilgi güvenliği konusunda eğitimler almaları ile olabilecektir.

SONUÇ ve ÖNERİLER

Dünyada ve ülkenizde sık sık örneklerini gördüğümüz bilgi güvenliği ihlali olayları bu olaylara maruz kalan kuruluşları telafisi zor maddi ve manevi sıkıntılara sokmuştur. Ülkenizde yeteri kadar önem verilmeyen, yeni bir olgu olan ve sürekli öneminin arttığı Bilgi Güvenliği gerçeği vardır. Bilgi Güvenliğini her kuruluş kendine özgü yöntemleri ile sağlanmaya çalışılmasından dolayı süreç sağlıksız bir şekilde yürümektedir. Özellikle E-devlet çalışmalarının kamu ve kurumsallaşmış özel sektörü bu konuda diğer kuruluşlardan daha ileride olduğunu göstermektedir. Kurumsallaşmamış ve Küçük Orta Boylu işletmelerde ciddi sıkıntılar mevcuttur. Kuruluşların kendilerine özgü oluşturdukları ve özel bilgilerini korumaya çalıştıkları bu yöntemlerin sürdürülebilirliği maalesef yoktur. Bilgi Güvenliğinin bir sistem dahilinde oluşturulması, bu sistem sayesinde bilgilerin korunması ve bunun sürdürülebilir hale dönüştürülmesi gerekmektedir. Bunun en kolay yolu uluslararası geçerliliği olan TS ISO EN 27001 Bilgi Güvenliği Yönetim Sistemi standardını uygulamaktır. Kuruluşların Prosedürleri, talimatları, politikaları ve risk yönetimleri olan bir sistemi kurmaları halinde kendilerine özgü bilgilerin korunmasını sağlarlar. Uyguladıkları bu sistemim belgelendirilmesi ile kuruluşlarının marka ve imaj değerlerini arttırırlar.

Teknik imkânlarla gerçekleştirilen bilgi güvenliği sınırlıdır. Bu sebeple personeli, politikaları, süreçleri, prosedürleri olan bir sistem kurulmalıdır. Kurumlar, birlikte iş yaptıkları taraflara karşı kendi üstlerine düşen sorumlulukları yerine getirerek, ortak asgari düzeyde bir bilgi güvenliğini sağladıklarını ispat etmek ihtiyacı duymaktadırlar. Tüm bu nedenlerden dolayı işletmeler teknik önlemlerin haricinde idari olarak da bir sistem oluşturmalıdır. Bu idari sistemi de uluslararası bir Standart olan TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile yapılabilir.

Bilgi güvenliğinin teknolojik boyutu olmakla birlikte sadece teknik bir konu değildir. Bilgi güvenliğinin sağlanmasında bireylerin, kurumların ve ülkelerin yapması gereken çok büyük işler vardır. Teknolojinin sürekli geliştiği küreselleşen dünyada kurulan sistemlerin yüzde yüz güvenli olduğunu söylemek doğru bir yaklaşım olmayacaktır. Bu konuda her şey insan ile başlayıp İnsan'da bitmektedir. Bilginin üretimi, iletimi, paylaşımı, saklanması ve kullanımı sürecinin en önemli unsuru ve en zayıf halkası yine

insandır. Bilinçli ya da bilinçsiz yapılan her türlü ihlallerin baş aktörleri insanlardır. Bu nedenle bilgi güvenliği yönetim sistemini dahilinde bulunan her seviyedeki insanların, kurumların, örgütlerin risk ve tehditler konusunda bilgilendirilmesi ve bilinçlendirilmesi gerekmektedir. Bu bilgilendirme ve bilinçlendirme sürekli canlı ve aktif tutulmalıdır. Kurumsal ve ulusal seviyelerdeki bilgi güvenliği riskleri analiz edilmeli ve gerekli önlemler alınmalıdır.

KAYNAKÇA

Kitaplar;

ÇOBAN, Hasan(1996), 'Bilgi toplumuna Planlı Geçiş', T.C Devlet planlama Teşkilatı, Ankara, s.123.

DAVENPORT, T. ve L. PRUSAK(2001), 'İş Dünyasında Bilgi Yönetimi', Rota Yayın, İstanbul.

Devlet Planlama Teşkilatı Müsteşarlığı, (2005) "E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları", DPT, KYR-22, Ankara, s.27.

DİNÇER, Önel ve DİNÇKAN, Ali(2007), TUBİTAK-UEKAE Bilgi Güvenliği Yönetim Sistemi Kurulumu Kılavuzu, s.7.

ERSOY, Eren Veysel (2012), 'ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar', ODTÜ Yayıncılık, Ankara, s.9.

KAPTAN, S. (1973). "Bilimsel Araştırma Teknikleri, Tez Hazırlama Yolları", Ayyıldız Matbaası, Ankara, s.235

KARASAR, N. (2003). "Bilimsel Araştırma Yöntemi", Nobel Yayın Dağıtım, Ankara, s.174

KOÇ, Fatih(2008), TUBİTAK-UEKAE, Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu, s.6 .

KOÇ, Net(2005), 'Türkiye Internet Güvenliği Araştırma Sonuçları,' Rizikometre, İstanbul.

KOÇEL, Tamer (2007), 'İşletme Yöneticiliği',7. Baskı, Beta Yayınları, İstanbul, s.13.

ÖZCAN, Kerim ve BARCA, Mehmet (2008), 'Sanayiden Bilgiye Toplum Ekonomi ve İşletmeler', 1 Baskı Siyasal Yayın Dağıtım, Ankara, s.149.

YILDIRIM, Mehmet Cemal (2000), 'Soru ve Yanıtlarıyla ISO 9000:2000', Rota Yayın, İstanbul, s.17.

Dergiler;

AĞAOĞLU, Metin ve GÖKŞEN, Yılmaz(2009), 'Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri,' *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* s 4, ss 7.

BHATT, Ganesh, (2001) 'Knowledge Management in Organizations: Examining the Interaction Betwwe Technologies, Technigues, and People', *Journal of Knowledge Management,* s.1. ss. 68-75.

DEMİRCAN ÇAKAR, Nigar ve YILMAZ, Sibel(2010), 'Bilgi Yönetimi ve Örgütsel Etkinlik İlişkisi: Örgüt Kültürü ve Örgüt Yapısının Temel Etkileri,' *Ege Akademik Bakış*, s. 10(1), s.77.

DOĞAN, Selen ve KILIÇ, Selçuk(2009), 'Bilgi Yönetiminde Liderliğin Rolü Üzerine Kavramsal Bir İnceleme' *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, s.2, ss.90-91.

ERGÜL, Ali E, ve KESKİN, Halit(2003), 'Sosyal Bir Etkileşim Süreci Olarak Bilgi Yönetimi ve Bilgi Yönetimi Süreci', *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, s.1, ss.176-177.

MARTİN, Vedat ve PEHLİVANLI İhsan (2009), 'ISO 27001:2005 Bilgi Güvenliği Yönetim Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları üzerine Bir İnceleme' *Mühendislik Bilimleri ve Tasarım Dergisi,* s.1. ss.52.

ÖZKAN, Mehmet(2010), 'Neden Bilgi Güvenliği', *Standard Ekonomik ve Teknik Dergisi,* s.579, ss.71.

TEKERLEK, Mehmet(2008), 'Bilgi Güvenliği Yönetimi,' *KSÜ Fen ve Mühendislik Dergisi,* s.11 (1), s.132.

Türk Standardları Enstitüsü (2013) ,Bilgi Güvenliği Yönetim Sistemi TS ISO/IEC 27001 Eğitim Notu, s. 14.

YILMAZ, Malik (2009), 'Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi,' Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi s.49, ss.100-110.

Tezler;

AYDOĞMUŞ, Emel, (2010), *Assessment of Information Security Maturity Levels And ISO/IEC 27001:2005 Compliance of Organizations In Turkey*, Basılmış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi fen Bilimleri Enstitüsü, İstanbul, s.105.

BİNGÖL, Ufuk (2010), *ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu*, Basılmış Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya, s.13.

ÇETİNKAYA, Mehtap (2008), *Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi,* Basılmış Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, s.16.

ERKAN, Ahmet (2006), *An Automated Tool For Information Security Management System*, Basılmış Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi Fen Bilimleri Enstitüsü, Ankara, s.110.

KAHRAMAN, Sunay (2006), *Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi Ve Aselsan A.Ş.'De Uygulaması*, Basılmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir, s.28.

KANDEMİRLİ, Bahadır Murat(2012), *Bilgi Teknolojileri Güvenliği ve Sigorta Şirketlerinde ISO/IEC 27001 Standardları Çerçevesinde Bilgi Güvenlik Yönetim Sistemi Uygulaması*, Basılmış Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, s.95.

METE, Hakan *(2010), ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminin Bilgi İşlem Merkezlerinde Uygulaması,* Basılmış Yüksek Lisans Tezi, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sakarya, s.37.

YILDIZ, Bünyamin (2012), *Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetim Standardlarının Uygulanması*, Basılmış Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü, Gebze, s.80.

YILMAZ, Vural (2007), *Kurumsal Bilgi Güvenliği ve sızma (penetrasyon) testleri,* Basılmış Yüksek Lisans Tezi*,* Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, s. 18.

Standartlar;

TS EN ISO 27799 (2009), Sağlık bilişim - Sağlık Bilgi güvenliği yönetimi kullanarak ISO / IEC 27002", Türk Standardları Enstitüsü, Ankara.

TS EN ISO 9000 (2004), "Kalite Yönetim Sistemleri- Temel Esasları ve Terimler ve Tarifler", Türk Standardları Enstitüsü, Ankara.

TS ISO IEC 17799 (2006), "Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri", Türk Standardları Enstitüsü, Ankara.

TS ISO IEC 27001(2006), "Bilgi Teknolojisi – Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimleri", Türk Standardları Enstitüsü, Ankara.

TS ISO/IEC 27000 (2012), "Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Genel bakış ve sözlük," Türk Standardları Enstitüsü, Ankara.

TS ISO/IEC 27006 (2010), "Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemlerinin denetimini ve belgelendirmesini yapan kuruluşlar için gereksinimler," Türk Standardları Enstitüsü, Ankara.

TS ISO/IEC 27011 (2011), "Bilgi teknolojisi – Güvenlik teknikleri – Bilgi güvenliği yönetim sistemleri – Telekomünikasyon kuruluşları için ISO/IEC 27002 standardını temel alan bilgi güvenliği yönetimi kılavuzu," Türk Standardları Enstitüsü, Ankara.

TS ISO/IEC TR 18044 (2007), "Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği ihlal olayı yönetimi," Türk Standardları Enstitüsü, Ankara.

TSE GUIDE 13268-1 (2007), "TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) belgelendirmesi için gereksinimler ve hazırlık kılavuzu", Türk Standardları Enstitüsü, Ankara.

TSE GUIDE 13268-2 (2007), "TSE GUIDE 13268-2, , TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) gerçekleştirmelerinin etkinliğinin ölçülmesi kılavuzu ",Türk Standardları Enstitüsü, Ankara.

TSE GUIDE 13268-3 (2007),"TS ISO/IEC 27001'e göre Bilgi Güvenliği Yönetim Sistemi (BGYS) denetimine hazırlık kılavuzu," Türk Standardları Enstitüsü, Ankara.

TSE GUIDE 13268-4 (2009), "TS ISO/IEC 27001'i esas alan bilgi güvenliği yönetim sistemi (BGYS) kontrollerinin gerçekleştirilmesi ve denetlenmesi kılavuzu," Türk Standardları Enstitüsü, Ankara.

Gazeteler;

RESMİ GAZETE (2010), "*Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ*", R.G. tarihi: 15.10.2010 ve sayısı: 27730.

İnternet Adresleri;

http://www.iso-belgesi.info

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.507d599d6c0821.29816596

http://www.tse.org.tr/eoq2010/54.EOQCongressPresentations/1.%20Bilgi%20Teknolojileri%20Fonksiyonel%20Performans%20Yonetim%20Sistemi%20ve%20Surec%20iyilestirmeye%20Katkisi-Dr.Ali%20Ozkaya.pdf.

http://www.tse.org.tr/tse-hakkinda/kurulus-ve-gorevleri

http://www.turkak.org.tr/online/search/akredite.asp?action=searc

https://intweb.tse.org.tr/TSEIntWeb/Standard/Standard/StandardAra.aspx

https://www.cen.eu/cen/pages/default.aspx

http://www.cagataycebi.com/security/bilgi_guvenligi.pdf

http://www.bilgimikoruyorum.org.tr/?b111_bilgi-guvenligi-neden-bu-kadar-onemli

http://www.habervitrini.com/haber/1-milyon-kisinin-banka-sifreleri-hackerlerin-elinde-261976/

http://www.turkhukuksitesi.com/showthread.php?t=52705

http://www.radikal.com.tr/haber.php?haberno=156182, 09.01.2006

EKLER

EK1: Türk Standardları Enstitüsünden Bilgi Güvenliği Yönetim Sistemi Belgeli Kuruluşlar Listesi

Sıra No	Şirket Adı	Faaliyet Alanı
1	Elektronik Bilgi Güvenliği A.Ş.	Elektronik Sertifika Hizmet Sağlayıcısı (Eshs) Olarak Elektronik Sertifika, Zaman Damgası Ve Elektronik İmzalarla İlgili Hizmetlerin Sunumu
2	SPK-Sermaye Piyasası Kurulu Bilgi İşlem, İstatistik Ve Enformasyon Dairesi	Bilgi İşlem, İstatistik Ve Enformasyon Dairesi Bilgi Teknolojileri Hizmetleri Sunumu
3	Plastik Kart Akıllı Kart İletişim Sistemleri San. Ve Tic. A.Ş.	Plastik Kart Üretimi
4	EBG Bilişim Teknolojileri Ve Hizmetleri A.Ş.	Elektronik Sertifika Hizmet Sağlayıcısı (Eshs) Olarak, Nitelikli Elektronik Sertifika, Zaman Damgası Ve Elektronik İmzalarla İlgili Hizmetlerin Sunumu
5	Sisoft Sağlık Bilgi Sistemleri Ltd. Şti.	Bilgisayar Yazılım Tasarım Ve Üretimi Bilgisayar Donanımı Satış Hizmetleri Sunumu
6	Eczacıbaşı Bilişim A.Ş.	Elektronik Sertifika Ve Mobil Elektronik Sertifika, Zaman Damgası Ve Elektronik İmza İle İlgili Güven Merkezi Hizmeti Sunumu
7	Pharmavısıon San. Ve Tic. A.Ş.	Beşeri İlaç Üretimi
8	İşlem Coğrafi Bilgi Sistemleri Mühendislik Ve Eğitim Ltd. Şti.	Coğrafi Bilgi Sistemleri, Uzaktan Algılama Ve Bilgi Teknolojisi Hizmetleri Yazılım Geliştirme Hizmetleri Tasarım, Üretim Ve Sunumu
9	STM Savunma Teknolojileri Mühendislik Ve Tic. A.Ş.	Danışmanlık Hizmetleri Sunumu Yazılım Ağırlıklı Sistem Tasarımı, Geliştirmesi, Kurulumu Ve Bakımı
10	Boydak Holding A.Ş.	Holding Kapsamında Yürütülen Bilgi İşlem Faaliyetleri Sunumu
11	Fintek Finansal Teknoloji Hizmetleri A.Ş.	Bilgi Teknolojileri Servis Yönetimi Ve Uygulama Yazılımı Üretimi
12	Belbim İstanbul Belediyeleri Bilgi İşlem Enerji San. Ve Tic. A.Ş.	Elektronik Sistemler İçin (Ödeme Ve Geçiş Kontrol Sistemleri) Donanım Ve Yazılım Tasarımı, Geliştirilmesi, Kurulumu Ve İşletilmesi

		İlgili Alanda Teknik Destek Ve Danışmanlık Hizmetleri Sunumu
13	T.C. Sağlık Bakanlığı Karabük Devlet Hastanesi	Karabük Devlet Hastanesi Bilgi Güvenliği Hizmetleri Sunumu
14	Globalstar Avrasya Uydu Ses Ve Data İletişim A.Ş.	Uydu, Ses Ve Veri İletişim Hizmetleri Sunumu
15	Ttnet A.Ş.	Internet Servis Sağlayacılığı Hizmetleri A-Kablolu Ve Kablosuz İnternet Hizmetleri B-Katma Değerli Servisler Sabit Telefon Hizmetleri Ttnet Kurumsal Bilişim Süreçleri Sunumu
16	Türk Telekomünikasyon A.Ş. İnternet Veri Merkezi	Veri Merkezi Hizmetleri Ve Süreçleri Sunumu
17	T.C. PTT Genel Müdürlüğü Teknik İşler Ve Otomasyon Dairesi Başkanlığı Posta Ve Telgraf Dairesi Başkanlığı Ulus PTT Merkezi Ve Konya Acil Durum Merkezi	Posta Teknik İşler Ve Otomasyon Dairesi Ve Konya Acil Durum Merkezi Dahilinde Bilgi Teknolojileri Faaliyetleri Ve Telgraf Dairesi Başkanlığı (Kayıtlı Elektronik Posta Faaliyetleri) Ve Ulus Ptt Merkezi (Kayıtlı Elektronik Posta Faaliyetleri) (25.07.2012 Tarihinden İtibaren)
18	T.C. İstanbul Büyükşehir Belediyesi - Bilgi İşlem Daire Başkanlığı	Belediye Bilgi Teknolojileri Faaliyetleri
19	Hobim Bilgi İşlem Hizmetleri A.Ş.	Bilgi İşlem Basım/Zarflama Kart Üretimi Arşiv Yönetim Hizmetleri Sunumu
20	Moreum Bilişim Teknolojileri A.Ş.	Sayısal Arşiv Ve Döküm Yönetim Sistemleri Geliştirme, Tasarım Ve Destek Hizmetleri Sunumu
21	Türksat Uydu Haberleşme Kablo Tv Ve İşletme A.Ş.	İnternet Ve İnteraktif Hizmetler Direktörlüğü Uydu Hizmetleri Kurumsal Çözümler Direktörlüğü Bilişim Sistemleri Ve Bilgi Güvenliği Direktörlüğü - E-Devlet Ve Bilgi Toplumu Direktörlüğü Uydu Kontrol Direktörlüğü, Kablo Sistemleri Altyapı Ve İşletme Direktörlüğü Faaliyetleri Sunumu
22	İstikbal Mobilya San. Ve Tic. A.Ş.	Bilgi İşlem Faaliyetleri Sunumu
23	Merkezi Finans Ve İhale Birimi - Central Fınance And Contracts Unıt	Avrupa Birliği Tarafından Türkiyede Finanse Edilen Programlar Çerçevesinde Gerçekleşen İhalelerin Bütçeleme, İhaleye Çıkma, Sözleşme İmzalama, Ödeme, Muhasebe Ve

		Mali Raporlama Hizmetleri Sunumu
24	Ilgın Ticaret Borsası	Ticaret Borsası Hizmetleri Sunumu
25	T.C. Atatürk Üniversitesi Sağlık Uygulama Ve Araştırma Merkez Müdürlüğü (Atatürk Üniversitesi Aziziye Ve Yakutiye Araştırma Hastaneleri)	Hastane Sağlık Hizmetleri İçin Bilgi İşlem Faaliyetleri Sunumu
26	T.C. Milli Eğitim Bakanlığı Bilgi İşlem Grup Başkanlığı	Milli Eğitim Bakanlığı Bilgi İşlem Faaliyetleri Sunumu
27	Karacadağ Kalkınma Ajansı	Kamu Adına Bölgesel Kalkınma Hizmetleri Sunumu
28	T.C. Bilim Sanayi Ve Teknoloji Bakanlığı Bilgi İşlem Dairesi Başkanlığı	Bilgi İşlem Faaliyetleri
29	Akgün Bilgisayar Program Ve Hizmetleri San. Tic. Ltd. Şti.	Yazılım Üretim Ve Yazılım Geliştirme, Yazılım Destek, Bilgisayar Ve Çevre Birimleri, Network Satış Ve Pazarlama Faaliyetleri Sunumu
30	T.C. Başbakanlık Hazine Müsteşarlığı Ekonomik Araştırmalar Genel Müdürlüğü - Bilgi İşlem Merkezi	Bilişim Hizmetleri Sunumu
31	T.C. Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı	T.C. Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı Bilgi İşlem Faaliyetleri Ve Felaket Kurtarma Merkezi Faaliyetleri Sunumu
32	T.C. Maliye Bakanlığı Strateji Geliştirme Başkanlığı Yönetim Bilgi Sistemleri Dairesi	T.C. Maliye Bakanlığı Strateji Geliştirme Başkanlığı Yönetim Bilgi Sistemleri Dairesi Faaliyetleri Sunumu
33	BSH Ev Aletleri San. Ve Tic. A.Ş	Veri Koruma Ve Bilgi Güvenliği Faaliyetleri; İthalat, İhracat Ve Lojistik Hizmetleri Sunumu
34	Eczacıbaşı Bilişim A.Ş. Veri Merkezi	Veri Merkezi Operasyonları ve Yazılım Geliştirme faaliyetleri Sunumu
35	Altay Kollektif Şti. Murad Dural ve Ortağı	Sistem Yazılım ve Yazılım Geliştirmesi Kurulumu ve Bakım Hizmetleri Sunumu Savunma Sanayi ve Endüstriyel Ticaret Ürünler Pazarlama, Tanıtım ve Danışmanlık Hizmetleri Sunumu

EK2: Anket

1. Kuruluşunuzun büyüklüğü nedir?(BGYS kapsamında yer alan)

0-10 çalışan

11-50 çalışan

51-100 çalışan

101-250 çalışan

251-500 çalışan

501 veya daha fazla çalışan

2. Kuruluşunuzun faaliyet gösterdiği sektör hangisidir? (uygun olanların tümünü seçiniz)

Doğal kaynak çıkarma veya hasat (birincil endüstri) - Örneğin; tarım, ormancılık, balıkçılık, madencilik/mineral çıkarma, petrol/gaz çıkarma, taşocakçılığı.

Hafif üretim veya işleme (ikincil endüstri, düşük çevresel etki) - Örneğin; giyim, mobilya veya küçük tüketim mallarının üretimi veya işlenmesi.

Ağır üretim veya işleme (ikincil endüstri, yüksek çevresel etki) - Örneğin; kimyasal, otomotiv, havacılık, tekstil ve kağıt üretimi; metal işleme veya baskı; gıda ve içecek üretimi ve işlenmesi; elektrik, doğal gaz, inşaat ve nükleer enerji üretimi.

Hizmet odaklı ve/veya entellektüel aktiviteler (üçüncül/dördüncül endüstri) - Örneğin; danışmanlık, denetim, hukuk, finans, sağlık, telekomünikasyon, otelcilik, toptancılık/perakendecilik, eğlence, ulaşım, eğitim, devlet, bilgi teknolojisi, araştırma.

3. Aşağıdaki faktörlerden hangisi Bilgi Güvenliği Yönetim Sisteminin uygulanmasında kuruluşunuzu etkiledi?

Geçerli olanları önem sırasına göre belirtiniz, 1 en önemli olan, 9 en az önemli olanı belirtecek şekilde. Not: Değerlendirilmeyen tüm faktörler için lütfen “bilmiyorum veya uygulanabilir değil” kutucuğunu işaretleyiniz.

Genel imaj

Müşteri şartı

Devlet/düzenleyici kuruluş şartı

Bilgilerin korunması ve muhafaza taahhüdü

Olumsuz bilgi güvenliği ihlali riskin azaltılması

Maliyet azaltma/finansal fayda

Kuruluşun uyguladığı diğer yönetim sistemleri ile entegrasyon fırsatı (örneğin ISO 9001, ISO 50001, ISO 14001, OHSAS 18001)

Diğer

Yukarıdakilerden hiçbiri

4. Kuruluşunuzda Bilgi Güvenliği Yönetim Sistemi ne zamandır uygulanmaktadır?

1 yıldan az

1 - 3 yıl

4 - 6 yıl

6 yıldan fazla

Bilmiyorum/uygulanabilir değil

5. Kuruluşunuzun Bilgi Güvenliği Yönetim Sistemi kapsamı nedir?

Tüm kuruluş

Bir kuruluşun altındaki sahalardan ve tesislerden bir seçim

Aynı yerde bulunan kuruluş, tesis ve işletmeler grubu

Tek bir saha veya tesis yeri

Tek bir iş birimi (bir kuruluşun veya tesisin bir parçası)

Tek bir proses (bir iş biriminin parçası)

6. Bilgi Güvenliği Yönetim Sistemi(nin) (lüffen kutucuklara tık atınız)

Ürün ve Hizmet kalitesine etkisi?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Paydaş ihtiyaçlarının	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek

karşılanmasına?					Değer
Stratejik hedeflere ulaşma da?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Rekabet avantajı sağlama da?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Genel imajı iyileştirme de?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
İş yönetim sistem(ler)i ile entegrasyon da?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Finansal fayda sağlama da?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Teknolojik Gelişme sağlama da?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
İnsan Kaynakları Gelişimine?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Çalışanların Bilgi Güvenliği Yönetimine katılımına?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Kuruluşa Özel Bilgilerin Korunmasına?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Paydaşlar ile	Değer	Düşük	Orta	Yüksek	Çok

iletişim Paydaş memnuniyetine?	Sağlamadı	Değer	Değer	Değer	Yüksek Değer
Yasal şartları yerine getirme yeteneğine?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Kuruluşun Bilgi Güvenliği yönetiminin performansının iyileşmesine?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer
Tedarikçilerin Bilgi Güvenliği yönetimi performansında iyileşmene?	Değer Sağlamadı	Düşük Değer	Orta Değer	Yüksek Değer	Çok Yüksek Değer

7. Bilgi Güvenliği Yönetim Sisteminin başarısını düşüren faktörler size göre nelerdir?

Geçerli olanları önem sırasına göre belirtiniz, 1 en önemli olan, 9 en az önemli olanı belirtecek şekilde. Not: Değerlendirilmeyen tüm faktörler için lütfen "bilmiyorum veya uygulanabilir değil" kutucuğunu işaretleyiniz.

Üst yönetimin desteğinin yetersizliği

Çalışanların katılımının eksikliği

Teknolojinin eksiklik

Dokümantasyon sistemini eksikliği

Finansal desteğin yetersizliği

Çalışanların eğitim ve bilinç eksikliği

Müşteri beklentilerinin karşılanamaması

Diğer

Yukarıdakilerden hiçbiri

8. Bilgi Güvenliği Yönetim Sisteminin başarısının yükselmesini sağlayan faktörler size göre nelerdir?

Geçerli olanları önem sırasına göre belirtiniz, 1 en önemli olan, 9 en az önemli olanı belirtecek şekilde. Not: Değerlendirilmeyen tüm faktörler için lütfen "bilmiyorum veya uygulanabilir değil" kutucuğunu işaretleyiniz.

Üst yönetimin desteği
Çalışanların katılımı
Son Teknoloji uygulanması
Uygun Dokümantasyon sistemini
Finansal destek
Çalışanların yeterliliği ve bilinci
Müşteri beklentilerinin karşılanması
Diğer
Yukarıdakilerden hiçbiri

9. Bilgi Güvenliği Yönetim Sisteminin Kritik Başarı faktörleri size göre nelerdir?

Geçerli olanları önem sırasına göre belirtiniz, 1 en önemli olan, 9 en az önemli olanı belirtecek şekilde. Not: Değerlendirilmeyen tüm faktörler için lütfen "bilmiyorum veya uygulanabilir değil" kutucuğunu işaretleyiniz.

BGYS'nin kurum Kültürü ile tutarlı olması
BGYS'nin stratejik hedeflerle uyumu
BGYS'nin Kuruluşun misyon/vizyonuna uyumu
BGYS'nin Kuruluşun politikasını karşılaması
BGYS'ye Üst Yönetimin tam desteği
Ektin bir şekilde oluşturulan risk değerlendirmeleri
BGYS'nin kaynak ihtiyacının karşılanması
Diğer
Yukarıdakilerden hiçbiri

ÖZGEÇMİŞ

1972 yılında Elazığ'da doğdu. İlk , orta ve lise eğitimini Elazığ'da tamamladı. Özel bir şirkette 1989-1994 yıllarında pazarlama bölümünde çalıştı. 1998-2000 yıllarında yine aynı şirketin İzmir Bürosunda yönetici olarak çalıştı. 2000 yılında Gazi Üniversitesi Beden Eğitimi Spor Yüksek Okulundan mezun oldu. Ankara Deneme Lisesinde 6 ay Öğretmenlik stajını yaptı. 2001 yılında Türk Standardları Enstitüsü'nde işe başladı. 1yıl Ürün Belgelendirme Müdürlüğünde, 7 yıl Sistem Belgelendirme Müdürlüğünde, 3 yıl TSE Azerbaycan Temsilciliğinde Temsilcisi olarak çalışmış olup, halihazırda Standard Hazırlama Merkezi Başkanlığı'nda uzman olarak çalışmaktadır. Atılım Üniversitesinde Avrupa Birliği Bilim Dalında Avrupa Birliği'ne Giriş Sürecinde Yönetim Sistemlerinin (Kalite, Çevre, OHSAS, HACCP) Entegrasyonu ve Bir Uygulama Örneği adlı tezi hazırlayarak yüksek lisans yapmıştır.