BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİNİN BELGELENDİRİLMESİ: BATI KARADENİZ'DE BİR ALAN ARAŞTIRMASI

2021
YÜKSEK LİSANS TEZİ
İŞLETME

Tuğba ÇELİK

Danışman

Dr. Öğr. Üyesi Mehmet Murat TUNÇBİLEK

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİNİN BELGELENDİRİLMESİ: BATI KARADENİZ'DE BİR ALAN ARAŞTIRMASI

Tuğba ÇELİK

Dr. Öğr. Üyesi Mehmet Murat TUNÇBİLEK

T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
İşletme Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

KARABÜK

Temmuz 2021

İÇİNDEKİLER

TEZ ONAY SAYFASI

Tuğba ÇELİK tarafından hazırlanan "BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ BELGELENDİRİLMESİ: BATI KARADENİZ'DE BİR ALAN ARAŞTIRMASI" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Dr. Öğr. Üyesi Mehmet Murat TUNÇBİLEK .....

Tez Danışmanı, İşletme Anabilim Dalı

Bu çalışma, jürimiz tarafından Oy Birliği ile İşletme Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 07/07/2021

Ünvanı, Adı SOYADI (Kurumu) **İmzası**

Başkan : Prof. Dr. Abdullah KARAKAYA (KBÜ) .....

Üye : Doç. Dr. Yaşar AKÇA (BÜ) .....

Üye : Dr. Öğr. Üyesi Mehmet Murat TUNÇBİLEK (KBÜ) .....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans Tezi derecesini onamıştır.

Prof. Dr. Hasan SOLMAZ .....

Lisansüstü Eğitim Enstitüsü Müdürü

DOĞRULUK BEYANI

Yüksek lisans/Doktora tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı herhangi bir yola tevessül etmeden yazdığımı, araştırmamı yaparken hangi tür alıntıların intihal kusuru sayılacağını bildiğimi, intihal kusuru sayılabilecek herhangi bir bölüme araştırmamda yer vermediğimi, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bu eserlere metin içerisinde uygun şekilde atıf yapıldığını beyan ederim.

Enstitü tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak ahlaki ve hukuki tüm sonuçlara katlanmayı kabul ederim.

Adı Soyadı: Tuğba ÇELİK

İmza :

ÖNSÖZ

Tez çalışmam süresince tecrübe, bilgi ve yardımlarını esirgemeyen Danışmanım Sayın Dr. Öğr. Üyesi Mehmet Murat TUNÇBİLEK'e teşekkürlerimi ve saygılarımı sunarım.

Tez çalışması için mülakat yaptığım kuruluşların değerli yöneticileri ve çalışanlarına vakit ayırdıkları ve yardımlarını esirgemedikleri için, hayatım boyunca destek ve sevgilerini her zaman yanımda hissettiğim, sevgili anne ve babama, beni her zaman destekleyen değerli eşim Yüksel Çelik'e , oğlum Bedirhan ve Selimhan'a çok teşekkür ederim.

ÖZ

Teknolojinin, iletişimin ve internetin hızlı bir şekilde gelişmesi ile kuruluşların sahip olduğu bilginin güvenliğini de sağlamanın önemi her geçen gün artmaktadır. Bilgi güvenliğinin öneminin ve bilinirliliğinin artması ile, kuruluşlar sahip olduğu bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için çözüm arayışına girmişlerdir. Kuruluşların hassas bilgilerini bilgi güvenliği unsurları çerçevesinde koruma altına alması meydana gelebilecek zararları en aza indirecektir. Bu da kuruluşlarda bir bilgi güvenliği yönetim sistemi kurulmasını gerektirmektedir. Bu çalışma, tüm dünyada kabul görmüş ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi standardını kurmak, uygulamak, sürdürmek ve sürekli iyileştirmek isteyen ve bu süreçte karşılaştıkları sorunlara bir rehber olması amacıyla Batı Karadeniz Bölgesinde ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi sertifikasına sahip olan kuruluşlar tespit edilerek mülakat çalışması yapılmıştır. Nitel araştırma yöntemine dayalı olarak yapılan bu çalışmanın verileri, nitel veri analizi şekli olan betimsel analiz tekniği kullanılarak analiz edilmiştir. Analiz edilen verilere dayanarak bu belgeyi almak isteyen ve halihazırda alan kuruluşların sistemi kurmaları ve yürütmeleri sırasında uygulayabileceği çözüm önerileri; bulundukları sektör ile ilgili araştırma yapması ve bilgi alışverişinde bulunarak ortaya çıkan tecrübelerin paylaşımı, üst yönetimin desteğini her aşamada alarak kuruma özgü bir BGYS oluşturmaları, çalışanları sürece dahil ederek sistemin sahiplenmesini, kendi kurumlarına özgü uygulama yöntemlerini geliştirmelerini ve bilgi güvenliği konusunda bilinçli bir IT departmanı kurulmasını, BGYS komitesinin bilgili, mutlaka BGYS kapsamını ilgilendiren birimlerden oluşması, şeklinde sunulmuştur.

Anahtar Kelimeler: Bilgi Güvenliği; BGYS; Bilgi Güvenliği Yönetim Sistemi; ISO/IEC 27001:2013

ABSTRACT

With the rapid development of technology, communication and the internet, the importance of ensuring the security of information that organizations have is increasing day by day. With the increasing importance and awareness of information security, organizations have sought solutions to ensure the confidentiality, integrity and accessibility of their information. If organizations protect their sensitive information within the framework of information security elements, it will minimize the damages that may occur. This requires the establishment of an information security management system in organizations. This study has been awarded the ISO / IEC 27001: 2013 Information Security Management System certificate in the Western Black Sea Region in order to establish, implement, maintain and continuously improve the globally accepted ISO / IEC 27001: 2013 Information Security Management System standard and to be a guide to the problems they encounter in this process. The data of this study, which is based on the qualitative research method, were analyzed using the descriptive analysis technique, which is a type of qualitative data analysis. Based on the analyzed data, the solution proposals that the organizations that want or have received this document can implement during the establishment and execution of the system; to do research about the sector in which it operates and to share its experiences by exchanging information, to create a customized ISMS with the support of the senior management at every stage, to embrace the system by including the employees in the process, to develop application methods specific to their own institutions and to establish an IT department with information security awareness, with the scope of ISMS It is presented as an ISMS committee, which is necessarily composed of relevant knowledgeable units.

Keywords: Information security, ISMS, Information Security Management System, ISO/IEC 27001:2013

ARŞİV KAYIT BİLGİLERİ

Tezin Adı	Bilgi Güvenliği Yönetim Sistemlerinin Belgelendirilmesi: Batı Karadeniz'de Bir Alan Araştırması
Tezin Yazarı	Tuğba Çelik
Tezin Danışmanı	Dr. Öğr.Üyesi Mehmet Murat Tunçbilek
Tezin Derecesi	Yüksek Lisans
Tezin Tarihi	07/07/2021
Tezin Alanı	İşletme
Tezin Yeri	KBÜ/LEE
Tezin Sayfa Sayısı	137
Anahtar Kelimeler	Bilgi Güvenliği; BGYS; Bilgi Güvenliği Yönetim Sistemi; ISO/IEC 27001:2013

ARCHIVE RECORD INFORMATION

Name of the Thesis	Certificatıion of Information Security Management Systems: A Field Study in The West Black Sea
Author of the Thesis	Tuğba Çelik
Advisor of the Thesis	Dr. Öğr.Üyesi Mehmet Murat Tunçbilek
Status of the Thesis	Master's Degree
Date of the Thesis	07/07/2021
Field of the Thesis	Business
Place of the Thesis	KBU/LEE
Total Page Number	137
Keywords	Information security, ISMS, Information Security Management System, ISO/IEC 27001:2013

KISALTMALAR

BGYS : Bilgi Güvenliği Yönetim Sistemi

BT : Bilgi Teknolojileri

CCTA : Central Computer and Telecommunications Agency (Merkezi Bilgisayar ve Telekomünikasyon Ajansı)

CEN : Avrupa Standardizasyon Komitesi

COBIT : Control Objectives for Information and Related Technology (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)

DF : Düzeltici Faaliyet

EA : European Co-operation For Accreditation (Avrupa Akreditasyon Birliği)

EK-A : Annex A Kontrol Maddeleri

EPDK : Enerji Piyasası Düzenleme Kurumu

IEC : International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)

ISACA : Information Systems Audit and Control Association (Bilgi Sistemleri Denetim ve Kontrol Birliği)

ISMS : Information Security Management System (Bilgi Güvenliği Yönetim Sistemi)

ISO : International Standart Organization (Uluslararası Standart Organizasyonu)

IT : Information Technologies (Bilgi Teknolojileri)

ITIL **:** Information Technology Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)

PUKÖ **:** Planla, uygula, kontrol et ve önlem al.

SOA : Statement of Applicability (Uygulanabilirlik Bildirgesi)

SPK : Sermaye Piyasası Kurulu

TDK : Türk Dil Kurumu

TS : Türk Standartları

TURKAK : Türk Akreditasyon Kurumu

TÜİK : Türkiye İstatistik Kurumu

UKAS : United Kingtom Accreditation Service (İngiltere Akreditasyon Kurumu)

YGG : Yönetimin Gözden Geçirmesi

YYS : Yetkili Yükümlü Statüsü

API : American Petroleum Institute (Petrol Kuyusu Çimentosu Lisansı)

KVKK : Personal Data Protection Authority (Kişisel Verileri Koruma Kurumu)

ARAŞTIRMANIN KONUSU

Bu çalışma, bir kurumdaki ISO/IEC 27001:2013 standardının sertifikasyonunu ve bu süreçte karşılaşılan zorlukları konu almıştır. Kuruluşlar ve işletmeler tarafından doğru bir şekilde uygulanan standart, alınan bilgi güvenliği yönetim sistemi sertifikasının gereklilikleri, yapılması gerekenler ve bu süreçte kuruluşların karşılaştığı zorluklar ele alınmıştır.

ARAŞTIRMANIN AMACI VE ÖNEMİ

Bilgi varlıkların korunmasına yönelik önemin her geçen gün artması sebebiyle, Batı Karadeniz Bölgesi'nde bulunan, ISO/IEC 27001:2013 sertifikasına sahip kurum ve işletmelerin sertifikasyon süreçleri ve bu süreçte karşılaştıkları zorluklar ele alınmıştır. Bu yolda kuruluşlara ve araştırmacılara, bilgi güvenliği yönetim sistemi kurulumu hakkında yardımcı olabilecek yöntem ve teknikleri sade bir dille, kurumların ve işletmelerin tecrübelerini dayanak göstererek, anlaşılır bir dille, BGYS kurmak isteyen kurum ve işletmelere bir yol gösterici olması amaçlanmıştır.

Bu tez çalışması, ülkemizdeki tüm kurum ve kuruluşlarda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin sertifikasyonunu ve karşılaşılan güçlükleri anlamak açısından önem arz etmektedir.

ARAŞTIRMANIN YÖNTEMİ

Nitel araştırma yöntemine dayalı olarak yapılan bu çalışmanın verileri, yarı yapılandırılmış görüşme tekniği ile toplanmıştır. Görüşmeler, içinde bulunduğumuz pandemi sürecinden dolayı telefon ve zoom programı ile kurumun BGYS komitesinde görevli olan çalışanlar ile gerçekleştirilmiştir.

Mülakat yapılan üç kuruluşun isimlerinin açıklanmaması nedeniyle kuruluşların adları A, B ve C şeklinde kodlanılmıştır. Tat Metal firma isminin görünmesinde hiçbir sakınca olmadığını belirttiğinden kodlanmamıştır.

Araştırmada elde edilen veriler nitel veri analizi şekli olan betimsel analiz tekniği kullanılarak analiz edilmiştir. Betimsel analiz tekniğinde elde edilen veriler daha önceden belirlenen başlıklar altında özetlenir ve yorumlanır.

ARAŞTIRMA SORULARI

Kuruluşlar neden ISO/IEC 27001 sertifikasına ihtiyaç duyarlar?

ISO/IEC 27001 sertifikasına sahip kuruluşların başarısına katkıları nelerdir?

Sertifika öncesi ve sonrasında karşılaşılan problemler ve çözüm önerileri nelerdir?

ISO/IEC 27001 bilgi güvenliği yönetim sisteminin iş süreçlerine katkıları ne derecedir?

ISO/IEC 27001 yönetim sistemine sahip olan firmalar başarılarını bilgi güvenliği bilincini sağlamış çalışanına mı dayandırırlar?

ISO/IEC 27001 bilgi güvenliği yönetim sistemi için insan kaynakları önemli bir faktör müdür?

ISO/IEC 27001 bilgi güvenliği yönetim sistemine sahip olan kuruluşların aşmış oldukları engellerden en önemlisi bilginin stratejik bir faktör olarak görülmesi midir?

KAPSAM VE SINIRLILIKLAR

Araştırmanın evreni, Batı Karadeniz Bölgesi sınırlarındaki ISO/IEC 27001:2013 sertifikasına sahip beş adet kurum ve işletmeden oluşmaktadır. Bu kapsamda dört kuruluşla görüşme gerçekleştirilmiş olup diğer kuruluşla iletişim kurulamadığından dolayı çalışma dışı bırakılmıştır.

Sertifika sahibi kuruluşların Batı Karadeniz Bölgesi'nde çok az olması araştırmanın önemli kısıtlarındandır.

Bu konuda yapılan akademik çalışmaların az olması, bilgi güvenliği hususunun hassas bilgiler içermesi ve kuruluşların bu konudaki araştırmalara ihtiyatlı yaklaşmaları da bu çalışmanın güçlüklerindendir.

Araştırma kapsamında olan ve bölgede sektörün öncü ve önemli bir kuruluşun araştırmaya dahil edilememesi elde edilen bulguların karşılaştırılması, katkı düzeyinin artırılması ve bilgi birikiminin aktırılamaması araştırmanın kısıtlarındandır.

GİRİŞ

Bilgi sürekli bir gelişim ve değişim içerisinde olmuş ve toplumlarda geçmişten günümüze kadar bu değişim ve gelişimden etkilenerek şekillenmişlerdir. Günümüzde kamu ve özel sektördeki kurumlar bilgilerini doğru bir şekilde kullanarak ve yöneterek rakiplerinin önüne geçmeye çalışmaktadırlar. Ancak kurumlar için önemli olan, sahip oldukları bilgileri koruyabilmeleri gerekmektedir. Kurum için güç ve ekonomik değer olan bilgi elektronik ortamlarda, kağıt üzerinde ve çalışanların hafızasında tutulmaktadır. Kurum bu bilginin güvenliğini sağlamalı ve gerekli tüm önlemleri almalıdır. Sürekli değişim halinde olan bilgi güvenliğinin sağlanması ihtiyacı, standartlaşmış yönetim sistemlerinin kurumlarda kurulması gerekliliğini ortaya çıkarmıştır (Irmak & Baz, 23-25 Ağustos 2019, s. 333).

Ülkemizde ve uluslararası seviyede kurumların bilgi varlıklarının korunması ile ilgili bazı hukuki düzenlemeler vardır. Kurumlar yasal şartlara uymak şartıyla kendilerine özgü bilgi güvenliği sistemlerini oluşturabilir ve yönetebilirler. Bu maksatla uyguladıkları ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı kuruma bir çok üstünlük sağlayacaktır (Bingöl, 2010, s. 1). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, bir bilgi güvenliği yönetim sisteminin oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için bir süreç yaklaşımı faaliyetini icra etmeyi gerektirir. Bu yaklaşım planla, uygula, kontrol et ve önlem al (PUKÖ) döngüsünü benimsemektedir. Böylece bu süreç yaklaşımı ile faaliyetler tanımlanır, izlenir ve performans ölçümü kolaylaşır. Standarda göre kurum tarafından iç ve dış hususlar belirlenerek kapsam oluşturulmalıdır. Üst yönetimin desteği ile bütün kurumun uyacağı ve uygulayacağı bir politika oluşturulmalı, rol ve sorumluluklar tanımlanmalıdır. Kurum risk ve fırsatlarını dokümante etmeli ve uygun risk işleme planı hayata geçirmelidir. Bilgi güvenliği yönetim sisteminin çalışmasını denetlemeli ve performans değerlendirmesi yapmalıdır. İç tetkikler yaparak görülen uygunsuzluklar ve yetersiz alanlar düzeltilmelidir (Emir Erdoğan, Ocak, 2020, s. 11).

ISO/IEC 27001 standardı bu alanda oluşturulmuş en geçerli standarttır ve sektöre ve kurum yapısına bakılmaksızın bütün kurum ve kuruluşlarda uygulanabilir olması sebebiyle kurulması zorunlu hale getirilmeye başlanan bir standarttır. ISO/IEC 27001

standartı kapsamında bulunan kontroller ile aktif yönetilen bir bilgi güvenliği ve ölçülebilen bir yaklaşım sunmaktadır (Rhodes-Ousley, 2013).

Bilgi güvenliği sadece bir departmanın, yetkilinin, donanım ve teknik alt yapısıyla sağlanacak bir işlem değildir. Bilgi güvenliği kavramının teknik bir yapıdan oluştuğu düşünülse de aslında bilgi güvenliği bireyde başlayan bir süreçtir. Bilgi güvenliğinin sağlanması konusunda ilk önce üst düzey yöneticilerin istikrarlı davranışları ardından bütün çalışanların uyacağı bir süreç başlamalıdır. Unutulmamalıdır ki sürecin en zayıf halkası insandır. Geri dönüşü olmayan hatalarla karşılaşmamak için bilgi güvenliği ile ilgili çalışanlara gerekli eğitimler sağlanmalıdır (Akay, 2014, s. 4).

Bilgi güvenliği yönetiminde amaç; durumları gerçekleşmeden önce tahmin etmek ve engelleyici önlemler almak, önlenemeyen durumlar olduğunda ise, en kısa zamanda minimum zararla uygun şartları sağlayabilmektir. Bunun için, kurumun en doğru süreçleri belirlemesi ve bu süreçleri hayata geçirmek gerekli bilgi, kültür ve olgunluğa sahip olması gereklidir. Günümüzde toplumda ve kurumlarda artan bilgi güvenliği farkındalığı, ortaya çıkardığımız bilginin ve ticari ayrıcalıklarımızın gizliliğini ve güvenliğini garanti altına alacak, bilgi kayıpları ile ortaya çıkan moral bozukluğu, iş, zaman ve para kayıplarını en aza indirecek, bilgi birikimi oluşacak, insanlar bilinçlenecek, genç kuşağın ileri teknoloji temelli ürün ve hizmet geliştirmesini gayretlendirerek ülkemizin kalkınmasına destek olacaktır.

Bilgi güvenliği yönetim sistemi kurulumu stratejik bir karardır ve üst yönetimin bilgi güvenliğine karşı aldığı tutum ve kararlı oluşu yönetim sistemini onaylaması ile yakından ilgilidir. Yani bilgi güvenliği yönetim sistemi, üst yönetimin verdiği karar ile oluşturulur. Üst yönetim, yasal şartları sağlamak için, daha güvenilir bir süreç yürütmek için, kurumlarını sektörde hedeflenen noktaya çıkarmak ve avantajlı bir rekabet ortamı yaratmak için gerekli bilgi güvenliği komitesini oluşturmalıdır ve bu ekibin başarılı olması için her türlü desteği sağlamak zorundadır.

Bilgi güvenliğinden üst seviyede fayda sağlanabilmesi için bilgi güvenliğinin istikrarlı bir şekilde sürdürülmesi gereken bir süreç olduğu ve bu sürecin bilgi güvenliği standartları ile yönetilmesi gerektiği unutulmamalıdır.

Bu çalışmada Bilgi güvenliği ile ilgili literatür taraması hakkında bilgi verildikten sonra çalışmanın **birinci bölümünde**, bilgi güvenliği yönetim sistemi sürecinin

önemini vurgulayabilmek için öncelikle bilgi güvenliği ile ilgili temel kavramlara yer verilmiştir. Bilgi güvenliği kavramı ile ilgili güvenlik kavramlarından bahsedilerek kurumda bilgi güvenliğinin sağlanması için alınması gereken önlemler olan yönetsel, teknolojik, eğitim ve farkındalık programları ve fiziksel ve çevresel önlemlere yer verilmiştir. Devamında bilgi güvenliği yönetiminde dünyada en yaygın kullanılan ITIL ve COBIT hakkında bilgi verilmiştir. Ardından bilgi güvenliği standartları ailesine dahil olan diğer standartların tanıtımı yapılmıştır.

Çalışmanın **ikinci bölümünde**, ISO/IEC 27001 sertifikası hakkında bilgi verilmiş, bilgi güvenliği yönetim sisteminin tarihsel sürecine değinilmiş, ISO/IEC 27001 belgesine sahip olmak zorunda olan ve sertifikayı almanın kuruma sağlayacağı faydalara değinilmiş, konunun içeriğinde ISO 27000 serileri ile bilgi verilmiştir. Ayrıca ISO/IEC 27001 sertifikası için gerekli olan bilgi güvenliği yönetim sistemi hakkında bilgi verilmiştir.

Çalışmanın **üçüncü bölümünde** pukö döngüsü hakkında bilgi verilmiştir. Pukö döngüsü aşamalarının standartın ana maddeleriyle olan ilişkisi hakkında bilgi verilmiş ve Pukö aşamalarında gerçekleştirilmesi gereken standart maddeleri açıklanmıştır. Bilgi güvenliği yönetim sistemi uygulama adımları olan; BGYS komitesi, roller ve sorumluluklar, BGYS için zorunlu dokümanların oluşturulması, kuruluşun bağlamını oluşturmak, kapsamın belirlenmesi ve BGYS ile uyumlu güncel veriler paylaşılmıştır. Devamında ise bilgi güvenliği için en önemli aşama olan risk yönetimi geniş bir şekilde incelenmiş ve risk yönetiminin alt başlıkları olan risk ve fırsatları belirleme, varlık yönetimi ve varlık envanteri hazırlama, bilgi sınıflandırma ve bilgi etiketleme, bilgi güvenliği risk değerlendirmesi, risk işleme planı, uygulanabilirlik bildirgesi (SOA) detaylı bir şekilde açıklanmıştır.

Çalışmanın **dördüncü bölümünde** ilgili literatür paylaşılmıştır.

Çalışmanın **beşinci bölümünde** ISO/IEC 27001 standardının sertifikasyonu ve bu süreçte karşılaşılan zorluklar ile ilgili araştırmanın sorularına ve bulgularına yer verilmiştir.

BİRİNCİ BÖLÜM: BİLGİ

1.1. BİLGİNİN TANIMI ve ÖNEMİ

İnsanlar asırlardır öğrenme içgüdüsünü gidermek, yaşamını sürdürebilmek, ihtiyaçlarını karşılayabilmek ve kısacası geleceğini sürdürebilmek için bilgiye ihtiyaç duymuşlardır. Bilgi, bütün oluşumlar ve insanlığın değişim ve gelişimi için gerekli ana yapıtı haline gelmiştir. Bu nedenle bilgiye doğru anlamı yüklemek bilgiyi kullanmak açısından önem kazanmaktadır. Bilgi kavramının ne olduğunu anlayabilmek için önce bilgi kavramıyla alakalı veri ve enformasyon kavramlarının ne anlama geldiğini bilmek gerekir. Çünkü bu kavramlar birbirleriyle doğrudan ilişkilidir.

Veri

Veri ingilizce anlamıyla data, işlenmemiş ham gerçekler anlamına gelmektedir. Bir konu üzerine yaptığımız araştırma, görüşme, soruşturma ve akıl yürütme sonucu edinilmiş ham, yorum yapma imkanı doğuracak sistemleştirilmemiş bilgidir. Veri, şimdi ve geçmişteki olaylarla ilgili ham gerçekleri kapsamaktadır. Bunlar ilk görüşte bir anlam ifade etmeyen sembol, harf, rakam, işaret ve izlenimlerdir (Öğüt, 2001). Veri, bilgi elde etmedeki temel faktördür.

Enformasyon

Fransızca information anlamına gelen enformasyon Türk Dil Kurumu (TDK)'na göre danışma, tanıtma, haberleşme anlamına gelmektedir. Bilginin oluşturulmasında veriden sonraki adımı enformasyon sağlar (Şentürk, 2008, s. 12). Enformasyonda ilgili veriler bir amaç doğrultusunda bir arada tutulan verilerdir. Bu anlamda enformasyona anlamlandırılmış veri de denilmektedir. Enformasyon, işlenmemiş verilere anlam kazandırmaktır. (Akgün & Keskin, 2003, s. 175-188)' ne göre enformasyon insan beyninde işlenmekte ve önceki bilgiler kullanılarak bu bilgiler yeni bilgilere dönüşmektedir. (Zaim, 2005, s. 68) enformasyon hakkında "belli bir şekle sokulmuş, anlam taşıyan ve insanlara faydalı olabilecek verilerdir" demiştir.

Bilgi

Bilgi, Türk Dil Kurumu tarafından Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf " ve " İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf " olarak tanımlanmıştır (TDK). Veriden

enformasyona, enformasyondan da bilgiye ulaşırız. Bilgi kavramı anlamlandırılmış enformasyondur. Veri, enformasyon ve bilgi arasındaki ilişkiyi örnekleyecek olursak, şirket müşterilerine ait elektronik posta (e-mail) adresleri bir veridir. Bu elektronik postalardan anlamlı bir şekilde oluşturulmuş e-posta tablosu bir enformasyondur. Bu e-posta rehberindeki bir elektronik postayı tanıyarak, bunun bir müşterimize ait olduğunu düşünmemiz bir bilgidir. Enformasyonun tanımını yaparak, eldeki veriyi irdeleyip, yorumlayarak, karar verme süreci sonrası uygulayarak bilgiye ulaşmış oluruz (Ok, Ekim 2013, s. 21).

Şekil 1. Veri, Enformasyon ve Bilgi Arasındaki İlişki.

İşletmeler, kurum ve kuruluşlar için ise bilgi; alıcılar, ortaya konulan değerler, süreçler, yapılan yanlışlar ve kazanılan başarılara ilişkin sahip olunan enformasyondur. Bu bağlamda enformasyonun, stratejilere dönüştürülmesi, rantabilite /yenilik/yaratıcılık ve birbirleriyle yarış süreçlerinde kullanılması bilgiyi önümüze çıkarır. Bu bağlamda işletmeler, kurum ve kuruluşlar için bilgi:

1. Yerinde karar vermede,

2. İleriye özgü çıkarımlar yapmakta,

3. Anlaşılır bir iletişimin kurulmasında,

4. Standart bir ürün/hizmet yaratmakta,

5. Var olan sorunların ortadan kaldırılmasında ve olabilecek sorunlara çözüm bulunmasında; kullanılan bir araçtır (Aktan & Vural, 2005, s. 121-173).

Günümüzde bilgiyi elinde tutup yönetebilen organizasyonlar güçlü konumuna ulaşmıştır. Bu organizasyonlar bilgilerine bilgi katarak, yeni fikirler üretip ekonomik üstünlük sağlayarak rakiplerinin hep bir adım önünde olmuşlardır (Atılgan, 2009, s. 201-212). Teknolojinin olmadığı ve gelişmediği dönemlerde, bilginin yönetilmesi ve güvenliği şu ana göre daha basit olmuştur. Günümüzde ise insanlar ve organizasyonlar bilgilerini genellikle bilgisayar ile yönetmektedir. Bilişim teknolojilerinin zamanla gelişmesi ve hayatımızın vazgeçilmez bir unsuru olmasıyla birlikte kişisel olarak sahip olduğumuz bilginin yönetilmesi, korunması daha basitleşmişken; bir topluluk, bir kurum, bir organizasyon olduğunda bunun korunması ve yönetilmesi daha karmaşık ve içinden çıkılamaz bir hal almaktadır (Yılmaz M. , 2018, s. 8).

1.2. BİLGİ YÖNETİMİ

Günümüzde teknolojik gelişmeler ve küresel ekonomik entegrasyon, dünya genelinde rekabetin şiddetlenmesine ve belirsizliğin artmasına neden olmaktadır. Organizasyonlar, rakiplerine üstünlük sağlayabilmek için daha fazla yenilik ve buluş ortaya koyarak ve evrensel çapta başarılı olduklarını ortaya koymak zorundadırlar. Evrensel çapta rekabeti elinde bulundurabilmenin en önemli noktası rakibine göre daha fazla yenilik bu buluş ortaya çıkaracak önemli bilgilere sahip olmaktır. Bu süreçte güçlü organizasyonlar daima yeni bilgiler türetebilen, bu bilgileri organizasyonda yeni teknoloji ile bütünleştirebilen organizasyonlardır. Bilgi yönetimi, rekabetin arttığı, değiştiği ve her şeye şüphe ile yaklaşılan bir süreçte, organizasyonların gücünü korumak, bu duruma uyum sağlamak ve rekabet güçlerini artırmak için, bilgi teknolojilerinin veri ve enformasyon oluşturma kapasitesi ile insan olgusunun yaratıcılık-yenilikçilik kapasitesini uyumlu bir şekilde birleştirmeyi amaçlamıştır (Malhotra, 1998, s. 58-60).

Bilgi yönetimi farklı bölümlere ve hedeflenen amaca göre değişik tanımlar içerebilir. Ancak tüm tanımlar ortak yanları vardır. İlk olarak bilgi yönetimi, adım adım kat edilmesi gereken bir süreçtir. İkinci olarak bilgi yönetimi, hedeflerin gerçekleşmesi için ortak aklın kullanılması demektir. Bu sebeple bilgi yönetimi ile ortaya çıkan

faaliyetlerin ölçülebilen verimlilik ve sonuçlara sahip olması gereklidir (Barquin, 2001, s. 129).

Bilgi yönetimi, organizasyonların başarılarının artması için bilgiyi icraata dönüştürmeye yönelik taktiksel bir girişimdir (Plunkett, 2001, s. 7).

Bilgi yönetimi, kuruluşların performansını arttırmak için bilgiyi ortaya çıkarmak, bilgiyi kurum içine almak, bilgiyi ilgili birimlerde paylaşmak, kullanmak ve geliştirmek kullanılacak yeni yöntem şeklinde ifade etmektedir (Barutçugil, 2002, s. 49).

Hüseyin Yılmaz (Yılmaz H. , 2010, s. 59-76) ise bilgi yönetimi hakkında, bilgiye ne zaman, nerede, kim tarafından, ihtiyaç olmadan, kuruluş için hazır ve kullanılabilir forma dönüştüren, fikir ve deneyimi kapsayan bir süreç olarak bilgi vermektedir.

Bilgi yönetimi Amerikan Üretim ve Kalite Merkezi tarafından, bilginin ortaya çıkması ve değer yaratması için zamanında ve ilgili kişilere ulaşmasını sağlamak için yöntemli yaklaşımlar olarak tanımlanmıştır (Buckman, 2004, s. 17).

Elias Awad ve Hassan Ghaziri (Awad & Ghaziri, 2004, s. 2) göre bilgi yönetimi, kurumların ana yapıtaşı ve birimlerin içerisinde bilgiyi yönlendiren disiplinler arası bir modeldir. Bilgi yönetimi; ekonomi, psikoloji ve enformasyon yönetimi gibi birçok bilim dalı üzerine kurulmuştur. Bilgi yönetimi, çağımız organizasyonlarının en üstünüdür. Bilgi yönetiminin bölümleri, beşeri faktörü, teknolojiyi ve sürekliliği içerir.

İsmet Barutçugil' e (Barutçugil, 2002, s. 84) göre örgüt politikasında bilgi yönetimine yer veren organizasyonlar, faaliyetlerini bir takım ilkeler çerçevesinde gerçekleştirmelidirler. Bu ilkeler:

- Bilgi yönetiminin sürekliliği vardır.
- Aktif bir bilgi yönetimi, beşer ve teknolojik unsurları bir araya gerektirir.
- Bilgi yönetimi aşırı politik bir yönetimdir.
- Bilgi yönetimi bilgi yöneticileri zorunlu kılar.
- Bilgi yönetimi, en çok, bilgi haritalarından ve piyasalarından yararlanır.
- Diğer taraflarla bilgiyi paylaşmamayı ve kullanmamayı gerektirir.

- Bilgiye ulaşma birinci adımdır.
- Bilgi yönetimi süreklilik arz eder.
- Bilgi yönetimi, bilgi sözleşmesini zorunlu kılar, olarak belirtmiştir.

Bilgi yönetimi farklı birimlerde uzmanlaşmış ekip ile gerçekleştirilmesi gereken bir süreç olarak değerlendirilebilir. Yukarıda verilen tanımlarda aktarıldığı gibi bu sürecin asla tamamlanamayacağı, sürekli bir değişim ve gelişim içerisinde olması gerektiği, farkına varılması gereken bir durumdur (Ünal, 2019, s. 20-21).

1.3. BİLGİ GÜVENLİĞİ KAVRAMI

Bilgi güvenliği, bilgisayar kullanımının insan hayatında yaygınlaşmasından sonra ortaya çıkan bir kavram gibi görünse de tarihin ilk dönemlerinden itibaren sosyal ve ekonomik bir değer olarak kullanılan bilginin başkaları tarafından ele geçirilmesinden sakınıldığı ve korunduğu bilinmektedir (Harold, 2007, s. 44). Sanayi devrimi, iletişim teknolojilerinin gelişmesini ve kullanımının artmasını sağlamış ve sinyal, ses sonrasında görüntünün taşınabilen bir boyuta gelmesiyle, bilgi güvenliğinin önemini artırmıştır. 1990' lı yıllarda internetin kullanılmaya başlanmasıyla birlikte insanların ve kurumları iletişimleri kolaylaşmış ve bu durum güvenlik tehditlerinin oluşmasına sebep olmuştur (Güngör, 2015, s. 26).

Bilgi güvenliği (information security), kuruluşun faaliyetlerinin devamlılığını sağlamak amacıyla bilgilerin her türlü riske karşı organize bir şekilde korunmasıdır (Çubukçu, 2018, s. 3).

Gün geçtikçe bilginin artması ve teknolojik fırsatların hayatımıza dahil olmasının yanı sıra organizasyonların bilişim teknolojilerine bağlı icraatta bulunmaları bilgi güvenliği kavramının ortaya çıkmasına sebep olmuştur. Bilgi güvenliği, kurumlarda bilgiyi tutmak ve ilgili birimlere ulaştırmak için kullanılan donanımın ve alt yapının korunması da dahil olmak üzere kurum için önemli bilgilerin üretilmesini, bir arada toplanmasını, depolanmasını, ihtiyaç halinde kullanılmasını, uygun birimlere iletilmesini ve korunmasını kapsamaktadır (FFIEC, 2010, s. 1).

ISO/IEC 27001 dokümanı bilgi güvenliğini, olası bir bilgi güvenliği açığı, bilgileri korumakla görevli kişilerin başarısızlığı ya da daha önceden öngörülemeyen

güvenlikle alakalı oluşabilecek bir durumu bildiren bir sistem, hizmet ya da ağ durumu olarak tanımlamaktadır.

(Yusufovna & Kim, 2007, s. 17-32) göre bilgi güvenliği kavramı, genel bir bakış açısı ile bilgi ve bilgi teknolojilerine yetkisiz bir şekilde erişime, faydalanmaya, dönüştürme veya ortadan kaldırma yollarından koruma olarak açıklanmıştır.

(Karadoğan, Daş, & Baykara, 2013, s. 231-239) ise kavramı, bilgiye erişimin zorunlu olduğu durumda bilginin kaynağından ulaşacağı noktaya kadar gizliliğini bozmadan, değişime uğramadan ve ele geçirilmeden ulaştırılması süreci ve işlemleri şeklinde tanımlamışlardır.

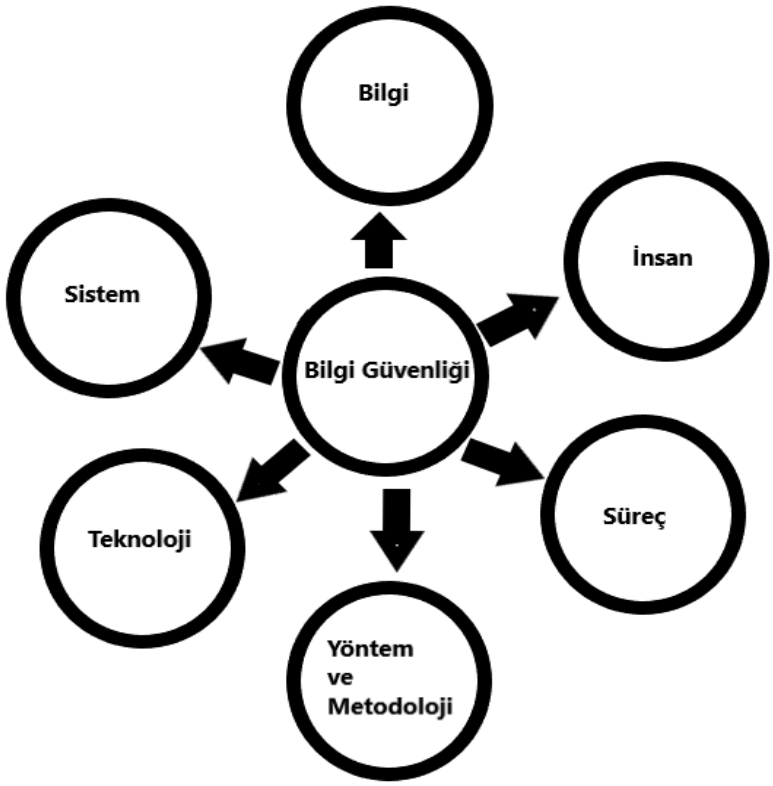
Öte yandan bilgi güvenliği, bir kısım ya da kişinin önemli ölçüde yüklediği değer, bu sebeple de bir bilginin ya da bilgi topluluğunun kısıtlanması ve gizli tutulduğu anda, bilgiye erişimi olmayan kişi veya topluluklar tarafından kullanımının engellenmeye çalışılmasıdır.

Bilgi güvenliğinden söz edebilmemiz için gizlilik, bütünlük, erişilebilirlik gibi temel güvenlik ilkelerinin varlığı önemlidir. Bu üç temel ilke dışında kimlik tespiti, güvenirlik ve inkâr edememe de alt bileşenler olarak sıralanabilir (Canbek & Sağıroğlu, Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme, 2007, s. 1-12).

Bilgi, asırlardır en önemli varlık olarak süregelmiştir. Kişiler, kurumlar ve ülkeler için fikri mülk olarak tanımlanan bilgiye ulaşılması ve saklanması kolay olmamıştır. İnsanlığın başladığından beri bilginin muhafaza edilmesi, süregelen zaman boyunca hayati derecede önemli olmuş ve bu önem şimdiki bulunduğumuz teknolojik çağda da önemliliğini daha çok arttırmıştır (Gülmüş, 2010, s. 1).

Yaşadığımız çağa damgasını vuran bilgi, geniş kapsamlı analiz edilmesi gereken bir soruna dönüşmüştür. Muasır medeniyetlerin bir göstergesi olan teknoloji, insan hayatını basitleştirmiş ve geliştirmiştir, Bu süreçte saldırıların hedefi haline gelmiştir (Öztemiz & Yılmaz, 2013, s. 87-100). İkinci Dünya Savaşından sonra teknolojik aletlerin hayatımıza dahil olmasıyla başlayan bilgi çağı, bilginin elektronik ortamda daha da çok çoğalmasıyla bilgi güvenliğinin kişisel ve kurumsal bazda en üst sınırda seyretmesine neden olmuştur (Güngör, 2015, s. 1).

Bilgi güvenliğinin sağlanması için geçerli tedbirler alınmalı ve alınan bu tedbirler titizlikle uygulanmalıdır. Ülkemizde, maalesef, çoğu kuruluşun ve her seviyeden bilgisayar kullanıcısının genellikle teknolojik aletlere ve bilgi güvenliğine bakış açısının yetersiz olduğu tespit edilmiştir (http://www.cagataycebi.com/security/bilgi_guvenligi.pdf). Bilgi güvenliğini sağlamak için ilk önce bilgisayar sistemlerinden bilgisayar ağ özelliklerine, iletişim ve internet teknolojilerine ilişkin gerekli bütün önlemler alınmalıdır. Bu teknik konular başlı başına yeterli olmamakla birlikte kuruluşun bazı düzenlemelere ihtiyacı vardır. Bunların başında fiziksel ve çevresel önlemler ve insan kaynakları biriminin çalışan görevliler üzerindeki çalışmaları gelir. Yaşadığımız çağda bilgi güvenliğinin ön plana çıkmasının ve ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemlerinin geliştirilmesinin bu kadar önem arz etmesinde "internet" in gözle görülür bir etkisi vardır. Çünkü internet sayesinde bütün bilgilere erişim ve paylaşım kolaylaşmıştır.



Şekil 2. Bilgi Güvenliği Kavramları.

Bilgi güvenliğinin kurumlara sayısız faydaları vardır. Bu faydaları şu şekilde belirtebiliriz (Çubukçu, 2018, s. 4):

- Bilgileri kurum içinde saklamak, yetkili erişimlere izin vermek,
- Bilgi güvenliği ihlallerini önlemek,
- Siber saldırı risklerinden korunmak,
- Rakiplerine üstünlük sağlamak,
- İş sürekliliği sağlamak,
- Teknolojik aletlerin verimli kullanmasını sağlamak,
- Ortaklar, tedarikçiler ve üçüncü şahıslara güven sağlamak,
- Yasal açıdan sorunsuz varlığını sürdürmek.

Bu şartlarda bilgi güvenliğini sağlamak kuruma birçok fırsat sağlayacaktır. Bilgi güvenliği sağlamanın kurumlar için en doğru yolu ISO/IEC 27001 standardı ve bu standartın yönetim sistemi olan Bilgi Güvenliği Yönetim Sistemini (BGYS) kurmaktır. Bilgi varlıklarının saptanması, risk değerlemesi için önlemler alınması, denetimler yapılması ve iyileştirmeler sonucunda bilgi güvenliğinin sağlanacağı düşünülür. Bilgi güvenliği sadece bilgisayar uzmanları tarafından değil bütün kurum çalışanları tarafından sağlanır (Çubukçu, 2018, s. 5).

Bilgi güvenliği, Gizlilik (Confidentiality), Bütünlük (Integrity), Kullanılabilirlik/Erişilebilirlik (Availability) prensiplerinin yeterli seviyede olması ile mümkündür. Bu üç bileşen birbirinden ayrı düşünülemez. Bilginin gizliliği bilginin erişilebilirliğini engellememelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de bozulmaması gereklidir. Eğer gizlilik sağlanıyor, erişimde sıkıntılar var ise bu bilgi kullanılamayacağından değer görmeyecektir. Bilgiye erişim var fakat bütünlük sağlanmıyor ise kurumlar ve kişiler açısından hatalı, eksik bilgi oluşturacağından istenmeyen sonuçlara neden olabilir. Bu sebeple bilgi güvenliği, bu üç faktörün birlikte sağlanmasını gerektirir. (Doğantimur, 2009, s. 7).

Şekil 3. Bilgi Güvenliğinin Üç Ana Bileşeni.

Gizlilik (Confidentiality): Bilginin yetki verilmemiş sistemler ve kişilerce erişilmemesi veya bilginin erişim sorumluluğu olmayan kişilerce açığa çıkarılmasının engellenmesidir (Güngör, 2015, s. 8). Bilginin ne derece gizli olduğuna, kurumun bilgi güvenliği yönetim sistemi uygulama sürecinde yapılacak olan risk analizine göre, kanun ve anlaşma gibi gerekçelere göre belirlemek gereklidir. Kurumlarda gizlilik prensibinin sağlanması için, bilginin gizlilik seviyesinin ve bunun için yapılması gerekenlerin açıkça belirtilmesi gerekmektedir (Ganbat, 2013, s. 4). Bilgi gizliliğinin sağlanması bazı önlemlerin alınmasıyla gerçekleştirilebilir. Bu önlemler:

- Bilginin gruplandırılması,
- Güvenli belge alanı,
- Güvenlik tedbirlerine uyulması,
- Bilgi saklama görevlileri ve son kullanıcıların eğitimi (Whitman & Mattord, 2014, s. 23).

Bütünlük (Integrity): Bütünlük, kasıtlı ya da kazara, bilginin izinsiz olarak içeriğinin değiştirilmesi, bozulması ve silinmesi tehlikesine karşı içeriğinin korunması anlamına gelmektedir (Güngör, 2015, s. 8). Bu amaçla önemli bilgi için erişim kontrolünün sağlanması ve belirlenen aralıklarla bilgi yedeklemenin yapılması gereklidir. Bu

bağlamda veri, değiştirilmemiş, yeni eklemeler yapılmamış, bir kısmı ya da hepsi tekrarlanmamış ve yerleri değiştirilmemiş şekilde alıcısına ulaşır. Bütünlük ilkesindeki önemli nokta, bilginin değiştirilmemesi değil, izinsiz değiştirilmesine engel olmak ve değişiklik sağlandığında bundan haberdar olunabilmektir (Başaranoğlu, 2016).

Kullanılabilirlik/Erişilebilirlik (Availability): Bilginin, erişilmek istenen süre zarfında ulaşılmasını ve kullanılmasını, erişimin tam ve sorunsuz yapılmasını sağlayan prensiptir. Erişilebilirlik ilkesi sayesinde, kullanıcılar, erişim yetkilerinin izin verdiği müddetçe, veri özelliğini yitirmeden, istenildiği anda ve güvenilir bir şekilde ulaşabilirler (Başaranoğlu, 2016). Bilginin istenilen zamanda ulaşılamaz olması erişilebilirliğe zarar verir. Kurumsal olarak iş sürekliliğinin sağlanması erişebilirlik ilkesine bağlıdır (Boşal, 2017, s. 11).

Bu üç ilkenin dışında bilgi güvenliğini destekleyen faktörler de vardır. Bunlar; hesap verebilirlik (accountability), erişim denetimi (access control), güvenilirlik (reliability) ve emniyet (safety)' tir. Bu faktörler bir takım çalışmalarda bilgi güvenliği ilkeleri olarak belirtilmektedir. Doğruluk ve inkâr edilemezlik faktörleri ise elektronik ticaretin artmasıyla kendiliğinden ortaya çıkmıştır (Güngör, 2015, s. 9).

1.3.1. Yazılım Güvenliği

Yazılım güvenliği, kanunlara uyumlu olmalıdır. Kullanılan yazılımların lisanslı olması kanunlara uyumlu olduğunu gösterir. Kurum için gerekli yazılımların sorumlu kişiler tarafından usul ve yöntemine uygun şekilde hazır edilmelidir (Akay, 2014, s. 21).

Günümüzde bir çok hizmet internet üzerinden verilmeye başlamıştır. Bu uygulama ile birlikte yazılım güvenliği kavramının güvenliğinin de sağlanması ortaya çıkmıştır. Bu yazılımlara yönelik ortaya çıkan güvenlik açıkları, bilgi güvenliğine yönelik tehdit oluşturmaktadır (Vural & Sağıroğlu, 2008, s. 191).

Güvenlik açığı oluşmuş yazılımlar kullanıcılar tarafından tercih edilmemektedir. Bu açıklıkların oluşmasını önlemek ve ortadan kaldırmak için "güvenlik" olgusunu göz önünde bulundurmalıyız (Beydağlı, Kara, Bahşi, & Alparslan, 2009, s. 17).

Bu sebeple kurumlar lisanslı yazılım kullanmalı, lisanssız yazılım kullanımı engellenmelidir. T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi

Toplumu Dairesi'nin "e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi" ve tüm yayınları kurum tarafından dikkate alınmalıdır. (Yıldız B. , 2007, s. 73).

1.3.2. Ağ ve Donanım Güvenliği

Ağ (Network), yan yana ya da uzak iki bilgisayarın birbiriyle bağlantılı olmasıdır. Bu bilgisayarlar arasındaki iletişim (paylaşım, uzak erişim vs.) güvenlik ihlallerini de beraberinde getirir. Bilgisayar ağlarının çoğalmasıyla bilgi güvenliğine yönelik alınan tedbirlerde artmıştır (Gülmüş, 2010, s. 30).

Şifresiz yayın yapan veya güvenilir olduğu kesin olmayan kablosuz ağlar, bilgi güvenliği bakımından ciddi riskler taşımaktadırlar. Kötü niyetli kişiler bu ağlar sayesinde bilgisayarlara girerek verileri ele geçirebilmektedirler. Bu tehlikenin önüne geçmek mümkün değildir. Bu bağlamda mümkün olduğu kadar bu ağlardan faydalanılmamalıdır (Çontar, 2013, s. 115).

Donanım güvenliği, bilişim sistemin dahilinde donanım ve ağların korunup, doğru kullanılmasına dair güvenlik önlemlerini kapsar. Donanım güvenliği diğer güvenlik önlemleri ile bağlantılıdır. Bir donanımın güvenliği fiziki güvenlik, çalışan güvenliği politikaları ile sağlanabildiği gibi sadece donanımsal güvenlik politikaları ile de korunabilir (Adak, Çakır, & Tuğ, 2014, s. 14).

Donanım güvenliği için, kurumdaki cihazlar sürekliliğin sağlanması amacıyla sürekli yedeklenmelidir. Taşınabilir yada cihazlardaki veri depolama ve kayıt aygıtları yetkili çalışan harici kullanılmamalıdır. Kullanılan cihazların bakım ve onarımı sorumlular dahilinde usulüne uygun olarak yapılmalıdır. Yeni alınan ve arızaya çıkan donanımın kontrolleri yapılarak sisteme giriş çıkışı sağlanmalıdır (Akay, 2014, s. 22).

Kurum bilgilerinin gizlilik, bütünlük ve erişebilirliğinin tehlikeye gireceği durumları önlemek için kurum içi güvenlik kültürünün benimsenmesi ve bu duruma göre gerekli bilgi güvenliği standartı ve prosedürlerinin hayata geçirilmesi gerekmektedir (Muharremoğlu, 2013, s. 42-43).

1.3.3. İnternet Güvenliği

Bulunduğumuz çağda kağıt üzerinde yapılan işlemlerin bir çoğu internet aracılığı ile elektronik iletişim ağları üzerinden gerçekleşmektedir. Ancak internetin bu kolaylığı yanında birçok güvenlik problemini de beraberinde getirdiği görülmektedir. Bu sebeple internet ortamının da bazı güvenlik kurallarına tabi olması gerekmektedir. Bu güvenlik kurallarına uyulmaması durumunda devlet tarafından cezai yaptırımlar uygulanacaktır (Gencer, 2015, s. 3). Kişi ve kuruluşların verilerini dış dünyayla paylaşabilmeleri bilgi güvenliği ile alakalıdır. Yasaklı siteler ve uygulamalara ilgili gerekli kısıtlamalar getirilmelidir. Sanal ortamda yaptığımız bütün işlemlerin sistem tarafından kayıt edildiğini ve bu sanal hareketliliğin kişileri ilgilendirdiğini kullanıcılara bildirmek gereklidir.

1.3.4. Kullanıcı Hesabı Güvenliği

Çalışanların kurum bilgisayarlarını bir kullanıcı hesabı ile kullanmaları gerekmektedir. Buna göre bilgisayarı kullanan kişilerin sergilemiş oldukları hareketlerin raporlanması sağlanmış olur. Kullanıcı şifreleri eşsiz ve güçlü olmalıdır. Bu bağlamda kullanıcının yaptığı işlemlerin kendi sorumluluğunda olduğu vurgulanır.

Kullanıcı hesabı güvenilirliğini sağlamak için;

- Tek kullanıcı adı ile bir oturum açılmasına müsaade edilmeli, ikinci bir oturum açılmamalıdır,
- Kullanıcı oturumu kapattıktan sonra çerezler (cookie), kullanıcı ve sunucu tarafından silinmelidir,
- İnsan faktörü baz alınarak kullanıcıların güvenli çıkış yerine tarayıcı sayfasını kapatabileceği olasılığı düşünülmeli,
- Şifremi unuttum aracılığıyla gönderilen elektronik postada, kullanıcının özel bilgileri olmamalı; kullanıcı giriş işleminden sonra bilgilerini görüntüleyebilmeli ve gerekli değişimi sağlayabilmelidir,
- Sistemde belli bir süre işlem yapmayan kullanıcılar, sistem dışına otomatik bir şekilde çıkarılmalıdır,
- Uzun bir süre sisteme giriş yapmayan kullanıcıların, bu kullanıcı adları askıya alınmalıdır (Altun, 2014, s. 27-28-29).

1.3.5. Şifreleme Güvenliği

Günümüzde kurumların ilk savunma hattının çalışanlardan oluştuğu ve bilgi güvenliğinin başında güvenli şifre kullanımının geldiği kabul edilen bir gerçektir. Buna rağmen bir çok kurum şifre kaynaklı siber saldırıların hedefi haline gelmektedir. Kurumlardaki şifreleme güvenliği ile ilgili en büyük hata, çalışanların kişisel ve kurumsal hesaplarda aynı kullanıcı adı ve şifreleri kullanmaları ve birbirleriyle paylaşmalarından kaynaklanmaktadır (cybermag, 2018).

Tüm hesapların özellikle perakende, finans, seyahat ve devlet kurumlarına ait hesapların güçlü ve eşsiz şifrelerle korunması gereklidir. Aynı şifrenin birden fazla hesapta kullanılmaması gerekmektedir. Güçlü bir şifre en az 8 karakterden, büyük, küçük harf, rakam ve özel karakterden oluşmalıdır. Şifrelerin yılda en az iki kez güncellenmesi gerekmektedir. Sözlükte yer alan kelimeler ve kişisel bilgilerimiz şifre olarak kullanılmamalıdır. Kurumun verdiği ilk şifreler hemen değiştirilmelidir. Şifreler herkesin görebileceği bir ortamda (kağıt yada elektronik) bulunmamalıdır. İnternet tarayıcılarının şifre saklama istekleri kabul edilmemelidir.

1.3.6. İnsan Kaynakları Güvenliği

ISO/IEC 27001 çalışanların olası BGYS tehlikelerinden haberdar olmasını ve bu tehlikeler için gereken kontrollerin sistemde tanımlanmasını istemektedir. Standardın Ek A.7 maddesi bu konuda A.7.1 İstihdam Öncesi, A.7.2 Çalışma Esnasında, A.7.3 İstihdamın Sonlandırılması ve Değiştirilmesi çerçevesinde incelemektedir. İstihdam öncesi, çalışanların sorumluluklarını ve rollerini kavramaları sağlanmalıdır. Çalışma esnasında, çalışanların politika ve prosedürleri çerçevesinde bilgi güvenliğini uygulamaları istenmektedir. İstihdamın sonlandırılması ve değiştirilmesinden sonra geçerli bilgi güvenliği sorumlulukları ve görevleri tanımlanmalıdır (Kum Eğitim Danışmanlık, 2019).

1.4. BİLGİ GÜVENLİĞİNİN SAĞLANMASI

Bir kurumda bilgi güvenliğini kazandırmada güvenlik politikaları ve standartlarının çok önemli bir yeri vardır. Güvenlik politikaları üst yönetimce onaylanan, kullanıcılar tarafından sürdürülebilir ve açık olmalıdır. Kurum kültürüyle örtüşen ve herkes tarafından kabul edilen güvenlik politikaları olmaksızın bilgi güvenliğinin sağlanması ve yönetilmesi çok zordur (Tekerek, 2008, s. 132).

Bulunduğumuz çağda kişi ve örgütler üzerinde ciddi zararlara yol açan, bilgi ve bilgisayar güvenliğini tehdit eden çeşitli saldırılar bulunmaktadır. Bu zararların minimum düzeyde tutulması için bilgi güvenliğine yönelik önlemlerin alınması kaçınılmazdır. (Vural, Yılmaz; Sağıroğlu, Şeref, 2007, s. 198). Eğitim, teknoloji, insan faktörü gibi birçok unsur göz önünde bulundurulup, önlemlerin alındığı, kontrollerin sağlandığı zaman bilgi güvenliği güvence altına alınmış olur. Bilgi güvenliğine dair alınması gereken önlemler 3 başlık altında toplanmıştır. Bunlar:

1. Yönetsel önlemler
2. Teknolojik önlemler
3. Eğitim
4. Fiziksel ve çevresel önlemler

Bilgi güvenliği yönetim, teknoloji ve eğitim bağlamında süreklilik arzeden bu üç unsurun birbirini tamamlayamadığı sürece başarılı bir güvenlikten bahsetmenin mümkün olmayacağı bir süreçtir. Bu önlemlerin her biri birbiriyle hatasız çalışmalıdır ki, başarıya ulaşılabilsin (Doğantimur, 2009, s. 22).

Şekil 4. Bilgi Güvenliğinin Sağlanması.

1.4.1. Yönetsel Önlemler

Yönetsel önlemler güvenlik yönetimi ile ilgili politikaların, yöntemlerin, standartların ve süreçlerin belirlenmesi, belgelendirilerek ve üst yönetim tarafından onaylanmasını içerir. Bilgi güvenliğinin yöneticilerden son kullanıcıya kadar kurumdaki herkesin

sorumluluğunda olduğu anlatılmalı ve herkes tarafından sahiplenilmelidir. Bilgi güvenliğinin sağlıklı bir şekilde yönetilmesi ve herkes tarafından uygulanması için olmazsa olmaz şart üst yönetim desteğidir (Örnek, 2003 , s. 43). Yönetimin belirlediği güvenlik politikaları yazılı hale getirilmeli; çalışanlara, iş ortaklarına ve paydaşlara aktarılmalı ve bu konuda gerekli bilinç oluşturulmalıdır (Doğantimur, 2009, s. 23).

Kurumlarda "bilmesi gerektiği kadar, en az yetki, erişmesi gerektiği kadar" gibi belirlenen ilkelere herkesten önce yöneticilerin uyması gerekse de bu ilkelerin en az uygulandığı ve tehlikeli olayların yaşandığı grup yöneticilerdir. Çünkü kuruma dair gizli bilgileri ve değerleri kullanan, taşıyan ve kaydedenler çoğunlukla yöneticiler olmaktadır (Tipton & Krause, 2007). Bilgi güvenliğinin üst yönetimce önemsendiği bazı kurumlarda hataların genelde aceleci ve gün kurtarıcı çözümlerle halledildiğine değinerek hataların teknolojik açıdan çözülebileceği yanılgısına düşmüşlerdir (Richardson, 2008, s. 28).

Kurumun değerlerinin korunması mevzubahis olduğunda risklerin bilinir ve yönetilir olmasına gayret gösterilmelidir. Bu, iş ve bilgi güvenliği risklerini ortaya koyma ve yorumlamayı aynı zamanda kontrol mekanizmalarının etkin bir şekilde uygulanmasını, takibini, etkin kontrollerin sürdürülebilirliğini aksi takdirde geliştirilmesini içerir. Özetle kurumların değerlerini koruyacak bir bilgi güvenliği yönetim süreci olmalıdır (Humphreys, 2008, s. 248).

Yönetsel önlemler kapsamında;

- Risk yönetimi,
- Güvenlik politikaları,
- Standartlar, yönergeler ve prosedürler,
- Güvenlik denetimleri oluşturulmalıdır (Yıldız M. , 2014, s. 63).

1.4.2. Teknolojik Önlemler

İnsan unsuru göz önünde bulundurulduğunda her alanda olduğu gibi bilgi güvenliği alanında da tam anlamıyla bir güvenlikten bahsetmek doğru olmayacaktır. Yazılım, donanım ve sistem ile ilgili alınacak tüm teknolojik önlemler kurum değerlerinin korunmasına yardımcı olacaktır (Gencer, 2015, s. 1). Bilgi güvenliğinin önemli bir

kısmı elektronik ortamdaki bilgilerin saklanmasını içermektedir. Teknolojik önlemler, elektronik ortamdaki bilgilerin korunmasını gerektirir (Doğantimur, 2009, s. 32).

Teknolojik alt yapının bilgi güvenliğini sağlayabilecek şekilde oluşturulması, güvenlik duvarı, şifreleme, anti virüs yazılımları, yedekleme, denetim gibi teknik içerikli çözümleri kapsayan teknolojik önlem süreçlerini içermektedir (Irmak & Baz, 23-25 Ağustos 2019, s. 339).

1.4.3. Eğitim ve Farkındalık

Bilgi güvenliğinde birçok unsurun birbirleriyle bağlantılı olduğu düşünüldüğünde en zayıf halka olarak insan faktörü söylenebilir. Bu sebeple insan faktörünün geliştirilmesi, sadece eğitim kurumlarında kazandırılacak bir takım eğitim ve beceriler olarak düşünülmemelidir. Özellikle yetişkinlerinde teknoloji ile haşır neşir olduğu bu dönemde her kesimden insanların bu konuyla ilgili farkındalıklarını artırmak için yaşam boyu öğrenme programları düzenlemek, kamu spotları hazırlamak, kurslar ve konferanslar düzenlemek farkındalık adına göz önünde bulundurulması gereken önemli noktalardır (Seferoglu, Karaoğlan Yılmaz, Yildiz- Durak, & Yılmaz, October 2018, s. 40).

Bilgi güvenliğinin sağlanması için kurum dışından gelebilecek tehlikeleri önlemek ne kadar gerekliyse kurum içinde oluşabilecek tehlikeler içinde gerekli önlemleri almak o kadar önemlidir. Kurumdaki en büyük risk kaynağı çalışandır. Kuruma kasten verilen zararları engellemek için öncelikle güvenilen kişilerle çalışmak olmalıdır. Bununla beraber yeteri kadar bilgili olmayan çalışandan kaynaklanan hataları en aza indirebilmek için eğitim farkındalık çalışmalarını kurum içinde belirli aralıklarla yapılması gerekmektedir. Ayrıca bilgi güvenliği bilincinin oluşturulmasında cezalar, yasaklar ve caydırıcı kuralların yanında çalışanları bilgi güvenliğine teşvik edecek ödüllendirme sistemleri de oluşturulmalıdır (Eminağaoğlu & Yılmaz, 2009, s. 9-10-11).

Mitnick ve Simon; çalışan bilgi güvenliğinin sadece teknolojik aletlerle sağlanabileceğini düşünerek yanılmaktadır. Kurumlarda verilen farkındalık oluşturma eğitimlerinin birincil amacı çalışanlarda kurum güvenliğine katkı sağlayacağının bilincini kazandırmaktır. Mitnick ve Simon, kurumun değerlerinin korunmasının,

sadece kuruma değil çalışanlara da kazanç sağlayacağını vurgulamıştır. Çünkü kurum, çalışanla ilgili makul bilgilere sahiptir (Mitnick & Simon, 2016, s. 231).

Wenger, Metzger ve Dunn yaptıkları çalışmada kurum çalışanlarına bilgi değerlerinin nasıl ve neden korunmasını öğrenmeleri hususunda eğitim verilmesini savunmuşlardır. Böylece çalışanlar hatalı davranışların doğuracağı sonuçların bilgi güvenliğini nasıl etkileyeceğini fark etmiş olacaklardır. (Wenger, Mauer, & Cavelty, 2008).

Eğitimler, her kurum çalışanına aynı formda ve içerikte sunulduğunda beklenen neticeye ulaşılamamıştır. Eğitim düzenlenmeden önce çalışanların gruplandırılarak her gruba özgü anlatım ve içerik belirlemek daha iyi sonuçlar alınmasını sağlar. Bu bağlamda insandan kaynaklanan güvenlik riski hiç bir zaman ortadan kaldırılamaz ama akıllıca koordine edilmiş bir eğitimle bu risk alt seviyelere çekilebilir (Doğantimur, 2009, s. 42).

1.4.4. Fiziksel ve Çevresel Önlemler

Fiziksel ve çevresel güvenlik, bilgi güvenliğinde özellikle bilgisayar sistemleri, sistem odası, önemli alanlar ve odaların sadece yetkili kişilerce girişlerini ve doğal afetlere karşı alınması gereken önlemleri içerir (Çubukçu, 2018, s. 16).

Belirli fiziksel güvenlik tehlikeleri:

- Sabotaj,
- Elektrik kesintisi,
- Su baskını,
- Deprem,
- Zehirli maddeler,
- Aşırı sıcak ve nem,
- Duman vs. (Çubukçu, 2018, s. 17).

Fiziksel güvenliğin uygulanması için kurumsal prosedür ve tedbirlere ihtiyaç vardır. Fiziksel güvenlik ilkeleri, bilgi kaynakları ve varlıklarının kullanımına kılavuzluk edecek nitelikte olmalıdır. Fiziksel güvenlik önlemleri farklı katmanlarda oluşturulmalı ve gerçekleştirilmelidir (Boşal, 2017, s. 89).

1.5. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

İletişim araçlarının çoğalması ve her kesimden kullanımının artması dolayısıyla bilgi güvenliği kavramının kazandırılması ihtiyacı artarak devam etmiştir. Şifreleme, güvenlik duvarı, donanım ve yazılım vb. teknik önlemlerle bilgi güvenliğinin oluşturulamayacağı görülmüştür. Bu sebeple teknik önlemlere ek olarak insanları, süreçleri ve bilgi sistemlerini de kapsayan ve üst yönetimin desteklediği bir yönetim sisteminin gerekliliği ortaya çıkmıştır (Yılmaz H. , 2014, s. 51).

Bilginin gizliliğini, bütünlüğünü ve sürekli kullanılabilirliğini (erişilebilirliğini) sağlamak üzere sistemli, kurallı, planlı, yönetilebilen, sürdürülebilen, dokümante edilmiş, üst yönetim tarafından kabul edilmiş ve uluslararası güvenlik standartlarını uygulayan faaliyetler bütününe Bilgi Güvenliği Yönetim Sistemi (BGYS) denilmektedir (Ersoy, 2012, s. 8-9).

Kuruluşların en yüksek seviyede bilgi güvenliğini ve iş sürekliliğini edinmeleri için, teknik önlemlere ek olarak teknik olmayan; insan faktörü, prosedürel faktörler, vb. önlemlerin ve denetimlerin alınması, sürekliliğinin sağlanması ve üst yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini içeren standartın gereklerine uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları gerekmektedir (Vural, Yılmaz; Sağıroğlu, Şeref, 2007, s. 196).

Kurumlar günümüzde iş süreçlerini, bilgi kaynaklarını ve iletişim sistemlerini çoğunlukla elektronik ortamlarda gerçekleştirmektedirler. Kurumlarda iş süreçlerinin hızlandırılması, yüksek kalite ve etkin denetimin yapılması bilgi teknolojilerinin kullanılmasıyla sağlanarak toplam etkinliğin yükseltilmesi amaçlanır. Ancak teknolojik alt yapıda ve bilgi kaynaklarına ulaşmada yaşanacak aksilikler iş süreçlerinde ve kurumsal güvenlikte aksaklıklara sebep olacaktır. Bu durum çalışanların ve müşterilerin güvenini olumsuz etkileyecektir. Bu noktada, bilgi güvenliği yönetimi kurumlarda bir sistem olarak kurulmalıdır. Ayrıca kurumsal ve toplum olarak bilgi güvenliği bilincinin oluşturulması da büyük önem arz etmektedir (İleri, 2016, s. 55-56).

Bilgi güvenliği yönetiminde amaç; olayları gerçekleşmeden önce tahmin edebilmek ve gerekli önlemleri almak, önlenemeyen durumlarda ise, minimum zararla en yakın zamanda normal çalışma şartlarına dönebilmektir. Bu durumda, süreçlerin etkili bir

şekilde uygulanması için kurumun belli bir bilgi, kültür ve yetkinliği sağlaması gerekmektedir. Ayrıca, oluşturulacak bilgi güvenliği yönetim sürecinin usul ve yöntemlerinin oluşturulması, sistemin düzeltici ve geliştirici eylemler ile devamlı eksikliğin giderilmesi, tüm kayıtların tutularak kurumsal bilgi güvenliği hafızasının ve kültürünün oluşturulması sağlanmalıdır (İleri, 2016, s. 56).

Kurumlarda devamlılığın sağlanması, riskin minimum seviyede tutulması ve hayati bilgilerin ve sistemlerin korunması, BGYS'nin kurumlarda oluşturulmasıyla mümkün olmaktadır. BGYS'nin hayata geçirilmesiyle; oluşabilecek risk ve tehlikelerin önceden tahmin edilip belirlenebilmesi, güvenlik tedbirlerinin düzenlenmesi, kontrollü bir şekilde denetim ve uygulamaların yapılması, gerekli yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması birbirini tamamlayacak şekilde gerçekleştirilir (Vural & Sağıroğlu, 2008, s. 509).

Eren Veysel Ersoy BGYS'nin bir kuruluşa sağladığı faydaları ana hatlarıyla şu şekilde belirtmiştir (Ersoy, 2012, s. 9):

- Tehlike ve risklerin önceden saptanarak geçerli bir risk yönetiminin oluşturulması,
- Kurumsal itibarın korunması, artırılması ve güçlendirilmesi,
- Standarda ve sektöre uyumluluk,
- Güvenlik açısından sektörel rekabette geriye düşmemek,
- Kanun ve yönergelere uymak,
- İş sürekliliğinin sağlanması,
- Riskler karşısında her daim tetikte olma,
- Bilgi kaynaklarına erişimin her daim kontrol altında olması,
- Bilgi sistemlerinin ve bütün varlıkların envanterine sahip olma,
- Çalışanlara, müşterilere ve üçüncü kişilere bilgi güvenliği konusunda farkındalık yaratmak için eğitim verilmesi ve bilgilendirme yapılması,
- Otomatik ve elle kontrol edilen sistemlerde hassas bilgilerin gerektiği gibi kullanılmasını güvence altına almak için kabul edilir bir kontrol sistemi kurulması,
- Bilgi varlıklarının bütünlüğünün ve doğruluğunun sağlanması,

- Bilgi varlıklarının gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması,
- Çalışanların, müşterilerin ve üçüncü kişilerin görevleri başında bilgi sistemlerini art niyetli kullanmalarını engellemek,
- Yetkisiz erişimin engellenmesi,
- Bilişim sistemlerini kullanan çalışanların, kasıtlı ya da bilmeyerek oluşan bilgi kayıpları, güvenlik saldırıları, donanım ve yazılımla alakalı arızalara karşı bilinçlendirilmesi.

Günümüzde yönetim, risk, kontrol ve bilgi güvenliği alanlarında geliştirilmiş uluslararası standartlar ve çerçeveler bulunmaktadır. Bu standartlar sayesinde, artan denetim ihtiyacının daha objektif ve güvenilir bir şekilde gerçekleşmesi amaçlanır. Belirtilen standart ve uygulamalardan bazıları bilgi sistemleri üzerinden oluşturulan bilgi güvenliğine değinirken, bazıları da işletme ve kullanıcılar için bilgi sistemlerinin az riskli olmasını ve kurumların iş süreçlerine paralel olmasını hedeflemiştir. Bu bağlamda en çok kullanılan standart çerçeveler COBIT, ISO/IEC 27000 Standart Serisi, ITIL olarak sayılabilir (Yıldırım, 2017, s. 6).

Bilgi toplumu olma yolunda devam etmek ve bilişim alanında diğer ülkelerle bütünleşebilmek gibi bir amacımız olacaksa bilgi güvenliği konusuna önem vermemiz gerekmektedir. Bunun için uluslararası bilgi güvenliği standartlarının bütün kuruluşlarda, organizasyonlarda kullanımına gayret göstermeliyiz.

1.5.1. Information Technologies Infrastructure Library (ITIL)

1990'ların başında İngiliz Birleşik Krallık Central Computer and Telecommunications Agency (CCTA) tarafından oluşturulan, Information Technologies Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi) sözlerinin baş harflerinden oluşmuş ITIL, karmaşık bir iş yönetimi ile ilgili en doğru sonuçları almak için, karışık bir bilgi teknolojisi yapılanmasında nasıl organize olacağımızı ve yönetmeyi içeren sektör liderlerinin görüşlerini içeren bir dizi kitabın kütüphanesidir (Alpay, 2008, s. 1).

ITIL, BT servislerindeki hizmet seviyesi kalitesinin yükselmesi, erişebilirliğin artması, yerinde kapasite planlaması ile maliyetlerin kontrol altına alınması gibi gözle görülür bir iyileşme elde edilmesinden ötürü kütüphane olmaktan çıkıp BT yönetim metodolojisi olmuştur (Ergen, 2010).ITIL, büyük veya küçük bütün işletmelere

uygulanabilen bilgi sistemlerinde verimlilik ve etkinlik sağlamayı hedefleyen bir yaklaşım sunar. ITIL benimseyen kuruluşlar aşağıda belirtilen amaçları hedefler;

- Maliyetleri Düşürmek,
- Erişilebilirliği Arttırmak,
- Kapasiteyi Ayarlamak,
- İş Gücünü Arttırmak,
- Kaynakların Verimli Kullanılmasını Sağlamak,
- Ölçeklenebilirliği Arttırmak,
- Yüksek Kalitede BT Hizmeti vermek (Yıldırım, 2017, s. 15).

ITIL süreçleri, yaklaşımları, görevleri, süreç ve faaliyetleri tanımlar; fakat bunların ne şekilde uygulanması gerektiğini açıklamaz. Daha çok pratiğe dayalı yapısıyla, dünyada normalde standart olarak benimsenen bu sürecin sonunda sertifika alınmaz ve resmi denetimler yapılmaz. Belli bir iş kolu için hazırlanmayan ITIL, bütün sektörlerin bilgi işlem grupları tarafından uygulanabilmektedir (Hacısüleymanoğlu, 2010, s. 10).

Şekil 5. ITIL Yapısına Genel Bakış (Yılmaz M. , 2018, s. 20).

Hizmet Seviyesi Yönetimi(Service Level Management) adındaki ilk ITIL kitabı 1989 yılında çıkarılmıştır. Sonra sırayla Servis Masası, Süreç Yönetimi ve Değişiklik Yönetimi kitapları yayımlanmıştır. 2001 yılında ITIL V2, 2007 yılında ITIL V3 sürümü yayınlanmıştır. Üçüncü Sürüm aşağıdaki 5 ana bölümden oluşur (Demirok, 2016, s. 21):

- Hizmet Stratejisi (Service Strategy)
- Hizmet Tasarımı (Service Design)
- Hizmet Geçişi (Service Transition)
- Hizmet Yönetimi (Service Operation)
- Sürekli Servis Gelişimi (Continual Service Improvement)

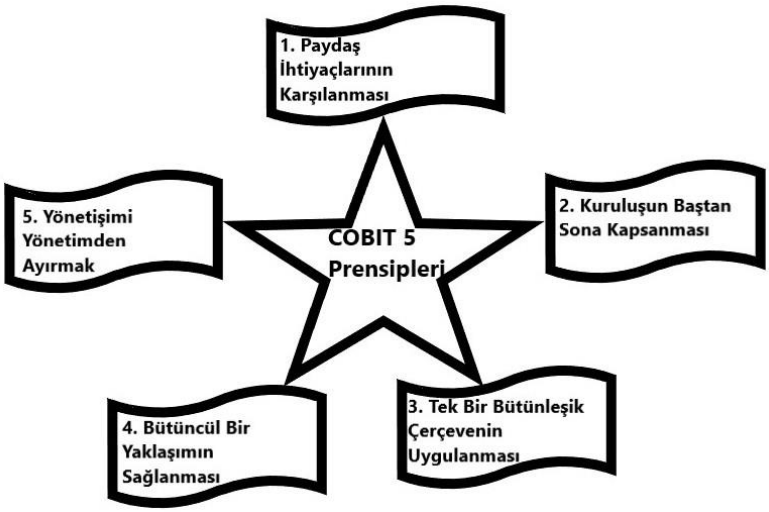
1.5.2. The Control Objectives For Information And Related Technology (Cobit)

Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) tarafından hazırlanan COBIT "Control Objectives for Information and related Technology"nin kısaltılmış halidir. Bilgi Teknolojilerine ilişkin kontrol hedefleri anlamına gelen COBIT, ISO ve ITIL' ı temel alan, kendini yenileyen, gelişen teknolojiyle beraber yeni versiyonları ile fayda sağlayan bir sistemdir (Akay, 2014, s. 30). Aynı zamanda bilgi sistemlerinin karşı karşıya kaldıkları riskleri, bu risklerin yorumlanması, yönetilmesi ve risklere karşı kontrolleri ve bu kontrollerin denetlenme usulleri üzerinde de duran bir bakış açısı ile hazırlanmış bir yapıya sahiptir (Yıldırım, 2017, s. 7).

COBIT, kontrole dayalı bir yaklaşım olmasından ötürü sunulan hizmetlerin belirtilen kalite, güvenlik ve hukuksal ihtiyaçlara cevap vermesini sağlayan bir yaklaşımdır. Bu sebeple bunların nasıl yapılacağı ile ilgilenmezken neler yapılacağına odaklanır (Yıldırım, 2017, s. 8). COBIT, ilk zamanlar denetim, kontrol, sonra yönetim, en son risk ve katma değer ile ilgili standartları da içine alarak zaman içinde bir bilgi sistemleri yönetişim çerçevesine dönüşmüştür (ISACA, 2012, s. 13).

COBIT ilk olarak 1996 yılında yayımlanmıştır. Bu sürüm genel olarak denetim ile alakalıdır. 1998 yılında yayımlanan ikinci sürüme yönetim rehberi eklenmiştir. 2000 yılında COBIT-3 denetim, kontrol ve yönetim çerçevesinde yeni sürümü yayımlanmıştır. 2005 yılında 4. versiyon, 2007 yılında bilgi teknolojileri yönetişimi

eklenerek güncellenmiştir. 2012 yılında ise kurumsal BT yönetişimi öne çıkarak COBIT-5 versiyonu oluşturulmuştur (Bilgin, 2016, s. 74).



Şekil 6. COBIT' in 5 Temel İlkesi (ISACA, 2012, s. 13).

COBIT-5 beş temel ilkeden oluşur. Bu ilkelere göre birbirini bütünleyen, diğer çerçeve ve standartların yetersiz noktalarını tamamlayan, kurumun devamlılığı için zorunlu alt sistemlerden oluşan dinamik bir sistemin birliğini tanımlamaktadır (ISACA, 2012).

Türkiye'de ise zaman geçtikte değişik sektörlerde ait birçok şirkette COBIT'in kullanıldığını görüyoruz. BDDK, Hazine Müsteşarlığı ve SPK'nın da BT'ye özgü düzenlemelerinde COBIT'i göz önüne aldığı görülmektedir.

1.5.3. ISO/IEC 27000 Standart Serisi

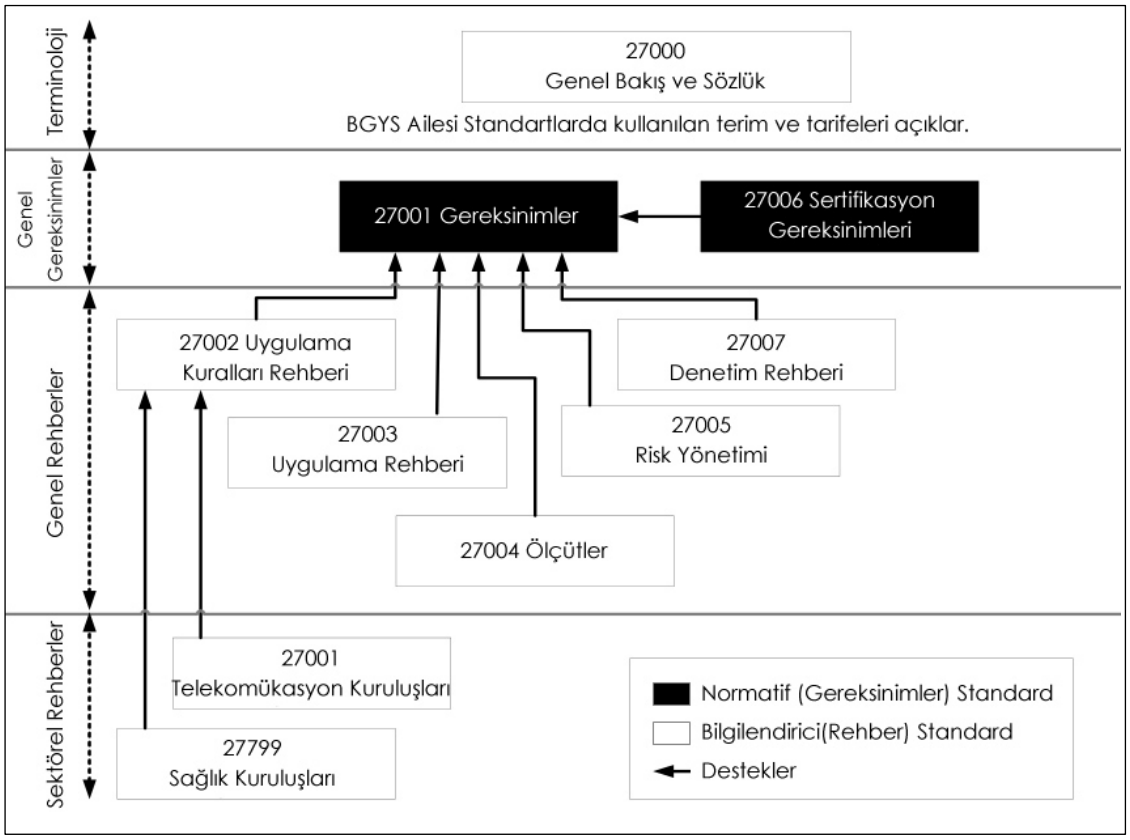
Organizasyonların iş devamlılığını ve etkili bilgi güvenliğini sağlamak için teknik önlemlerle beraber insan faktörü, prosedürel faktörler, eğitim gibi teknik olamayan önlemlerin sağlanması, bu süreçlerin bilgi güvenliği standartlarına uygun olması ve sürekliliğin sağlanması amacıyla Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaları gerekmektedir (Şen & Yerlikaya, 2013). ISO/IEC 27000 ailesi finans, sağlık, savunma, hizmet sektöründeki özel durumlar hariç, haberleşme, bilgi teknolojileri, tasarım, Ar-Ge, üretim gibi ana faaliyet hususlarında kuruluşların ihtiyaçlarını karşılamaktadır (Kılıç & Gökçöl, 2010, s. 1-3). Bilgi güvenliği süreçlerini tam karşılaması, eksik noktaları standart ailesindeki diğer standartlar ile karşılaması bu standart ailesini

popüler kılmaktadır. Ayrıca kapsam belirlemede, karar verme, planlama ve uygulama aşamasında organizasyonlara fayda sağlayacaktır (Perendi, Ünal, 2008, s. 6-7).

ISO/IEC 27000 ailesi standartları, organizasyonların bilgi varlıklarını garanti altına almaları sebebiyle düzenlenmiştir. Bu standartlardan fayda sağlamak, kuruluşların mali bilgiler, fikri mülkiyet hakları, çalışan bilgileri veya üçüncü kişilerin sahip olduğu bilgilerin, varlıkların güvenliğini yönetmek demektir (Çakır & Tuygun, 2019, s. 63).

Uluslararası Standartlar Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) geliştirdiği ISO/IEC 27000 Serisi, bilgi güvenliği yönetimi için global olarak tüm dünyada tanınan bir yapı olarak bilinmektedir. ISO/IEC 27000 standartlar serisi bilgi güvenliğine özgü olsa da en popüler olan standart ISO/IEC 27001'dir (Koç, Şeker, & Şeker, 2019, s. 127).

ISO/IEC 27000 standart serisine dahil olan ve ISO 27001' e ait güvenlik kontrollerinin olduğu standart; ISO/IEC 27002:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenlik Yönetimi için Uygulama Kılavuzu'dur. Bu standart ilk olarak ISO/IEC 17799:2005 adıyla biliniyordu. ISO yaptığı teknik bir düzenlemeyle 1 Temmuz 2007 tarihinde, ISO/IEC 17799:2005 standardının adı, ISO/IEC 27002:2005 (ISO 27002) olarak değiştirilmiştir (Peker, 2008, s. 8).



Şekil 7. ISO/IEC 27000 Standart Ailesi (Yılmaz M. , 2018, s. 34).

27000 ile 27999 arasındaki standartlar bilgi güvenliği standartları olarak belirlenmiştir. ISO 27001 standardından sonra ihtiyaçlar oluşmasından dolayı yeni standartlar eklenmiştir. Sektörlerin bilgi güvenliğine olan gereksinimleri önceden tasarlanarak sonraki standartlar için yer ayrılmıştır. Yeni standartlar için ayrılan yerler genelden özele doğru doldurulmaktadır. Zaman geçtikçe standartlarda eksiklik gözlemlenmiş aynı standart numarası ile yeni ihtiyaçları karşılar nitelikte yeniden hazırlanmıştır. Zamanla oluşan açıklık, ihtiyaçlar ve yeni tehditler bu değişikliklere gidilmesine sebep olmaktadır. Çünkü standartlar etkin, aktif yapılarını muhafaza ettikleri zamana ve güncel tehlikelere karşı ayakta durabilirler (Akay, 2014, s. 39).

- ISO/IEC 27001: Dokümante edilmiş bir bilgi güvenliği yönetim sisteminin kurulması, gerçekleştirilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve iyileştirilmesi için oluşturulmuş bir standarttır.
- ISO/IEC 27002: Güvenliği sağlayabilmek için gerekli kontrollerin bu kontrollerle alakalı iyi uygulamaların olduğu standarttır.

- ISO/IEC 27003: ISO/IEC 27001 ile uyumlu BGYS'nin uygulanması ile ilgili bilgiler içerir.
- ISO/IEC 27004: Bilgi güvenliğinin yönetilmesi ile ilgili ölçüm tekniklerine kılavuzluk eder.
- ISO/IEC 27005: Risk yönetimi ile ilgili standarttır.
- ISO/IEC 27006: ISO/IEC 27001 ile uyumlu BGYS sertifikasyonu ve denetim sağlayan kuruluşların gerekliliklerine kılavuzluk yapar.
- ISO/IEC 27007: BGYS ile ilgili denetimlere ve denetçiler için rehberlik yapar.
- ISO/IEC 27011: Telekomünikasyon kuruluşlarına yönelik bilgi güvenliği standardıdır.
- ISO/IEC 27799: Sağlık kuruluşlarına yönelik bilgi güvenliği standardıdır.

İKİNCİ BÖLÜM: BİLGİ GÜVENLİĞİ STANDARDI

2.1. STANDARDIN TANITIMI

2.1.1. ISO/IEC 27001 Standardın Tanımı ve Önemi

Türkçe adı Bilgi Güvenliği Yönetim Sistemi (BGYS), İngilizce adı Information Security Management System (ISMS) olan ISO/IEC 27001; bilgi güvenliği için oluşturulmuş uluslararası geçerliliği olan bir yönetim sistemi standardıdır. ISO/IEC 27001, ISO – International Standarts Organization (Uluslararası Standart Organizasyonu) ve IEC – International Electrotechnical Commission (Uluslararası Elektrik Komisyonu) çalışmaları sonucu ortaya çıkmış ve böylelikle ISO/IEC ön eki belirlenmiştir. Technical Specification ön ekiyle birlikte TS ISO/IEC 27001 şeklinde adlandırılmıştır (Çubukçu, 2018, s. 20).

ISO'nun kabul ettiği bu standart, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca oluşturulmuş ve ISO/IEC 27001 (2005) standardı baz alınarak, 02 Mart 2006 tarihinde TSE Teknik Kurulu'nun Türk Standardı olarak kabul edilerek yayımına karar verilmiştir (Çiğdem, 2009, s. 53).

Bu standart, bir organizasyonda bilgi güvenliği yönetim sistemi için gerekli olan kurulum, uygulama, sürdürülmesi ve sürekli iyileştirilmesi için zorunlulukları belirlemek amacıyla geliştirilmiştir. Kurum içinden yada dışından art niyetli ve doğru olmayan kullanımlara karşı bilginin muhafaza edilmesi gerekliliklerini tanımlar. TSE tarafından yayınlanma amacı "Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek amacıyla geliştirilmiştir." şeklinde belirtilmiştir (Ersoy, 2012, s. 14-15). Büyük, küçük ve sektör ayırmaksızın (ticari işletmeler, devlet kurumları, kar amacı gütmeyen kuruluşlar, mikro işletmeler, çokuluslu şirketler, perakendecilik, bankacılık, savunma, sağlık, eğitim kurumları vb.) tüm kuruluşların yararlanabilmesi üzerine geliştirilmiştir. (Gündoğan, 2016, s. 20). ISO 27001 ile sadece bilişim güvenliği değil, her türlü sürecin hatta kağıt üstündeki bilgilerin dahi güvenliği sağlanmış olur (Çetinkaya, 2008, s. 512).

Bu belgeye sahip olmanın ayrıcalıklarını şu şekilde sıralayabiliriz (Çubukçu, 2018, s. 21):

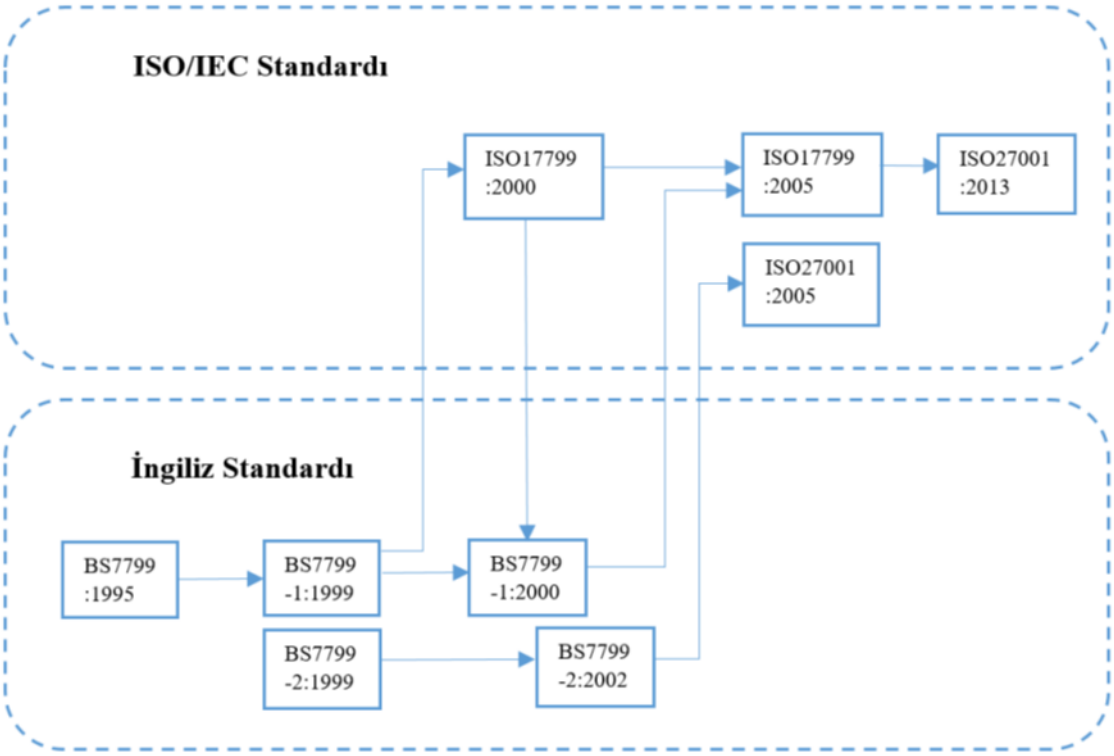
- Dünyanın her yerinde geçerli bir yönetim sistemine sahip olduğunuzun göstergesidir.
- Kurum için korunması gereken bilgisayar, dosyalar, sözleşmeler, e-posta gibi önemli noktaların farkına varmayı ve belirli bir düzende korumayı öngörür.
- Bir afet anında kaybı en aza indirebilmek için iş sürekliliği sağlar.
- Tedarikçi, müşteri ve çalışanların bilgilerinin korunmasını sağlar.
- Siber saldırılar karşısında bilgi varlıkları korunmuş olur.
- Bilgi hırsızlığı, yetkisiz erişimler, yasal durumlar gibi bilgi güvenliğinin ihlal edildiği durumlarda yasal kanıtların hazırlanmasına imkan sağlar.
- Bilgi güvenliğini tehlikeye atacak sistem açıklıklarını ve riskleri azaltır.
- Bilgi güvenliği dahilinde fiziksel ve çevresel güvenlik – yükleme alanları, sistem odaları, özel alanlar koruma altına alınır.
- Daha düzenli ve sistemli bir bilgisayar hizmetleri gerçekleştirilir.
- Bilgilere erişimin ve aktivitelerin kayıt altına alınmasını sağlar.

2.1.2. ISO/IEC 27001 Gelişim Süreci

Bilgi güvenliğinin tarihi BS-7799 olan İngiliz Standardına dayanır. Türk Standartları Enstitüsü (TSE) Teknik Kurulu'nun 11 Kasım 2002 tarihinde almış olduğu kararla bu standardın tercüme edilmiş halini TS ISO/IEC 17799 (Kısım-1) olarak kabul etmiştir. BS 7799-2:2002 olarak yayınlanan ikinci kısım ise, Türk Standartları Enstitüsü Teknik Kurulu'nun 17 Şubat 2005 tarihinde aldığı kararla TS 17799-2 (Kısım-2) olarak kabul edilmiştir. 1993 yılında BS 7799-1 Standardı yayınlandıktan sonra Uluslararası Standartlar Organizasyonu (ISO, The International Organization for Standardization) ve Uluslararası Elektroteknik Komisyonu (IEC, International Electrotechnical Commission) birlikte oluşturdukları komite ile birlikte BS 7799-1 Standardına ek katkılar yaparak 2000 yılında ISO/IEC 17799 Standardını yayınlamışlardır. Bu standart Kısım 1 olarak 10 bölüm, 127 kontrol maddesiyle çalışma kurallarını anlatmaktadır. Kısım 2 olarak yayınlanan Bilgi Güvenliği Yönetim Sistemleri (Information Security Management System- ISMS) gerekleridir. BS 7799-2:2002 olarak yayınlanan bu sürüm BS 7799-2:1999 sürümünü geçersiz bırakmıştır (Ersoy, 2012, s. 12-13).

2005 yılında 7799:2000 standardı ISO (International Standard Organization) içine dahil olmuş ve 27000 grubu içinde numara verilerek ISO/IEC 27001:2005 ortaya çıkmıştır. Bundan sonra ISO/IEC 27001 ve diğer kalite yönetim sistemleri, PUKO döngüsü ve Uygulanabilirlik bildirgesiyle (SOA) uyumlu olmuştur. Ülkemizde ISO 9001 ve ISO 14001 ile uyumlu hale getirilen ISO/IEC 27001:2005 sürümü TSE (Türk Standartları Enstitüsü) tarafından kabul edilmiştir. 8 yıl sonra 1 Ekim 2013 yılında ISO/IEC 27001:2013 versiyonu yayınlanmıştır (Çubukçu, 2018, s. 22).

ISO/IEC 27001:2013 standardı 2017 yılında CEN (Avrupa Standardizasyon Komitesi) tarafından revize edilmiştir. Bu değişiklik ISO tarafından yapılmayıp CEN tarafından Avrupa' da ki düzenlemeler için gerçekleştirilmiş bölgesel bir düzenlemedir. Ancak bu değişiklik ISO tarafından da dikkate alınacağından ISO 27002 ve ISO 27000 standartlarında da yenilik gerçekleştirilmiştir. ISO 27002 kapsamında Varlık Envanteri ve Varlıkların Kabul Edilebilir Kullanımı maddelerinde değişiklikler yapılmıştır (CEN/Cenelec ISO/IEC 27001:2017 Revizyonu, 2020).



Şekil 8. Uluslararası Bilgi Güvenliği Standartları Tarihçesi (Ilgaz, 2018, s. 28).

2.1.3. ISO/IEC 27001 Belgesi ve Zorunlu Olan Kuruluşlar

ISO/IEC 27001, bir organizasyon için alınan bir belge ve sertifikadır. Bir BGYS kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek amacıyla ortaya çıkmıştır (Doğantimur, 2009, s. 12). Bu sertifika, organizasyonlarda bilgi güvenliğinin sağlanmasının bağımsız denetim kurumları tarafından yapılan denetlemeler sonucunda verilir. Üç yıl geçerli olan bu sertifikanın yılda bir kez denetimi olmaktadır. Belgeyi alan kurumlar bu sertifika sayesinde bilgi güvenliği kriterlerini sağladıklarını karşı tarafa kanıtlamış olmaktadırlar (Çubukçu, 2018, s. 25-26).

ISO 27001 Bilgi Güvenliği Yönetim Sistemine sahip olmak, organizasyonun tam anlamıyla güvenlik seviyesine ulaştığı anlamına değil, organizasyonun güvenlik risklerini bilmesi, yönetmesi, belli riskleri yok etmek için kaynak ayırdığı ve harekete geçtiği anlamına gelmektedir (Şen & Yerlikaya, 2013). Zaten güvenlik seviyesinin tam olarak karşılamak mümkün değildir ve standardın bu tür bir amacı da yoktur.

Türkiye' de ISO/IEC 27001 sertifikası Türk Standartları Enstitüsü veya danışmanlık firmalarından edinilebilmektedir. Bu standardı almak için bazı çalışmalar yapılmaktadır. Bu çalışmalar kurum tarafından görevlendirilmiş bilgi işlem yöneticileri, eğer varsa kalite, insan kaynakları ve satın alma gibi bölümlerden görevlendirilmiş kişiler tarafından gerçekleştirilir. Görevlendirilen kişiler hazırlık çalışmalarını planlayıp uygularlar. Bağımsız belgelendirme kuruluşlarına başvuru yapıldıktan sonra gerçekleştirilen denetimin ardından başarılı görüldüğü takdirde belge almaya hak kazanılır (Çubukçu, 2018, s. 26). Akreditasyon kurumundan akredite edilen kuruluşlar ISO/IEC 27001 sertifikasını verebilmektedir. Bu standardın İngiltere' de ki akreditasyon kurumu (United Kingtom Accreditation Service) UKAS' tır. Türkiye' de, 27.10.1999 tarih ve 4457 sayılı kanunu ile kurulan Türk Akreditasyon Kurumu (TURKAK)'tır. Türk Standartları Enstitüsü, TURKAK tarafından akredite edilmiştir. TURKAK, European Co-operation for Accreditation (EA) üyesidir (Ersoy, 2012, s. 18).

Her organizasyonun ISO/IEC 27001 belgesini alması elbette zorunlu değildir. Ama ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesinin bazı kamu ve özel sektörde alınması zorunlu hale getirilmiştir.

Özel sektörde kamu ihale kanuna göre ihale açan kuruluşlar ISO/IEC 27001 belgesini zorunlu kılmaktadır. Proje üst düzeyde gizlilik ve güvenlik gerektiriyorsa bu belge özellikle istenmektedir. Örneğin savunma sanayi ile ilgili ihalelerde, yazılım hizmeti veren ve ürün üretip satış gerçekleştiren kuruluşlardan bu belge istenmektedir. Ayrıca Telekomünikasyon Kurumu tarafından, elektronik haberleşme hizmeti veren ve şebekesi sağlayan kurumların ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alması zorunlu hale getirilmiştir.

Bilgi Teknolojileri ve İletişim Kurumu, TS ISO/IEC 27001 standartı uygulamasına dair bildirisinde (isokalitebelgesi);

- Görev Sözleşmesi İmzalayan kuruluşlar,
- İmtiyaz Sözleşmesi İmzalayan kuruluşlar,
- Uydu Haberleşme Hizmeti sağlayıcıları,
- Altyapı İşletmeciliği Hizmeti sağlayıcıları,
- Sabit Telefon Hizmeti sağlayıcıları,
- GMPCS Mobil Telefon Hizmeti sağlayıcıları,
- Sanal Mobil Şebeke Hizmeti,
- İnternet Servis Sağlayıcıları,
- GSM 1800 Mobil Telefon Hizmeti sağlayan hava taşıtlarında, ISO 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi almak zorundadırlar. Bilgi Teknolojileri ve İletişim Kurumu bu belgenin alınıp sürdürülebilir olmasını istemektedir ve belirli zaman aralıklarında denetimlerle bunu denetlemektedir.

Maliye Bakanlığı Gelir İdaresi Başkanlığı e-fatura uygulama kılavuzunda bilgi güvenliğini sağlamak için ISO/IEC 27001 standardına sahip olmalıdır şeklinde belirtmiştir (isokalitebelgesi). Bu hizmeti verecek kurumların sadece ISO/IEC 27001 belgesini alarak bilgi güvenliği yönetim sistemini kurarak doğru bir şekilde yönetmeleri gerekmektedir.

Kamu kurumlarında ISO/IEC 27001 belgesini almak zorunluluğu yoktur ama bazı kanun ve yasalar gereği ISO 27001 Bilgi Güvenliği Yönetim Sistemini kurmaları zorunlu tutulmuştur.

10.12.2003 tarihli 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunuyla, tüm kamu kurumlarında kamu mali yönetim sistemi uluslararası standartlar ve Avrupa Birliği uygulamalarına uygun olarak düzenlenip etkin bir kontrol sistemi oluşturmak için Maliye Bakanlığı 26.12.2007 tarihinde 26738 sayılı Kamu İç Kontrol Standartları tebliği Resmi Gazete de yayınlanmıştır. Bu tebliğe göre kamu idarelerinde iç kontrol sisteminin oluşturulması, uygulanması, izlenmesi ve geliştirilmesi amacıyla belirtilen 18 standart ve 79 genel şarttan en az 10 tanesi kurumlarda bilgi güvenliği yönetim sisteminin oluşturulması ile ilgilidir.

2003/48 sayılı Başbakanlık Genelgesi ile e-Dönüşüm Türkiye Projesi yürürlüğe girmiştir. Bu projeye göre 4.1.1.' inci maddesinde bütün kurumlarda Bilgi Güvenliği Yönetim Sisteminin (BGYS) kurulmasının amaçlandığı bildirilmektedir.

05/08/2005 tarihli ve 25897 sayılı Resmi Gazete' de yayımlanan, 2005/20 sayılı Başbakanlık Genelgesi gereği Birlikte Çalışabilirlik Esasları Rehberinde elektronik olarak gerçekleştirilen hizmetlerin başarı ve güven ortamında sağlanması için gerekli politika ve düzenlemelere vurgu yapılmıştır.

2006 / 38 sayılı Yüksek Planlama Kurulu Kararı ve 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete' de yayımlanan Bilgi Toplumu Stratejisi Belgesinde bilgi güvenliğinin bütün ülkede ve kamu kurumlarında, bilgi sistemleri, elektronik ve ağ iletişiminde güvenliğin edinilmesi ve sürdürülmesi için gerekli düzenlemelerin gerçekleştirilmesi gerektiği belirtilmiştir. Ayrıca, yasal düzenlemelerin bilgi güvenliği çerçevesinde gerçekleştirileceği de belirtilmektedir (isokalitebelgesi).

10.01.2013 tarihli Resmi Gazetede yayımlanan Gümrük İşlemlerinin Kolaylaştırılması Yönetmeliği gereğince Yetkili Yükümlü Statüsü Sertifikası (YYS)'nı isteyen ihracatçı kuruluşların ISO/IEC 27001 sertifikasını alması zorunlu tutulmuştur. YYS için ISO/IEC 27001 sertifikalarının güncel olması gereklidir. ISO/IEC 27001 belgesi; gümrük ve dış ticaret işlemlerine ilişkin çalışma birimlerini ve bu çalışma birimlerine ait lojistik, depolama, muhasebe, finans ve bilgi işlemin elektronik bilgi varlıkları faaliyetlerini bu varlıkların güvenliğini sağlamayı kapsamalıdır.

2.1.4. ISO/IEC 27001 İçin Gerekli Olan Sistem – BGYS

Ekonomimizin büyük ölçüde bilgiye dayandığı bu çağda kuruluşlar, ekonomide meydana gelen değişiklikleri yakından takip etmek ve güncellenen teknolojiye uyum sağlamak için rakiplerine karşı daha fazla rekabetçi olmaya çalışmaktadır. Ayrıca devamlı değişen teknoloji var olan bilgilerin değişmesine ve geçerliliğinin kaybolmasına sebep olmaktadır. Bu sebeplerle kuruluşlar özgün bilgi kaynaklarını çoğaltmak ve büyük verilerini kısa zamanda etkin bir şekilde işleyip yönetmek durumundadırlar (Aktan & Vural, 2005).

ISO/IEC 27001 standardı, bilgileri korumak ve yönetmek için bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulmasını önerir (Çubukçu, 2018, s. 29). ISO 27001, kurumlara uluslararası kabul görmüş yöntem ve kuruma özgü politika, prosedür, kılavuz oluşturmasını sunar. Aynı zamanda kurumların ISO 27001sertifikasına sahip olması o kurumun güvenliğe önem verdiğini ve bu konuyu ciddiye aldığını göstermektedir. (Özbilgin & Özlü, 2019). BGYS, bilginin bütünlüğünü, gizliliğini ve erişebilirliğini sağlamak üzere yöntemli bir şekilde planlanan, yönetilebilen, sürdürülebilen, belgelendirilen yönetim tarafından kabul edilmiş ve uluslararası güvenlik standartlarının temel alındığı faaliyetlerin tümüdür (Ersoy, 2012, s. 8).

Kuruluşa faydalı bir BGYS'nin dinamik bir şekilde uygulanması gerekmektedir. Kuruluşun iş ve kültürünün sürekli iyileşen devam eden bir yapısı olmalıdır. Çünkü BGYS bunu gerektirir (Kajava, Anttila, Varonen, Savola, & Röning, 2006, s. 2091-2095).

Bilgi güvenliği yönetim sistemi, kuruluş organizasyonunu, politika ve prosedürleri ayrıca kuruluşun iş kültürüyle ayrılmaz bir bütün olan amaçları, hedefleri ve faaliyet alanını kapsamalıdır. Kurumsal süreçlerin ve yönetim yapısının bir parçası olması, bunlarla bütünleşik olması ve bilgi güvenliği süreçlerinin, bilgi sistemlerinin ve kontrollerin planlanmasında göz önünde bulundurulmalıdır. (Gündoğan, 2016, s. 22)

Bir kuruluşta teknik önlemlerle beraber BGYS dahilinde kavramsal ve denetimsel bir takım önlemlerin alınması konusu dünyanın her yerinde kabul görmüş bir yaklaşımdır. Bu yaklaşım üst yönetim, üçüncü kişi - kuruluşlar ve tüm çalışanlar tarafından eksiksiz bir şekilde uygulanmalıdır. Böylece BGYS'nin sadece bilgi işlem ve IT (Information

Technology) bölümlerinin değil tüm kurum birim ve çalışanlarının da görevleri olduğu vurgulanmaktadır (Ersoy, 2012, s. 8-9).

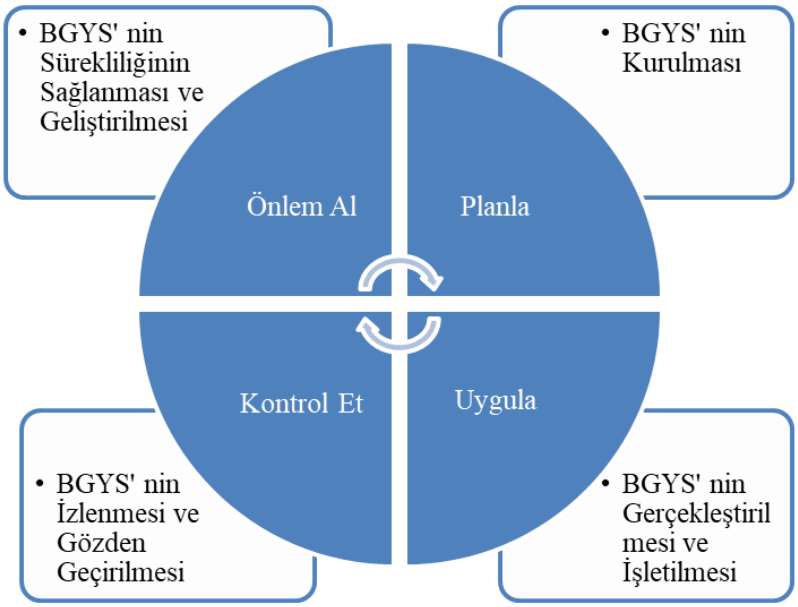
BGYS kurulurken ISO/IEC 27001 gereklilikleri ve ISO/IEC 27002'nin önerileri dikkate alınır. Aynı zamanda güvenlik standartları baz alınarak yapılan bütün çalışmaların dokümante edilmesi ve raporlanması standardın getirdiği bir zorunluluktur. Bir kuruluşta bilgi güvenliği yönetim sistemini kurmak, uygulamak ve bununla ilgili çalışmalar yapabilmek için üst yönetimin karar vermesi gerekmektedir. Bu karar maddi ve insan gücü kaynaklarının atanmasında ve bundan sonraki süreçlerde üst yönetimin bu konuya ve çalışmalara destek verdiğini göstermektedir (Ersoy, 2012, s. 29).

BGYS kurulumu deyince akla bilgi teknolojileri kurulumu gelmemelidir. BGYS kuruluşun iş yapma yöntemini etkileyen bir sistemdir. Bütün bölümlerdeki çalışanlar bilgi güvenliği ilkelerini göz önüne alarak çalışmalarını yürütmek zorundadırlar. BGYS üst kademeden alt kademeye kadar kuruluşun tüm bölümlerinin aktif katılımıyla hedefe ulaşılabilecek bir sistemdir (Aydoğan, 2011, s. 13).

ISO/IEC 27001 belgesini alma sürecinde yapılacak çalışmalar öncelikle kurumun sertifikayı almasına karar vermesi, bu süreç için bir komite oluşturulması, kuruma ait bilgi varlıklarının ortaya konması, risk analizi yapılması ve bir dokümantasyon sisteminin oluşturulması, ardından iç ve dış denetim yapılarak belgenin alınması planlanır.

2.2. STANDARDIN ANA MADDELERİ ve PUKÖ DÖNGÜSÜ

Kuruluş BGYS'yi, gerçekleştirdiği ticari faaliyet ve riskler karşısında, geliştirir, sürdürür ve sürekli ilerletir. Bu bağlamda standard PUKÖ modeline dayanır (TSE, Mart 2006, s. 2). PUKÖ modeli, kurumda ne yapılması gerektiğinin açıkça oluşturulması, kararların uygulanır duruma getirilmesi ve çalıştığının temin edilmesi, amaca uygun olmayan kontroller için gerekli önlemlerin alınmasıdır (Ötegen, 2018, s. 52). Bu süreç yaklaşımı faaliyetlerin tanımlanmasını, izlenmesini ve performansının ölçülmesini kolaylaştırır (Çubukçu, 2018, s. 93).



Şekil 9. PUKÖ Döngüsü (Çubukçu, 2018, s. 95).

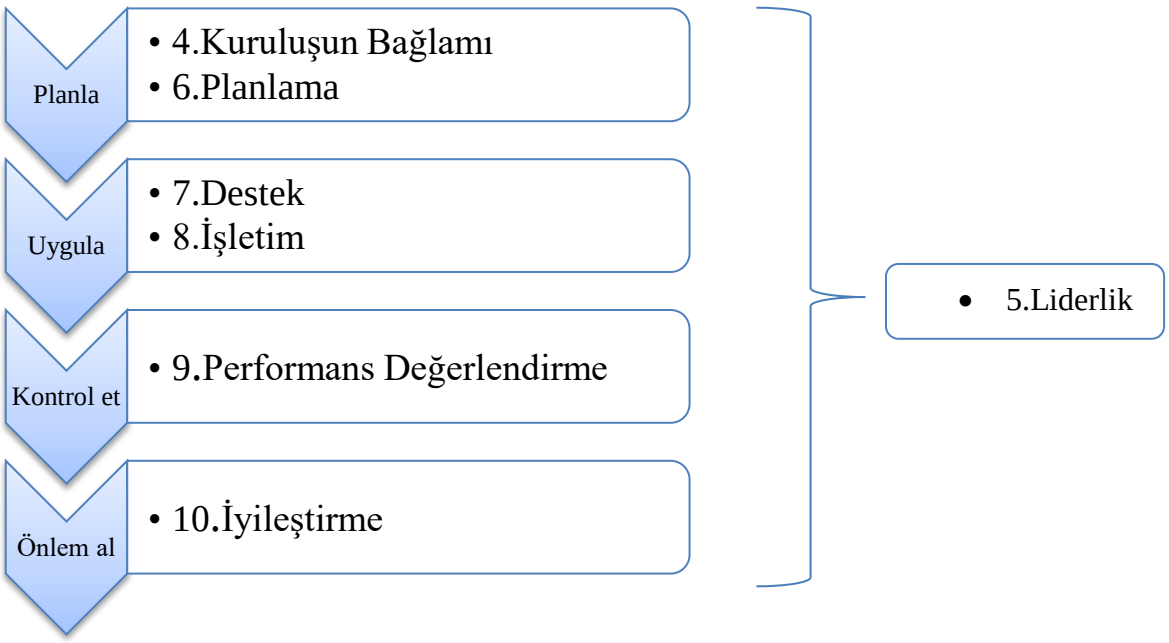
BGYS proseslerine uygulanan PUKÖ modeli "Planla-Uygula-Kontrol Et-Önlem Al" yöntemi temeline dayanır.

1. **Planla:** BGYS'nin tasarlanması ve kurulması gerçekleştirilir. Standardın ana maddeleri olan Kuruluşun Bağlamı, Liderlik ve Planlama, bu adımla ilişkilidir. Planlama süreci BGYS'nin ana öğeleri, prensip ve çalışma şekli ortaya konduğu için diğer süreçlere göre daha önemlidir. Bu süreçteki en önemli çalışmalar Varlık Envanteri ve Risk Analizi çalışmalarıdır (Çubukçu, 2018, s. 97).

2. **Uygula:** Uygulama süreci BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi anlamına gelmektedir. Standardın Destek ve İşletim maddeleri bu sürece karşılık gelmektedir.

3. **Kontrol Et:** Bilgi güvenliği yönetim sisteminin kurulumu tamamlandıktan sonra daima izlenmeli ve gözden geçirilmelidir. Belirlenen güvenlik politikaları ve bu politikalar ışığında belirlenen tedbirlerin çalışıp çalışmadığının tespit edilmesi, denetimler ve kontroller çerçevesinde uygunsuzlukların belirlenmesi gerekmektedir. Performans Değerlendirme bu süreçte yapılmaktadır.
4. **Önlem Al:** Gözden geçirme, denetimler ve kontrollerde belirlenen yetersizliklerin giderilmesi, sisteminin devamlı geliştirilmesi, iyileştirilmesi bu

adımda gerçekleştirilmektedir (Çek, 2017, s. 19-20). Standardın 2005 yılı sürümünde sürekli üzerinde durulan Planla–Uygula–Kontrol Et–Önlem Al (PUKÖ) döngüsüne verilen önem 2013 yılında yayımlanan versiyonunda yer almamaktadır. Fakat, iyileştirme ve geliştirmenin aralıklarla yapılmasının gerekliliği vurgulanmaktadır. Bu husus, sürekli iyileşmeyi sağlamak için PUKÖ döngüsünün istenirse güncel sürümde de kullanılabileceğini göstermektedir (Gündoğan, 2016, s. 21).



Şekil 10. ISO/IEC 27001 Ana Maddelerinin Puko Döngüsüne Karşılık Gelen Maddeleri (Çubukçu, 2018, s. 97).

2.2.1. Planla

PUKÖ modelinin ilk ve en önemli aşamasıdır. Güvenlik politikasının oluşturulması, amaçların, hedeflerin, süreçlerin ve prosedürlerin belirlenmesi bu aşamada gerçekleştirilir. Bu adımın başarısı, belirlenen hedeflerin kurumun amaç ve hedefleriyle örtüşmesidir. Planlama safhasında, görev paylaşımının ve hedeflerin

doğru bir şekilde belirlenmesi önlem al aşamasının yükünü hafifletecektir. Bu aşamada BGYS'nin kurulumu ile ilgili çalışmalar yapılacağından diğer aşamalara göre en çok yol bu aşamada kat edilir. Kapsam, Politika, Risk Değerlendirme, Risk İyileştirme Planı ve Uygulanabilirlik Beyanı işlemleri bu adımda tanımlanır (Gazdağı & Çetinyokuş, 2020, s. 480).

Üst Yönetimin Desteği: Üst yönetim, kurumda karar verici kişilerdir. Bunlar, kurum sahipleri, yönetim kurulu başkan ve üyeleri, CEO'lar ve şirket yönetiminde görevli kişilerdir. ISO/IEC 27001 standardına geçiş ve BGYS kurulumu için üst yönetimin kararı gereklidir. Bu karar sürecin ve çalışmaların ciddiyetini vurgulamak için de önemlidir.

Üst yönetim sorumlulukları :

- Görev dağılımı ve atamalar yapmak,
- Bilgi güvenliği politikasını onaylamak ve yayınlamak,
- Bilgi güvenliği farkındalık çalışmasına destek olmak,
- Finansal ve insan gücü kaynaklarını sağlamak,
- BGYS'nin başarısının değerlendirildiği toplantılar yapmak,
- Süreçle ilgili bütün çalışmalara önderlik etmek ve yardımcı olmaktır (Çubukçu, 2018, s. 107-108).

BGYS Komitesinin Kurulması: Kurumlarda ISO/IEC 27001 in işletilmesi, yönetilmesi ve gerekli kontrollerinin sağlanmasından sorumlu olan BGYS komite üyeleri ve yöneticisi üst yönetim tarafından atanır (Çakır & Tuygun, 2019, s. 66). Kurumun büyüklüğüne ve üst yönetim kararlarına göre BGYS Komitesinde görev alacak kişiler değişiklik gösterebilir. Burada amaç var olan bölümlerden kişilerin bir araya gelerek BGYS kurulum ve yönetim çalışmalarını yürütmesidir. Kurumdaki bütün bilgi güvenliği çalışmalarından sorumlu olan BGYS Komitesinin görevleri:

- BGYS süreçlerini planlar ve kontrol eder,
- Kurumun bilgi varlıklarını tespit eder,
- Riskleri saptar ve bunları düşürmek için önlem alır,
- Bilgi güvenliği politikalarını belirler,
- BGYS için gerekli olan dokümanları hazırlar,
- İç tetkikleri gerçekleştirir,

- İş sürekliliği sağlar,
- Kurum içi eğitimler düzenler,
- Kurumda çalışanlarında farkındalık oluşturur (Çubukçu, 2018, s. 35).

GAP Analizi: GAP Analizi, kurumda BGYS kapsamına dahil olacak her sistemin ISO/IEC 27001 standardına uygunluğunu ve eksikliklerin belirlenmesi için bu uygulama yapılır. Hedeflediğimiz nokta ile şuan ki durum arasındaki farkın ayrıntılı bir şekilde analiz edildiği yöntemdir. Kontrol listeleri, mülakatlar, önceki tetkik veya gözden geçirme sonuçları, önceki vakalar ile ilgili kayıtların incelenmesi gibi işlemler yapılarak GAP analizi gerçekleştirilebilir. GAP analiz çalışmalarında çoğunlukla mülakat üzerinden ISO 27001 standardının 4. Ve 10. Maddeler arasında ki maddelere verilen cevaplar değerlendirilir. Daha sonra, ISO 27001 EK-A kontrol maddeleri gözden geçirilir. Çalışma sonucunda standardın tüm maddelerine ne kadar uygun olunduğu değerlendirilerek çalışma tamamlanır (Emir Erdoğan, Ocak, 2020, s. 28).

Bilgi Güvenliği Politikası: BGYS politikası, yönetime ışık tutan, hedefleri ortaya koyan, harekete geçiren, kurumun karşılaşabileceği risklerin değerlendirileceği ve yönetileceğine ilişkin kapsam ve kriterlerini açıklayan bir metin olmalıdır. BGYS politikasının başarılı olabilmesi için üst yönetim, bu politika maddelerinin kararlılıkla uygulanacağını çalışanlara hissettirmelidir (Önel, Dinçer; Dinçkan, Ali, 2007, s. 11).

Politika genel anlamda şu özellikleri içermelidir:

- Kuruluş amacına uygun olmalıdır,
- Belirlenen hedefleri karşılamalıdır,
- Çalışanlara haberdar edilmelidir,
- Üçüncü şahıslara duyurulmalıdır,
- Belirlenen aralıklarla gözden geçirilmelidir (Çubukçu, 2018, s. 119).

Kapsamın Belirlenmesi: Bir kuruluş; kendi bünyesinde BGYS'yi kurarken öncelikle sistemin neleri içine alacağı ve kapsamında nelerin yer alacağını dikkatlice belirlemesi gerekmektedir (Akay, 2014, s. 75). Kuruluşlar iç ve dış bağlamı, bu bağlamın gereksinimlerini, kuruluşun gerçekleştirdiği faaliyetler arasındaki ara yüzleri, bağımlılıklar ve diğer kuruluşları da göz önünde bulundurarak kapsamı oluşturmalıdır. Kapsam dışında bırakılan bütün öğelerin dışarda bırakılma gerekçeleri açıklanmalıdır.

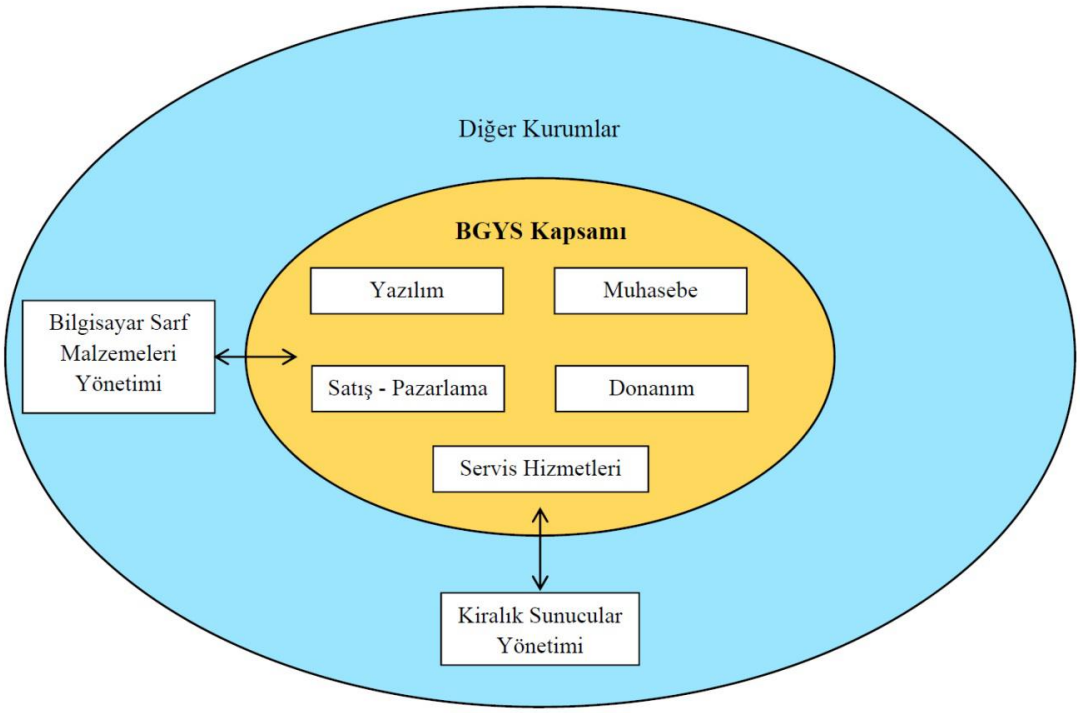
(Emir Erdoğan, Ocak, 2020, s. 29). Kapsam belirlenirken tüm bölüm ya da alanlar kapsama ekleneceği gibi, sadece önem arzeden kritik alanlarda uygulanabilir. Ayrıca ilerleyen zamanlarda sınırlarının genişletilmesi veya daraltılması mümkün olmaktadır. BGYS kapsamı belirlenirken geniş kapsamlı hazırlandığı halde uygulama ve kontrollerde oluşabilecek problemler kapsamda değişikliklere sebep olabilmektedir (Ersoy, 2012, s. 34). Fakat projenin yönetilebilir boyutta olması önemlidir. Bu yüzden kurumun fiziksel yapısı ve süreçleri göz önüne alınmalıdır (Perendi, 2008, s. 5).

ABY BİLGİSAYAR YAZILIM LTD.ŞTİ. BGYS KAPSAM DOKÜMANI		
YAYIN NO : 27001- POL- 01	**DOKÜMAN ADI: DOK-POL-V1**	**VER: 0.1**

ABY BİLGİSAYAR YAZILIM LTD. ŞTİ. BGYS KAPSAMI

Amaç ve Kapsam

2006 yılında Konya'da kurulan ABY Bilgisayar Yazılım Ltd. Şti. müşterilerine, kendine ve alt yüklenicilere ait olan bilgilerin korunması için ISO/IEC 27001 standart kapsamına uygun Bilgi Güvenliği Yönetim Sisteminin kurulmasına karar verilmiştir. Kurulacak ve uygulanacak sistem ABY Bilgisayar Yazılım Ltd. Şirketin tüm departmanlarını kapsayacaktır.



Organizasyon

ABY Bilgisayar Yazılım Ltd. Şti. 5 bölümden oluşmaktadır.
- Yazılım
- Muhasebe
- Satış pazarlama
- Servis hizmetleri

Yerleşke

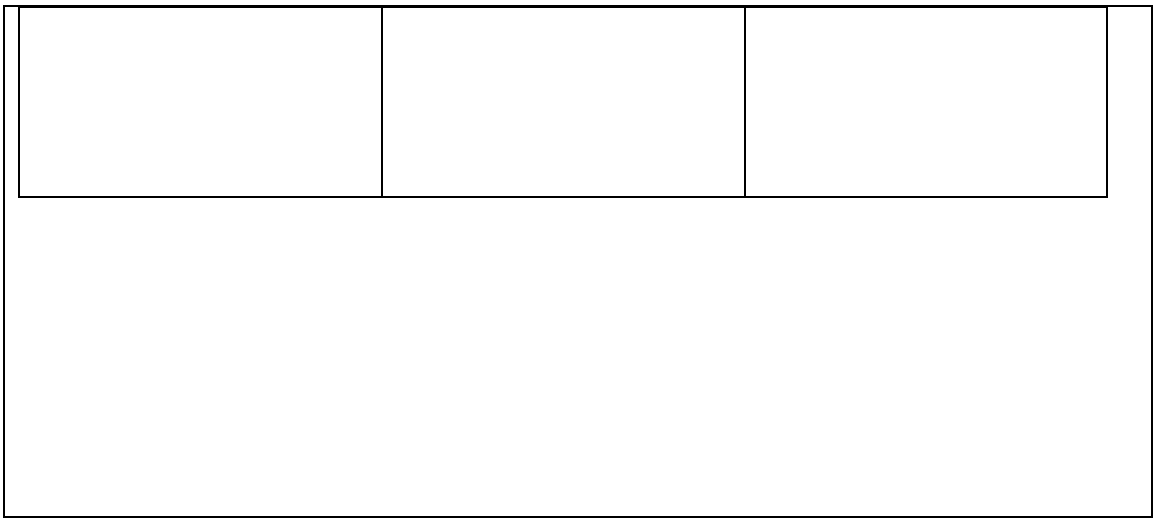
Innopark Konya Teknoloji Geliştirme Bölgesi Büyük Kayacık Mah. 101. Cad. No:13 Selçuklu/KONYA
Depo ve şubesi bulunmamaktadır.

Varlıklar ve Teknoloji

ABY Bilgisayar Yazılım Ltd. Şti. Bilgisayar sarf malzemeleri ve kiralık sunucular haricindeki kendi bünyesinde verilmekte olduğu, yazılım, satış - pazarlama, servis hizmetleri, muhasebe işlemlerini kendi bünyesinde sağlanmaktadır. BGYS aşağıda belirtilen tüm varlıkları kapsamaktadır.

1) Şirkete ait bütün ticari bilgiler
2) Bilgi teknolojileri, sunucular ve bilgisayar sistemleri
3) Tüm müşterilerin kişisel özel bilgileri
4) Şirketin çalışma ekibine ait olan bilgiler
5) Tüm Dokümantasyon Bilgileri

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN



Şekil 11. Örnek BGYS Kapsam Dokümanı (Perendi, 2008, s. 8).

Varlık Envanteri Oluşturma, Sınıflandırma ve Etiketleme: Kuruluşun ticari faaliyetlerini devam ettirebilmesi için gerekli olan varlık; donanım, yazılım, teknik altyapı ve dış hizmetler, bilgisayar ortamındaki dosyalar ve kağıt üzerindeki bilgiler, çalışan, kuruluşun prestij ve imajı gibi değerlerden oluşmaktadır. Ayrıca BGYS iş süreçlerine de önem vermekte ve onları da bir varlık olarak tanımlamaktadır. Kapsam dahilinde olan bütün bilgi varlıkları belirlenmeli ve bilgi varlığı envanteri oluşturulmalıdır. (Ersoy, 2012, s. 39), (Çubukçu, 2018, s. 126). Risk analizinin doğru bir biçimde yapılabilmesi, bilginin net bir şekilde korunması için bilgi varlıkları da dahil tüm varlıkların envanterinin hazırlanması ve sınıflandırılması gereklidir (Koç F. , 2008, s. 8).

Varlık Envanteri: Varlık envanteri, bilgi varlıklarını detaylı bir şekilde gösteren bir listedir. Genellikle BGYS yetkilileri tarafından hazırlanır. Fakat kurumda iş süreçlerinden sorumlu olan kişiler, departmanın sahip olduğu bilgi varlıklarını çıkarırlarsa bu daha iyi olur. Varlık tanımlamaları ile ilgili yapılan çalışmalar kurumdan kuruma, kullanıcıdan kullanıcıya değişiklik gösterebilir. Uygulayıcı (BGYS yöneticisi) istediği şekilde varlıkları tanımlayabilir, sınıflayabilir ve değerlerini verebilir (Çubukçu, 2018, s. 132). Aşağıdaki tablo varlık envanteri çalışmasına örnek verilebilir.

Tablo 1. Örnek Varlık Envanteri Çalışması (Gürsel, 2019, s. 77).

VARLIK ENVANTERİ FORMU									
Departman	**Varlık Türü**	**Varlık Adı**	**Yeri**	**Varlık Sahibi**	**Gizililik Sınıfı**	**Bütünlük Sınıfı**	**Erişebilirlik Sınıfı**	**Varlığın Toplam Değeri**	**Bilgi Etiketleme**
İnsan Kaynakları	İş Süreçleri ve faaliyetleri	İşe Alım Süreci	İK Ortak Alan	İnsan Kaynakları Süpervizörü	1	1	1	3	Ş.Ö.
Mali İşler	Bilgi	Acente Sözleşmeleri	Mali İşler Müdürü Odası Kasanın karşısındaki dolapta	Satış Direktörü	3	2	1	6	G
Bilgi Teknolojileri	Ağ	Server Network	2.Kat Server Odası	Bilgi İşlem Şefi	4	2	2	8	G
Bilgi Teknolojileri	Donanım	Yedekleme sunucusu	1.Kat Network Odası	Bilgi İşlem Şefi	3	3	1	7	G
İnsan Kaynakları	Yazılım	PDKS kart okuma programı (puantaj)	Server	İnsan Kaynakları ve İdari İşler Takım Lideri	2	3	2	7	D.Ö
Satış /Pazarlama	İnsan	Satış Ofisi Sorumlusu	Satış Ofisi	Satış Ofisi Müdürü	2	2	1	5	D.Ö
İnsan Kaynakları	Site	Arşiv	İnsan Kaynakları Odası	İnsan Kaynakları Müdürü	2	1	1	4	D.Ö

Varlık envanterinde bulunan bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ile ilgili unsurlarına bir değer ataması yapılarak, varlığın toplam değeri hesaplanmalıdır. Bu değerler ileriki adımlarda varlıkların risklerini hesaplamak için de kullanılacaktır. Aşağıda bu değer atamasının yapılabilmesi amacıyla yararlanılabilecek örnek bir puanlama tablosu paylaşılmıştır (Gürsel, 2019, s. 77).

Tablo 2. Örnek Varlık Envanteri Puanlama Matrisi (Gürsel, 2019, s. 78).

GBE		**Varlık Envanteri Puanlama Matrisi**	
No	**Gizlilik**	**Bütünlük**	**Erişilebilirlik**
1=DÜŞÜK	Varlık zarar gördüğünde önemli bilgi ortaya çıkmaz. Ortaya çıkan önemli bilgi kuruluşu etkilemez/çok az etkiler.	Varlık zarar gördüğünde önemli bilgi kontrol dışı değişmez. Ortaya çıkan bilgi kurumu etkilemez / çok az etkiler.	Varlık zarar gördüğünde önemli bilgiye erişim sağlanabilir. Erişilebilirliği zarar gören bilgi kurumu etkilemez / çok az etkiler.
2=ORTA	Varlık zarar gördüğünde önemli bilgi açığa çıkmaz. Açığa çıkan önemli bilgi kurumu etkiler. Sonucu orta vadede karşılanabilir.	Varlık zarar gördüğünde önemli bilgi kontrol dışı değişmez. Kontrol dışı değişen önemli bilgi kurumu etkiler. Sonucu orta vadede karşılanabilir.	Varlık zarar gördüğü durumda önemli bilgiye erişim sağlanabilir. Erişilebilirliği zarar gören önemli bilgi kurumu etkiler. Sonucu orta vadede karşılanabilir.
3=YÜKSEK	Varlık zarar	Varlık zarar	Varlık zarar

	gördüğünde önemli bilgi açığa çıkar. Açığa çıkan önemli bilgi kurumu etkiler. Sonucu orta vadede karşılanabilir.	gördüğünde önemli bilgi kontrol dışı değişir. Kontrol dışı değişen önemli bilgi kurumu etkiler. Sonucu orta vadede karşılanabilir.	gördüğünde önemli bilgiye erişim olmaz. Erişilebilirliği zarar gören bilgi kurumu etkiler. Sonucu orta vadede karşılanabilir.
4=ORTA	Varlık zarar gördüğünde önemli bilgi açığa çıkar. Açığa çıkan önemli bilgi kurumu etkiler. Sonucu telafi edilemez ya da bu uzun sürebilir.	Varlık zarar gördüğünde önemli bilgi kontrol dışı değişir. Kontrol dışı değişen önemli bilgi kurumu etkiler. Sonucu Telafi edilemez ya da bu uzun sürebilir.	Varlık zarar gördüğünde önemli bilgiye erişilemez. Erişilebilirliği zarar gören bilgi kurumu etkiler. Sonucu telafi edilemez ya da bu uzun sürebilir.

Varlıkların toplam değerinin hesaplanması; varlıkların gizlilik, bütünlük ve erişilebilirlik değerlerinin toplanması, çarpılması ya da ortalamasının alınması ile hesaplanabilir. Örnek olarak verilen Varlık Envanteri Puanlama Matrisi baz alınarak, tanımlanan her bir varlığa gizlilik, bütünlük ve erişilebilirlik puanı verilir. Kurum varlık değerini hesaplarken yine gizlilik, bütünlük, erişilebilirlik unsurlarını göz önüne alarak uygulanabilir bir hesaplama yöntemi geliştirebilir (Gürsel, 2019, s. 79).

Varlık Sahibi ve Varlık Emanetçisi: Varlık sahibi, varlıkların kayıtlı olduğundan, sınıflandırıldığından, güvenliğinin sağlandığından, varlıklara gerekli kişilerin erişim sağladığından ve düzenli aralıklarla olarak gözden geçirildiğinden sorumludurlar. Varlık emanetçisi kullanıcılardır. Fakat sorumluluk yine varlık sahibindedir (Ekşi, 2021).

Varlıkların İadesi ve İmhası: Varlığın iadesi, kurum çalışanının görevinin bitmesi sonucu varlığın uygun bir form doldurularak, kontrol edilip geri alınmasıdır. Varlıkların imhası ise varlık yönetim sürecinde kullanım ömrü dolan varlığın uygun bir şekilde imha edilmesidir (Çubukçu, 2018, s. 139).

Varlıkların Sınıflandırılması: Bilgi sınıflandırması, ISO/IEC 27001 BGYS standardının Ek.A 8.2.1 kontrol maddesinin gerekliliği olarak varlık envanterinde

kayıtlı bütün bilgi varlıkları yasal gereksinimleri, iş ihtiyacı, önemlilik ve kritiklik gibi kıstaslar göz önünde bulundurularak, tüm kurum kültürüne de entegre edilerek yapılmalıdır (Almeman & Saymaz, 2018, s. 58). Varlıkların sınıflandırılması genellikle üç ya da dört düzeyle yapılır. Sınıflandırmanın ve etiketlemenin kullanıcılar tarafından zorluk yaşanmaması açısından kolay ve anlaşılır şekilde olmasında fayda vardır. Ülkemizde ise genellikle Gizli, Şirkete Özel ve Genel olarak ya da Gizli, Departmana Özel, Şirkete Özel ve Halka Açık gibi sınıflandırmalar kullanılmakla birlikte sınıflandırma kuruma göre değişmektedir (Gürsel, 2019, s. 80). Varlıkların gizlilik değerleriyle bilgi varlıklarının sınıfı uyumlu olmalıdır. Örneğin, GİZLİ olan varlığın, varlık envanterindeki gizlilik değeri de yüksek olmalıdır (Çubukçu, 2018, s. 143).

Tablo 3. Bilgi Varlıkları Sınıfları ve Kullanım Alanları (Gürsel, 2019, s. 81).

SINIF Kullanım	GİZLİ	ŞİRKETE ÖZEL	GENEL
Erişim Hakları	Sadece görevi gereği bu varlığı kullanması gerekli olan ve özel olarak yetkilendirilmiş çalışanlar tarafından erişilebilir. Erişebilecek kişiler, bilgi sahibi tarafından belirlenir ve belirlenen kişiler dışında erişim engellenir.	Bilgi varlığının teknik ve iş sahibi birimleri tarafından erişilebilecek olan varlıklarıdır. Kuruluş çalışanlarının erişimine açık varlıklardır. Kurum içi genel erişim engellenir.	Genel erişime açık varlıklardır. Yetkisiz kişiler tarafından değişiklik yapılmaması için önlemler alınır. WEB sitesinde duyurulan bilgiler de bu sınıftadır.
Saklama	Erişim güvenliği sağlanmış (kilit, manyetik erişim kontrolü yapılabilen) ortamlarda saklanır. Bilgisayar ortamlarında ise sadece yetkili kullanıcıların erişebileceği şekilde saklanır. Varlığın yasal olarak belirli bir süre saklanması gerekiyorsa kilitli kasada veya arşivde saklanır.	Kurum içi erişime açık olduğu için varlık sahibi tarafından talep edilmemiş ise özel bir saklama uygulanmaz. Korumalı saklama gerektiği durumda erişim güvenliği sağlanmış (kilit, manyetik erişim kontrolü yapılabilen) ortamlarda saklanır. Bu elektronik veya diğer ortamlardaki varlıklar genel erişimin olmadığı alanlarda saklanır.	Yetkisiz kişiler tarafından değişiklik yapılmaması için önlemler alınarak saklanır.
İletim	Posta veya kurye aracılığıyla ve kapalı zarfta iletilir. Zarfın arkası yetkisiz değişikliğin tespit edilebilmesi için kaşelenir ve imzalanır. Elektronik ortamdaki bilgiler kurumsal iletişim araçları üzerinden iletilir. İletim sırasında yetkisiz kişiler tarafından değişiklik yapılmayacak önlemler alınması yeterlidir.	Basılı evraklar zarf içinde gönderilir. Elektronik ortamdaki bilgiler kurumsal iletişim araçları üzerinden iletilir. İletim sırasında yetkisiz kişiler tarafından değişiklik yapılmayacak önlemler alınması yeterlidir.	Elektronik posta sistemi ve taşıma görevlileri kullanılabilir. İletim sırasında yetkisiz kişiler tarafından değişiklik yapılmayacak önlemler alınması yeterlidir.
İmha	Basılı dokümanlar için kağıt parçalama cihazı kullanılır. Elektronik ortamda ise bilgiye tekrar ulaşılmasını engelleyen yöntemler (formatlanan bilgiye geri dönüşüm sağlanamayacak şekilde üzerine yazılması) kullanılarak silinir. Cihazların geri dönüşüm imkânı yok ise parçalanır.	Varlıkların tipine göre uygun geri dönüşüm yöntemi belirlenir. Basılı varlıklar kağıt dönüşüm çözümleri, elektronik ortamdaki varlıklar üzerindeki veri silindikten sonra uygun geri dönüşüm çözümleri belirlenerek elden çıkarılır.	Varlıkların tipine göre uygun geri dönüşüm yöntemi belirlenir. Basılı varlıklar kağıt dönüşüm çözümleri, elektronik ortamdaki varlıklar üzerindeki veri silindikten sonra uygun geri dönüşüm çözümleri belirlenerek elden çıkarılır.

Yukarıdaki tabloda bilgi varlıkları ve kullanım alanları ile ilgili üç düzeyden oluşturulmuş bir örnek paylaşılmıştır.

Varlıkların Etiketlenmesi: Etiketleme işlemi, renkli ya da yazılı etiketlerin fiziksel varlıkların üzerine yapıştırılmasıyla olur. Elektronik dosyalar için, dosyanın içinde , alt

ve üst başlık alanlarında GİZLİ, ŞİRKETE ÖZEL gibi yazılarak etiketlenebilir. Tüm kurum çalışanları bilgi sınıflandırılması ve etiketlenmesinden haberdar edilmelidir. Bu sebeple bilgi güvenliği bilgilendirme ve farkındalık eğitimlerinde bu konuya da değinilmesinde fayda vardır (Çubukçu, 2018, s. 144). Bilgi sınıflandırması ve bununla uyumlu bilgi etiketlemesi ile ilgili çok farlı örnekler vardır. Aşağıdaki tablo etiketlemeye örnek verilebilir.

Tablo 4. Örnek Varlık Etiket Tablosu (Çubukçu, 2018, s. 144).

Etiketleme	Elektronik Dosyaları	Basılı Evraklar	Aygıtlar/Medya	RENK
GİZLİ	Uygun etiket gerekir. Kapak sayfası, alt bilgi, Konu vb. alanlarda GİZLİ yazılabilir.	Uygun etiket gerekir. Kağıt üzerinde damga olarak basılabilir.	İsteğe bağlı.	KIRMIZI
ŞİRKETE ÖZEL	Uygun etiket gerekir. Kapak sayfası, alt bilgi, konu vb. alanlarda gizlilik etiketi belirtilmelidir.	Uygun etiket gerekir. Kağıt üzerinde damga olarak basılabilir.	İsteğe bağlı.	SARI
GENEL	Etiket gerekmez.	Etiket gerekmez.	Etiket gerekmez.	YEŞİL

Risk Yönetimi: ISO/IEC 27001 standardının kurulmasında ve bilgi güvenliğinin sağlanmasında en önemli konulardan biri de bilgi güvenliği risklerinin yönetimidir. ISO 31000 Risk Yönetimi' ne göre risk genel olarak, amaçlar üzerindeki belirsizlik etkisi olarak belirtilmektedir (ISO, 2018). Bilgi güvenliğine göre ise risk, bir varlıktaki bir açıklığın bir tehdit tarafından kullanılma olasılığıdır (Çek, 2017, s. 53).

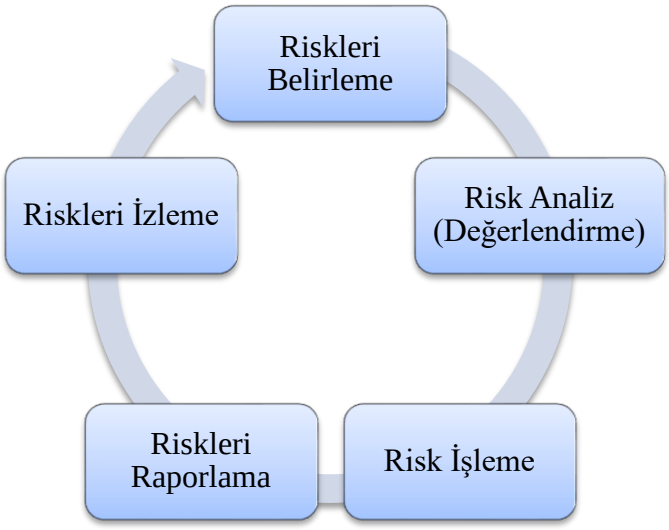
Sürekli ve sürdürülebilen bir süreç olan bilgi güvenliği yönetim sistemini aslında bir risk yönetim süreci olarak da düşünebiliriz. Sürekli değişen teknoloji ve değişken

durumların sonucunda devamlı yeni riskler ortaya çıkmaktadır. Bu sebeple bilgi kaynaklarının riskleri, tehditleri ve zayıf yönleri belli aralıklarla gözden geçirilmelidir. Aslında yapılan bu işlemler bilgi güvenliği yönetim sisteminin temelini oluşturmaktadır (Djapić & Lukić, 2007, s. 124). Risk analizi, kurumlarda bilgi güvenliğinin oluşturulmasında iki ana şarttan biridir. Yapılan risk analizi, kurumun karşılaşabileceği olası güvenlik risklerini ortaya çıkararak, kurumun önceliklerini belirleyip, tehditleri tespit ederek, risklerin ortadan kaldırılmasını sağlayarak, bilgi güvenliğinin sağlanmasında oldukça çok önemlidir (Çek, 2017, s. 57).

ISO/IEC 27001 standart her ne kadar risklerin ortaya çıkarıldığı bir çalışma olsa da bir risk yönetim metodolojisi içermez. Bu konuda diğer ISO standartlarından olan ISO 31000 Risk Yönetimi standardından yardım alır. Buna göre kurumun göreceği faydalardan bazıları:

- Belirlenen hedeflere ulaşma ihtimalini artırma,
- Riski belirleme ve müdahale etme de haberdar olma,
- Kanunlara ve ilgili şartlara, uluslararası şartlara uyum sağlama,
- Paydaş güvenini ve inancını iyileştirme,
- Kontrolleri iyileştirme,
- Operasyonel etkinliği ve verimliliği iyileştirme,
- Sağlık, güvenlik ve çevresel korumada verimi en yüksek tutmak ve iyileştirmek,
- Kayıpları en aza indirme, şeklinde açıklayabiliriz (Çubukçu, 2018, s. 148-149).

Riskin temel bileşenlerini tehlike, tehdit, açıklık, zayıflık, olasılık ve olumsuz etki (zarar görme) şeklinde sıralayabiliriz. Risk yönetim sürecinde, riskler tanımlanarak uygun önlemler alınır ve böylece riskleri azaltmış oluruz.



Şekil 12. Risk Yönetim Süreci (Çubukçu, 2018, s. 151).

Riskleri Belirleme: Kurumun bilgi varlıklarını tehdit eden riskler, risk değerlendirme yöntemi aracılığıyla tespit edilmelidir. BGYS varlık envanterinin çıkarılması risk değerlendirme işinin temelini oluşturur. Kurum, BGYS kapsamındaki kayıtlı varlıkların sahiplerini, türünü ve önem derecesini bir envanter listesi olarak dokümante etmelidir (Önel & Dinçkan, 2007, s. 12).

Risk tanımlarının daha iyi bir şekilde yapılması adına riskleri iç risk ve dış risk olarak belirtebiliriz. İç riskler, kurumun kontrolü altında olan olaylardan kaynaklanan risklerdir. Dış riskler ise kurumun kontrolü dışında meydana gelen olaylar sonucunda ortaya çıkan risklerdir. Riskler belirlenirken görüşmelerden, olay envanterinden, eski verilerden, sektörel verilerden ve anketlerden yararlanılabilir. Belirlenen riskler Risk Kütüğü adlı tabloya riske ait iş süreçleri, tehlikeler, olasılıkları, etkileri ve diğer bilgiler girilerek kaydedilir. Yine bu tabloda risklere ilişkin hesaplamalar yapılarak riskin derecesi belirlenir. ISO/IEC 27001 BGYS risk tanımlamaları yaparken riskin sahibinin de tanımlanmasını ister. Risk sahibi riski yöneten ya da riskten sorumlu olan kişidir (Çubukçu, 2018, s. 161).

Risk Analizi (Değerlendirme): Riskleri tespit etmek ve değerlendirmek de uygulanan risk analizi; bilgi kaynaklarının belirsiz olaylar sonucunda etkilenmesini ortaya çıkarmak, denetlemek, tamamen yok etmek ya da minimum seviyeye indirgemeyi kapsayan süreç olarak adlandırılabileceği gibi, fayda-maliyet analizi, seçim,

önceliklendirme, gerçekleştirim, sınama, önlemlerin güvenlik değerlendirmesi gibi komple güvenlik gözden geçirmesini de içerebilir (Kumaş, 2009, s. 174-180).

Risk analizi, risk değerlendirmesine ve riskleri azaltmamıza ihtiyaç olup olmadığı konusunda kararlara ve yerinde risk iyileştirme taktikleri ve yöntemlerine özgü durumları gösterir. Risk analizi ayrıca, seçimlerin yapılacağı kararların alınmasına ve farklı tür ve düzeylerde risk gerektiren seçeneklere de bir girdi sağlar. Risk analizi, riskin sebep olduğu durum ve kaynaklarının, onların olumlu ve olumsuz sonuçlarının ve gerçekleşebilme olasılıklarının önemsenmesini gerektirir. Sonuçların etkileri somut veya soyut olarak belirtilebilir. Bazı durumlar için sonuçlar ve oluşma ihtimalini tanımlamak için birden fazla sayısal değer veya açıklayıcı gerekir (ISO/IEC 31000, 2011, s. 38).

Riskin değerleri, bir metrik sistem (ölçme sistemi) ile riskler puanlanarak ortaya konur. Bu sayısal ve sayısal olmayan değerler ile 1 - 5 arasında ya da düşük, orta, yüksek gibi değerler verilerek yapılabilir.

RİSK DÜZEYİ	RİSK DÜZEYİ
1	Çok Düşük
2	Düşük
3	Orta
4	Yüksek
5	Çok Yüksek

BGYS açısından bilginin gizlilik, bütünlük, erişilebilirlik kayıpları ile ilgili belirlenen risklerin ortaya çıkması durumunda olası sonuçları riskin etki değeridir. Bu olası sonuçlar finansal, yasal, itibar, stratejik, müşterinin sesi, operasyonel/iş sürekliliği, ticari, ürün kalitesi, finansal getiri vb. olabilir (Gürsel, 2019, s. 85). Etki değerini belirlemek için aşağıdaki maddeler göz önünde bulundurulabilir:

- Kurumun uğrayacağı maddi ve manevi zararlar,
- Çalışanların karşılaşabileceği maddi ve manevi zararlar,
- İş süreçlerindeki kesintiler,
- İş kaybının boyutları,
- Yasal durumlar,
- Olası diğer kayıp ve zararlar (Çubukçu, 2018, s. 166).

				ETKİSİ		
VARLIK	**DEĞERİ**	**TEHDİT**	**OLASILIĞI**	**GİZLİLİK**	**BÜTÜNLÜK**	**ERİŞİLEBİLİRLİK**
Desktop PC	4	Arıza	2	4	3	2
Laptop	4	Çalınma	3	3	3	3
Server	4	Durma	1	5	3	5

Tablo 5. Varlıklar, Tehditler ve Etki Değerleri (Çubukçu, 2018, s. 166).

Risk değerini bulmak için bir diğer faktör de olasılıktır. Olasılık, beklenmedik bir olayın meydana gelme ihtimali olarak tanımlanmaktadır. Risk analizinde bir açıklığın gerçekleşme olasılığının ortaya çıkarılması çok önemlidir ve belirlenen bütün açıklıklar için bir olasılık değerlendirilmesi yapılmalıdır. Olasılığın belirlenmesi için, tehdit kaynağını, açıklığın cinsi, var olan denetimlerin varlığı ve etkinliği göz önünde bulundurulmalıdır. Olasılığı değerlendirirken ilk önce BGYS ekibinin kaç aşamalı değerlendirme yapacağını ve bu aşamaların nasıl belirleneceğini tanımlaması gerekir (Yılmaz M. , 2018, s. 64). Olasılık değerleri için örnek tablo aşağıda paylaşılmıştır.

OLASILIK	**ANLAMI**	**SIKLIK**
1 (ÇOK KÜÇÜK)	Olayın gerçekleşmesi mümkün değil. Çok nadiren meydana gelebilir.	Hemen hemen hiç.
2 (KÜÇÜK)	Olayın gerçekleşme olasılığı çok düşük ama yine de olabilir.	Yılda bir kez.
3 (ORTA)	Olayın gerçekleşme olasılığı var. Geçmişte gerçekleşmiş. Bazen meydana gelebilir.	Yılda birkaç kez.
4 (YÜKSEK)	Olayın gerçekleşme olasılığı yüksek. Daha önce birçok kez gerçekleşmiş. Sıklıkla meydana gelebilir.	Ayda bir kez.
5 (ÇOK YÜKSEK)	Olayın gerçekleşme olasılığı çok yüksek. Her an olabilir. Neredeyse her gün gerçekleşir.	Her hafta ya da her gün.

Tablo 6. Örnek Olasılık Değerleri Tablosu (Çubukçu, 2018, s. 164).

Tespit edilen bilgi güvenliği risklerinin gerçekleşmesi halinde muhtemel sonuçları ve risklerin gerçekleşmesi ihtimalinin bileşkesiyle risk seviyeleri belirlenir ve böylece bilgi güvenliği riskleri analiz edilmiş olur (Gürsel, 2019, s. 86). Bu durumu aşağıdaki gibi formüle edebiliriz :

Risk = Tehdidin Olma Olasılığı * Tehdidin Etkisi

Örnek olarak, olasılık:2 , etki:3 bu durumda riskin sayısal değeri: 2*3=6 olarak hesaplanır.

Fakat olasılık ve etki değeri, varlığın gizlilik, bütünlük ve erişilebilirlik özellikleri için de yapılmalıdır. O zaman aşağıdaki formülü kullanırız (Çubukçu, 2018, s. 167).

Risk=[(Olasılık Değeri * Gizlilik)+(Olasılık Değeri * Bütünlük)+(Olasılık Değeri *Erişilebilirlik)]

Olasılık seviyesi ve etki analizi seviyelerini ortaya çıkardıktan sonra kurumun etkileneceği risk faktörleri belirlenir ve derecelendirilir. Bu işlem sonucunda bir risk değerlendirme matrisi oluşturulması gerekmektedir (Bingöl, 2010, s. 22). Örnek risk matrisi aşağıda paylaşılmıştır.

Tablo 7. Örnek Risk Matrisi (BGYS Danışmanlık DAS Smart, 2018).

Risk ve Fırsat Matrisi Tablosu							
Risk Matrisi							
Etki							
5	Çok Ciddi	5	10	15	20	25	
4	Ciddi	4	8	12	16	20	
3	Orta	3	6	9	12	15	
2	Hafif	2	4	6	8	10	
1	Çok Hafif	1	2	3	4	5	
Risk		Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek	
		1	2	3	4	5	Olsalık

I. Önceliklili Riskler	II. Öncelikli Riskler	III. Öncelikli Riskler	IV. Öncelikli Riskler
25, 20, 16	15, 12, 10	9, 8, 6, 5	4, 3, 2, 1

Risk İşleme: Kuruluş, belirlenen risklere uygun önlemleri seçmek ve bu önlemleri uygulama işlemleridir. Risk işleme seçenekleri, riskin kabul edilmesi, riskten kaçınılması, riski azaltma ve kontrol etme, riskin transferi şeklinde seçilebilir (Emir Erdoğan, Ocak, 2020, s. 48).

- Riskin Kabul Edilmesi, halihazırda bulunan önlemlerin uygun olduğu, ek önlemlere ve kontrollere ihtiyaç duyulmadığını ifade eder. Riskin belirlenen düzeyde ekstra bir güvenlik denetimine gerek olmadan devam etmesi kararıdır. Güvenlik riski olan fakat saldırı riski bulunmayan bilgi varlıkları için riskin göz ardı edilmesi tercih edilmektedir (Gülmüş, 2010, s. 82).
- Riskin Transfer Edilmesi, kurumların sorumluluğunda bulunmayan varlıkların ve yine kurumların müdahalede bulunamayacağı risklerin başka kurumlara transfer edilmesine denir. Örnek olarak hırsızlık, doğal afet, yangın gibi tehditleri azaltmak için yapılan denetimlerden sonra çıkan artık riskin, itfaiye, emniyet güçlerine ve sigorta şirketlerine aktarılmasıdır (Gülmüş, 2010, s. 81).
- Riskten Kaçınma, risk doğuran eylemlere son verilmesidir.
- Riskleri Azaltma ve Kontrol Etme, risklerin gerekli önlem ve uygun kontrollerle seviyelerinin düşürülmesidir (Çek, 2017, s. 62).

Risk işleme süreci tanımlandıktan sonra artık risklerin belirlenmesi gereklidir. BGRS'nin bir sonraki adımında oluşacak risk hesaplamada bu artık risklerin listesi ve risk kabul kriteriyle beraber, risk işleme işleminin yenilemesi yapılabilmektedir (Ganbat, 2013, s. 44).

Risk Değerlendirme Raporu: Bu rapor, risk düzeylerinin ve gerekli önlemlerin açıklandığı, üst yönetimce onaylanan rapordur. Risk değerlendirme raporu, risk analizi, metodoloji, risk derecelendirme, risk matrisi hakkında bilgi verir. Ardından yapılan çalışmaya göre yüksek riskler ve önlemleri belirlenir. Burada amaç belirlenen riskler ve önlemleri hakkında üst yönetimi haberdar etmek ve onaylarını almaktır (Çubukçu, 2018, s. 174).

Kontrollerin Seçilmesi: Belirlenen risklerin azaltılması ya da ortadan kaldırılması gerekmektedir. Kurum bunun için bazı kontroller seçmelidir. Bu kontroller ISO/IEC 27001 standardının Ek-A kısmındaki kontroller olabileceği gibi teknik, yönetimsel, fiziksel ya da uygulayıcının geliştirdiği kendi kontrolleri de olabilir. Uygun kontrollerin seçiminde maliyet, emniyet, kurumun prestij ve itibarı, yasal zorunluluklar, kurum kültürü ve politikaları gibi faktörler de göz önünde bulundurulmalıdır. ISO/IEC 27001 standardı kurumlara önleyici, destekleyici, düzeltici, düzenleyici, teknik, yönetimsel ve operasyonel kontroller sağlamaktadır (Bingöl, 2010, s. 23).

ISO/IEC 27001 standardının Ek-A kısmında on dört bölüm ve yüz on dört kontrol maddeleri vardır. Ek-A kontrol maddelerinde, A-5'ten A-18'e kadar her bir alt bölüm (A.7.1, A.8.1 vb.) için bir amaç tanımlanmıştır. Bu alt bölümlerin altında kontroller A.7.1.1, A.7.1.2, A.8.1.1, A.8.1.2, şeklinde belirtilmiştir. Amaç ve hedeflere erişmek için bu belirlenmiş kontroller uygulanmalı ve bu amaçlar 6.1.3 maddesindeki risklerin işlenmesine yardımcı olmalıdır (Gürsel, 2019, s. 103).

Alan	Kontrol Hedefleri	Kontroller
A.5: Bilgi Güvenliği Politikaları	1	2
A.6: Bilgi Güvenliği Organizasyonu	2	7
A.7: İnsan Kaynakları Güvenliği	3	6
A.8: Varlık Yönetimi	3	10
A.9: Erişim Kontrolü	4	14

A.10: Kriptografi	1	2
A.11: Fiziksel ve Çevre Güvenliği	2	15
A.12: İşletim Güvenliği	7	14
A.13: Haberleşme Güvenliği	2	7
A.14: Sistem Temini, Geliştirme ve Bakımı	3	13
A.15: Tedarikçi İlişkileri	2	5
A.16: Bilgi Güvenliği İhlal Olayı Yönetimi	1	7
A.17: İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	2	4
A.18: Uyum	2	8

Tablo 8. Ek-A Kontrol Maddeleri.

Uygulanabilirlik Bildirgesi (SOA):

ISO/IEC 27001 standardının Ek-A kontrol maddelerinin hangisinin seçilip hangisinin hariç tutulduğunu belirtmek için SOA (State of Applicability) denen uygulanabilirlik bildirgesi dokümanı hazırlanır.

Uygulanabilirlik bildirgesi, TS EN ISO/IEC 27001 standardı için temel yapının oluşturulmasında önemli rolü olan bir dokümandır. Standart, Uygulanabilirlik Bildirgesinin hazırlanmasını ve dokümante edilmesini zorunlu kılmaktadır (TSE, 2013, s. 3). 6.1.3 maddesi risklerin değerlendirilmesi ve işlenmesinde gerekli kontrollerin uygulanmasını belirtiyor.

Bir riskin oluşması sonucunda kurumun öncelikle risk değerlendirmesini gözden geçirmesi, uyguladığı kontrolleri gözden geçirmesi ve risk işleme planlarını devreye sokması oldukça önemlidir. Bu aşamada Uygulanabilirlik Bildirgesi bu ilişkilerin açıkça ortaya konmasına yardımcı olmaktadır (Almeman & Saymaz, 2018, s. 18).

Tablo 9. Örnek Uygulanabilirlik Bildirgesi (Gürsel, 2019, s. 104).

UYGULANABİLİRLİK BİLDİRGESİ				Doküman No	BGYS-SOA-01
				Yayın Tarihi	16.12.2018
				Revizyon No	00
				Revizyon Tarihi	16.12.2018

Kontrolün Amacı	Madde No	Kontrol	Uygulanabilirlik (E/H)	Referans Dokümanı	Doküman Kodu
Bilgi güvenliği politikaları					
Bilgi güvenliği için yönetimin yönlendirilmesi	A.5.1.1	Bilgi güvenliği için politikalar	E	Tarsim Tarım Sigortaları Bilgi Güvenliği Politikası	P S210.11
	A.5.1.2	Bilgi güvenliği için politikaların gözden geçirilmesi	E	Bilgi Güvenliği Politikası	P S210.11
İç Organizasyon	A.6.1.1	Bilgi güvenliği rolleri ve sorumlulukları	E	BGYS Komitesi Çalışma Standardı	IT-093
	A.6.1.2	Görevlerin ayrılığı	E	IT Role and Responsibility Matrix	
	A.6.1.3	Otoritelerle iletişim	E	Bağlam Dökümanı	P S210.05
	A.6.1.4	Özel ilgi grupları ile iletişim	E	Bağlam Dökümanı	P S210.05
	A.6.1.5	Proje yönetiminde bilgi güvenliği	E	Change Mgmt Process Guide_Autoliv	IS-SEC-A12-001
Mobil cihazlar ve uzaktan çalışma	A.6.2.1	Mobil cihaz politikası	E	Mobile Device Policy	IS-SEC-A07-008
	A.6.2.2	Uzaktan çalışma	E	Connection to ALV network from outside	IT-077
İstihdam öncesi	A.7.1.1	Tarama	E	İşe Alma Prosedürü	PS112.01
	A.7.1.2	İstihdam hüküm ve koşulları	E	İşe Alma Prosedürü	PS112.01
Çalışma esnasında	A.7.2.1	Yönetim sorumlulukları	E	Bilgi Güvenliği Yönetim Sistemi Politikası Görev Tanımları	P S210.11 F01 PS113.01
	A.7.2.2	Bilgi güvenliği farkındalığı ve eğitimi	E	Eğitim Yönetimi Prosedürü	P S121.01
	A.7.2.3	Disiplin prosesi	E	Kapsam Dışı Personel Disiplin Uygulamaları Standardı	HR-GN-025
İstihdamın sonlandırılması veya değiştirilmesi	A.7.3.1	İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi	E	İşten Ayrılan Personel Standardı	HR-GN-023
Varlıkların sorumluluğu	A.8.1.1	Varlıkların envanteri	E	Varlıkların Yönetimi Prosedürü	P S210.09
	A.8.1.2	Varlıkların sahipliği	E	Varlıkların Yönetimi Prosedürü	P S210.09
	A.8.1.3	Varlıkların kabul edilebilir kullanımı	E	Varlıkların Kabul Edilebilir Kullanım Prosedürü	P S210.07
	A.8.1.4	Varlıkların iadesi	E	İşten Ayrılan Personel Standardı	HR-GN-023
Bilgi sınıflandırma	A.8.2.1	Bilgi sınıflandırılması	E	Bilgi Sınıflandırılması Prosedürü	P S210.10
	A.8.2.2	Bilgi etiketlemesi	E	Bilgi Sınıflandırılması Prosedürü	P S210.10
	A.8.2.3	Varlıkların kullanımı	E	Bilgi Sınıflandırılması Prosedürü	P S210.10
Ortam işleme	A.8.3.1	Taşınabilir ortam yönetimi	E	Varlıkların Kabul Edilebilir Kullanım Prosedürü	P S210.07
	A.8.3.2	Ortamın yok edilmesi	E	Atık Akış Standardı	SHE-GN-036
	A.8.3.3	Fiziksel ortam aktarımı	E	Tarsim Tarım SigortalarıTSM Backup Standard	IT-038

2.2.2. Uygula

Bu aşamada kontrollerin ve prosedürlerin uygulanması için yapılacak çalışmalar ele alınacaktır. Uygulama süreci genel olarak planladığımız BGYS'yi gerçekleştirmek, işletmek anlamına gelir. Bu adımda ISO/IEC 27001 Ek-A maddelerinden seçilen kontroller uygulanır. Yedek alma, izleme vb. görevler yapılır. Ayrıca risk işleme

çalışmaları da gerçekleştirilir ve belirlenen riskler için önlemler alınır ve riskler düşürülmeye çalışılır (Çubukçu, 2018, s. 358).

Risk İşleme ve Seçilen Kontrollerin Uygulanması: Risklerin giderilmesini sağlamak amacıyla belirlenen kontrollerin bu aşamada uygulanmasıyla BGYS'nin gerçekleştirilmesi sağlanmış olmaktadır. BGYS komisyonu bir risk işleme planı sunmalıdır. Bu plan, belirlenmiş risklere için yönetimin alması gereken önlemleri, bunların öncelik sırasını, sınırlayıcı etkenleri ve bu adımlar için atılacak adımların kaynaklarını içermelidir. Risk İşleme işleminden sonra belirlenen riskler için kontrollerin gerçekleştirilmesi ve etkinliğinin ölçülmesi işlemi gerçekleştirilmelidir.

Seçilen kontrollerin uygulanmasındaki önemli nokta, belirlenmiş riskleri en aza indirmek ya da ortadan kaldırmak ve kurum için en düşük maliyetli olacak kontrolün uygulanmasını sağlamaktır. Bazı kontrol uygulama süreçleri uzun zaman alacağından BGYS komisyonu belli aralıklarla seçilen bu kontrollerle ilgili değerlendirme toplantıları yapmalıdır. Seçilen kontrollerin etkinliğinin ölçülmesi önemlidir. Kontrol etkinliğinin belirlenmesinde uygulanan ölçütler, karşılaştırılabilir ve yeniden elde edilebilir sonuçlar vermelidir. Yani ölçüm sonuçları kontrollerin uygulanmasından önceki durumu mutlaka yansıtmalıdır (Bingöl, 2010, s. 26).

Farkındalık Eğitimleri: Kontrollerin uygulanması ve tüm BGYS sürecinde periyodik olarak önemli işlemlerden birisi de farkındalık sağlama ve eğitim sürecidir. Bilgi güvenliğinin sadece teknik konulardan oluşmadığını ve en önemli noktasının insan olduğunu biliyoruz artık. Ayrıca bilgi güvenliği, bilgi işlem çalışanı sorumluluğunda olmayıp bütün kurum çalışanlarını da ilgilendiren bir konudur. Çalışanların bilgi güvenliği kapsamında üstüne düşen görevleri gerçekleştirmeleri için BGYS komisyonunun, tüm çalışanlara bilgi güvenliğinin önemi hakkında farkındalık sağlaması gerekir. Farkındalık ise eğitimle hayat bulur. Bu kapsamda bilgi güvenliği ile ilgili belli zamanlarda, kurum içinden veya kurum dışından bilgi güvenliği hakkında uzman kişiler aracılığıyla eğitimler verilmelidir. Verilen eğitimlerin etkinliği değerlendirilmeli ve elde edilen beceriler ve nitelikler dokümanlara eklenmelidir. Eğitim süreci, tüm BGYS süreçlerinde sürekli gelişim düşüncesine göre uygulanmalıdır. Çalışanlar, bilgi güvenliği konusunda sürekli geliştirildiği sürece BGYS'ye katkıda bulunacaklardır (Bingöl, 2010, s. 27).

Komite Toplantıları: BGYS kurulum sürecinde oluşturulan ekibe BGYS Komitesi denir. Bu ekip üst yönetim tarafından atanır ve belli zamanlarda toplanarak çalışmaları düzenlerler. Yapılan toplantılarda alınan kararlar, toplantı tutanağı ile kaydedilir (Çubukçu, 2018, s. 364).

2.2.3. Kontrol Et

Kontrol Et aşamasında BGYS'nin işletilmesi sırasında eksiklikler tespit edilmeli, seçilen kontrollerinin verimliliği ölçülmeli, başarılı ve başarısız olan güvenlik kontrolleri tanımlanmalı, bilgi güvenliği vakaları ortaya koyulmalı, alınan önlemlerin güvenlik açıklıklarını giderip gidermediği ya da işe yarayıp yaramadığı tespit edilmelidir. Kurumda düzenli aralıklarla BGYS kapsamındaki politikalar, prosedürler ve kontrollerin etkinliklerinin ölçülerek gözden geçirilmesi gerekmektedir.

Bu aşamada İç Tetkik (İç Denetim), Yönetimin Gözden Geçirmesi (YGG) ve İzleme, Ölçme, Analiz ve Değerlendirme işlemleri yapılır.

İç Tetkik (İç Denetim): Kurumda yılda en az bir kere, belli zaman aralıklarla standardın 9.2 " İç tetkik" maddesine göre iç tetkikler (denetimler) yapılmalıdır. İç tetkiklerde; BGYS'nin bilgi güvenliği politikalarının, prosedürlerinin ve uygulamalarının, uygulamaların etkinliğinin, birimler arasındaki bütünlüğün ve çalışanların bilgi güvenliğinin farkındalığının kontrolleri yapılmalıdır ve sonuçları da üst yönetime raporlanmalıdır.

İç tetkik işlemi, planlama, denetleme ve raporlama şeklinde, belirlenen sorulara göre saha çalışmasıyla yapılır. İç tetkikçi, denetleyeceği departmanı inceleyip, sorular sorarak ve değerlendirerek denetimi gerçekleştirir. Bu süreçte dokümanları ele alır, çalışanın farkındalığını ölçer ve işlemlerin BGYS prosedürlerine uygunluğunu ortaya koymaya çalışır. Bu sırada uygunsuzlukları raporlayarak kurumun dış denetime hazır olmasını sağlar. Denetim sonucunda ortaya çıkarılan bulgular "majör", "minör" ve "gözlem" olarak belirtilir. Majör uygunsuzluk, standardın maddesinin hiçbir şekilde uygulanmadığını gösterir. Minör uygunsuzluk, standartın maddesini uygulamada eksiklik olduğu ya da uygulamaların dokümanda yazılı olduğu şekilde yapılmamasından dolayı oluşan uygunsuzluktur. Gözlem ise "geliştirilmeli" şeklinde öneri olarak yapılır (Çubukçu, 2018, s. 368).

İç tetkik sayesinde bulunan uygunsuzluklar, eksiklikler sonrasında düzeltici faaliyet düzenlenerek bu sorunlar ortadan kaldırılır. İç tetkiki, BGYS komitesi üyesi olan ve "iç tetkikçi" eğitimi almış çalışan yapar. Ayrıca dışardan iç tetkikçiler de sağlanabilir. İç tetkik yapan kişilerin kendi departmanını denetlememesi, farklı bölümlerin birbirini denetlemesi ve böylece ilgi çelişkisi olmamasına dikkat edilmesi gereklidir. Her bir denetimin kriterleri ve kapsamı belirlenmelidir (Bureau Veritas Gözetim Hizmetleri, 2017).

İç tetkiklerin ne zaman, nasıl ve kimin tarafından yapıldığını gösteren iç tetkik planının ve iç tetkik ile ilgili gerçekleştirilen faaliyetlere ait kayıtların tutulması zorunludur. **Yönetimin Gözden Geçirmesi:** ISO/IEC 27001 standardının 9.3 maddesi, yöneticilerden BGYS üzerinde etkili olacak önemli kararlar almalarını istemektir. Bunun için BGYS ile ilgili gerçekleştirilen çalışmalar belirlenen zamanlarda toplantı yapılarak değerlendirilmelidir. BGYS Yöneticisi sorumluluğunda gerçekleşen bu toplantı, öncelikle üst yönetim olmak üzere, BGYS komitesi, yöneticiler ve diğer ilgili çalışanlardan oluşur. Toplantı, sunum eşliğinde gündemdeki konular ve katılımcıların görüşleri alınarak yapılır (Gürsel, 2019, s. 128).

YGG toplantısının gündemi aşağıdaki konulardan oluşabilir:

- Bilgi Güvenliği Politikası'nın değerlendirilmesi,
- Risk Yönetim metodolojisinin değerlendirilmesi,
- Risk İşleme planının değerlendirilmesi,
- Düşürülen risklerin açıklanması,
- Güncel risk raporunun değerlendirilmesi,
- Artık risk ve kabul edilebilir risk düzeyi hakkında bilgilendirilme yapılarak üst yönetim tarafından onaylanması,
- Güvenlik ihlal olaylarının değerlendirilmesi,
- İç tetkik raporlarının değerlendirilmesi,
- Varlık envanteri, sahiplik ve kullanıcı erişimin gözden geçirilmesi,
- İzleme ve ölçme sonuçları,
- Gizlilik anlaşmalarının gözden geçirilmesi,
- Çalışan politikalarının ve insan kaynakları uygulamalarının gözden geçirilmesi konuları değerlendirilir (Çubukçu, 2018, s. 378).

2.2.4. Önlem al

Bu adımda, BGYS'nin kurulum ve sürdürme sürecinde Düzeltici Faaliyetler ve İyileştirme işlemleri yapılmaktadır.

Düzeltici Faaliyetler: Düzeltici faaliyet (DF), BGYS süreçlerinde tespit edilen bir uygunsuzluğun saptanması ve giderilmesi için yapılan "düzeltme" çalışmalarıdır.

ISO/IEC 27001:2013 sisteminden önce Düzenleyici ve Önleyici Faaliyetler kullanılıyordu. DÖF, uygunsuzlukları tespit ederek gerçekleşmemesi için önlemler almak için yapılan çalışmalardır. Fakat ISO/IEC 27001:2013 versiyonu ile DÖF yerine DF kullanılmaktadır. Çünkü ISO/IEC 27001:2013 versiyonu risk temelli bir sistemdir. 2013 versiyonunun risk temelli olması, uygunsuzluklar karşısında daima "önlemler" almayı gerektirir. Bu nedenle DÖF yerine DF kullanılmaktadır.

BGYS uygunsuzlukları tespit edilerek düzeltici faaliyetler ile birlikte tekrar oluşmaları önlenmelidir. Uygunsuzluğun kök sebebi araştırılmalıdır. Kuruluş sadece bulguları çözmek yerine uygunsuzluğun neden oluştuğunu araştırmaya devam etmelidir. Kök sebep belirledikten sonra başka uygunsuzlukların olup olmadığını veya oluşma olasılığı olup olmadığını belirlemelidir.

Kök neden analizinin ardından sorunların çözümü için yapılacak işlemler açıklanır ve düzeltme işlemi uygulanır. Uygunsuzluk ve düzeltici faaliyetlerin kanıtı olarak bilgiler dokümante edilmelidir.

İyileştirme: BGYS'nin uygunluğu, BGYS'nin etkinliği ve BGYS'nin doğruluğu için kuruluşular daima iyileştirme sürecinde olmalıdırlar. Bu süreç bazı faaliyetleri içerebilir;

- İç tetkikler,
- YGG toplantıları,
- Açıklık testlerinin yapılması,
- Ölçme ve değerlendirme çalışmaları,
- Risklerin sürekli olarak değerlendirilmesi (Çubukçu, 2018, s. 383).

2.3. AMPİRİK LİTERATÜR

Bu tez çalışması hazırlanırken öncelikle literatür, tez, makale taraması yapılmış, yabancı kaynaklar araştırılmış ve Türkiye'de yapılan çalışmalar detaylı olarak incelenmiştir. Bu konuda araştırmacılar tarafından yapılmış çeşitli çalışmalar, tezlerden ve yararlanılan kaynakların bazıları ise şunlardır:

Eminağaoğlu & Yılmaz (2009), dünyada ve Türkiye' de bilgi güvenliği konusunda yapılan ortak hatalar ve yanlışlıkları ortaya koymuş ve bu hataların çözümleri için insanların bilinçlendirilmesini ve doğru güvenlik çözümlerinin ve stratejilerinin doğru yerde ve zamanda yapılması önerilerinde bulunmuştur.

Ötegen (2018), uzmanlık tezinde; ISO 27001 Bilgi Güvenliği Yönetim Sistemine geçiş yapacak kurumların gerçekleştirmesi gereken adımlara yer vermiş ve ISO 27001 sertifikası edinmiş Wirefast ve GASCO, BGYS' ye uyum sürecinde yaşanan zorluğun çalışanın değişikliğe karşı direnmesi, yeniliklere uyum sağlamak istememesi ve eski alışkanlıklarına devam etmek istemeleri olduğunu belirtmiştir. Araştırmamızda kullanılan "ISO/IEC 27001 yönetim sistemine sahip olan firmalar başarılarını bilgi güvenliği bilincini sağlamış çalışanına mı dayandırırlar?" sorusu bu çalışma üzerine elde edilmiştir.

Boşal (2017), bu tez çalışmasında; İller Bankası yapısını inceleyerek, bilgi güvenliği ile alakalı yönetimsel ihtiyaçların yönetilememesi, ağ güvenliği için gerekli aygıtların düzgün bir şekilde yapılandırılamaması, zaman ve maliyet unsurlarının gözetilerek bilgi güvenliği projelerinin ikinci plana atılması, çalışanların bilgi güvenliği hakkında yeterli bilgiye sahip olmaması sorunlarına ulaşmıştır. Bu sorunlar karşısında, yöneticilerin ve yasa koyucuların insana yatırım yapması ve insanların bilinçlendirilmesi gerektiğini belirtmiştir. Bu çalışmadan araştırmamızda kullanılan "ISO/IEC 27001 bilgi güvenliği yönetim sistemi için insan kaynakları önemli bir faktör müdür?" sorusu elde edilmiştir.

Yılmaz (2018) yüksek lisans tez çalışmasında; Konya ilinde ISO/IEC 27001 Bilgi güvenliği yönetim sistemleri sertifikasına sahip olan işletmelerle mülakatlar yapılmış ve sonucunda; Konya'da belgelendirme ve denetleme yapan yeterli uzman kuruluşların olmaması, ISO/IEC 27001 sertifikası için Konya' da penetrasyon testi yapabilecek firma ve işletmelerin olmaması sorunları ile karşılaşmıştır. BGYS' nin kurulmasının

uzun vadeli bir fayda sağlamayacağı düşünülerek bu süreçte verilen emeklerin boşa zaman kaybı olduğu görülmüştür. Sektördeki diğer firmalarla iletişime geçerek yaşanan zorluklar, edinilen tecrübeler, zorluklar karşısında geliştirdikleri çözüm yolları hakkında bilgi alışverişinde bulunarak çözüm önerileri sunmuştur. Araştırmamızda kullanılan "Sertifika öncesi ve sonrasında karşılaşılan problemler ve çözüm önerileri nelerdir?" sorusu bu çalışma üzerine elde edilmiştir.

Çetinkaya (2008), bu bildiri çalışmasında; ISO/IEC 27001 BGYS için gerekli çalışmaların neler olduğu, nasıl uygulandığı ile ilgili bilgilere yer verilmiştir. Bu çalışmada iş sürekliliği, uyum, bilgi güvenliği ihlal olay yönetimi ile ilgili sorunlarla karşılaşılmıştır.

Irmak & Baz (2019), yaptıkları çalışmada; kurumsal bilgi güvenliğini ve önemini açıklayarak bilgi güvenliğine yönelik siber sorunlardan bahsetmiştir. Bu sorunlar karşısında; eğitim ve farkındalık yaratmayı, yönetsel ve teknolojik önlemler almayı, yetki denetimi ve fiziksel önlem almayı, yedekleme ve FKM (Felaket Kurtarma Merkezleri) kurmayı alınması gereken önlemler olarak bildirmiştir.

Şen & Yerlikaya (2013), yaptıkları çalışmada; kurumların bilgi güvenliği yönetim sistemi sürecini inceleyerek tehditleri ve riskleri tanımlayıp bu riskleri kabul edilebilir seviyeye çekmek için ISO 27001'in öngördüğü bir BGYS'nin kurumlara nasıl uygulanması gerektiği hakkında bilgilere yer vermiştir. Ayrıca sistem sayesinde kurumların bilgi varlıklarının farkında olması, kurumların risklerini belirleyerek yönetebildikleri için iş sürekliliğini sağlama, BGYS sayesinde bilgileri korunacağı için kurumun iç ve dış paydaşlarına karşı güven duygusu oluşturması sonuçlarına yer vermiştir.

İleri (2016) yapmış olduğu çalışmada; hastanede kurulumu üç yıl süren bilgi güvenliği yönetim sisteminin politika ve prosedürleri hakkında bilgi vermiş, uygulanan yöntemler karşısında kalınan teknik ve yönetimsel zorlukları ve bu zorluklarla nasıl başa çıkılacağını bir uygulama örneği üzerinden paylaşarak bilgi güvenliği kültürü ve bilincini oluşturmayı ayrıca sistemin kurulmadan önce ve sonra bilgi güvenlik seviyesinin durumunu karşılaşmalı şekilde aktarmıştır. Bu çalışma sonucunda hastanede sistem kurulmadan önceki tehditlerin %72'nin insan kaynaklı olduğunu ortaya çıkarmıştır. Akabinde bilgi kaynaklarına karşı tespit edilen 13 majör tehdit bilgi

sistemlerini %6 oranında kesintiye uğratmıştır. Bilgi güvenliği yönetim sisteminin kurulumunu takip eden iki yıl içerisinde bilgi sistemlerindeki kesinti %1'e düşmüş ve kurulumun son yılı itibariyle bilgi kaynaklarına ait hiçbir majör tehdit görülmediğini belirlemiştir. Bu çalışmadan araştırmamızda kullanılan "ISO/IEC 27001 sertifikasına sahip kuruluşların başarısına katkıları nelerdir?", "Sertifika öncesi ve sonrasında karşılaşılan problemler ve çözüm önerileri nelerdir?" soruları elde edilmiştir.

Henkoğlu (2017) yapmış olduğu çalışmada; kişisel verilerin korunması çerçevesinde; korunması istenen bilgiye ilişkin kavramlar üzerindeki belirsizlikler, sorumlulukların paylaşılamaması ve bilgi güvenliği stratejilerinin geliştirilememesi sorunlarının değişmediğini tespit etmiştir. Veri iletim yolunun ve saklama ortamının kriptolanması, sanallaştırma yönteminin kullanılması, hukuksal etki alanında veri bulundurulması, veri sorumlusunun belirlenmesi hakkında dikkate alınması gereken çözüm önerilerinden bahsetmiştir.

Akay (2014), bu tez çalışmasında; ISO/IEC 27001 BGYS standardının kurulum, kontrol, denetleme ve iyileştirme adımlarını var olan versiyon ve yeni versiyon ile beraber değerlendirerek bilgi güvenliği yönetim sistemini açıklamıştır. Yeni versiyonda standardın Ek A yapısı ve yenilenen kontrol maddelerine değinerek diğer yönetim sistemleri ile uyumunu açıklamıştır. Çalışmasında BGYS sertifikası sahibi Pendik Belediyesi ve Keçiören Belediyesi ile BGYS kurulumu hakkında mülakatlar gerçekleştirmiştir.

Çubukçu (2018), kitabında ISO/IEC 27001'i genel olarak açıklayarak BGYS'yi kurmak için yapılan çalışmalara kılavuzluk etmeyi amaçlamıştır.

ÜÇÜNCÜ BÖLÜM: ALAN ARAŞTIRMASI

3.1. Araştırmanın Tanıtılması

Bu başlık altında araştırmanın konusu, amacı ve önemi, yöntemi, soruları, kapsam ve sınırlılıklar ile ilgili bilgiler verilmiştir.

3.1.1. Araştırmanın Konusu ve Alanı

Batı Karadeniz Bölgesi'nde ana metal ve çimento saktöründe faaliyette bulunan ISO/IEC 27001 sertifikasına sahip 5 işletme üzerinde gerçekleştirilmiştir. Bu çalışma, işletmelerdeki ISO/IEC 27001:2013 standardının belgelendirilmesi sürecindeki işlemleri ve bu süreçte karşılaşılan zorlukları konu almıştır. Standardın kuruluşlar tarafından doğru bir şekilde uygulanması, sertifikanın gereklilikleri, yapılması gerekenler ve bu süreçte kuruluşların karşılaştığı zorluklar ele alınmıştır.

3.1.2. Araştırmanın Amacı ve Önemi

Bilgi varlıkların korunmasına yönelik önemin her geçen gün artması sebebiyle, Batı Karadeniz Bölgesi'nde bulunan, ISO/IEC 27001:2013 sertifikasına sahip kurum ve işletmelerin sertifikasyon süreçleri ve bu süreçte karşılaştıkları zorluklar ele alınmıştır. Bu şekilde işletmelere ve araştırmacılara, bilgi güvenliği yönetim sistemi kurulumu ve çalıştırılması hakkında yardımcı olabilecek yöntemleri yalın bir biçimde sistemi uygulamak isteyen işletmelere katkı sağlamayı amaçlamaktadır.

Bu tez çalışması, ülkemizdeki tüm kurum ve kuruluşlarda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin sertifikasyonunu ve karşılaşılan güçlükleri anlamak açısından önem arz etmektedir.

3.1.3. Kapsam ve Sınırlılıklar

Araştırmanın evreni, Batı Karadeniz Bölgesindeki ISO/IEC 27001:2013 sertifikasına sahip beş adet kuruluştan oluşmaktadır. Bu kapsamda dört kuruluşla görüşme gerçekleştirilmiş olup diğer kuruluşla iletişim kurulamadığından dolayı çalışma dışı bırakılmıştır.

Sertifika sahibi kuruluşların Batı Karadeniz Bölgesi'nde çok az olması araştırmanın önemli kısıtlarındandır.

Bu konuda yapılan akademik çalışmaların az olması, bilgi güvenliği hususunun hassas bilgiler içermesi ve kuruluşların bu konudaki araştırmalara ihtiyatlı yaklaşmaları da bu çalışmanın güçlüklerindendir.

Araştırma kapsamında olan ve bölgede sektörün öncü ve önemli bir kuruluşun araştırmaya dahil edilememesi elde edilen bulguların karşılaştırılması, katkı düzeyinin artırılması ve bilgi birikiminin aktırılamaması araştırmanın kısıtlarındandır.

3.1.4. Araştırma Soruları

Kuruluşlar neden ISO/IEC 27001 sertifikasına ihtiyaç duyarlar?

ISO/IEC 27001 sertifikasına sahip kuruluşların başarısına katkıları nelerdir?

Sertifika öncesi ve sonrasında karşılaşılan problemler ve çözüm önerileri nelerdir?

ISO/IEC 27001 yönetim sistemine sahip olan firmalar başarılarını bilgi güvenliği bilincini sağlamış çalışanlara mı dayandırırlar?

ISO/IEC 27001 bilgi güvenliği yönetim sistemi için insan kaynakları önemli bir faktör müdür?

3.2. Yöntem

Bu araştırmada nitel araştırma yöntemi kullanılmıştır. Görüşmeler, içinde bulunduğumuz pandemi sürecinden dolayı telefon ve zoom programı ile kurumun BGYS komitesinde görevli olan çalışanlar ile gerçekleştirilmiştir. Görüşme yapılan üç kuruluşun isimlerinin açıklanmaması nedeniyle kuruluşların adları A, B ve C şeklinde kodlanılmıştır. Tat Metal firma isminin görünmesinde hiçbir sakınca olmadığını belirttiğinden kodlanmamıştır.

3.2.1. Veri Toplama Yöntemi

Nitel araştırma yöntemine dayalı olarak yapılan bu çalışmanın verileri, yarı yapılandırılmış görüşme tekniği ve derinlemesine mülakat ile toplanmıştır. Bu teknikte konuyla ilgili önceden hazırlanan belli konu başlıkları ya da sorularla görüşme gerçekleştirilir. Yarı yapılandırılmış görüşme tekniği, önceden hazırlanmış görüşme formuna bağlı olarak sürdürülmesi sebebiyle daha sistematik ve karşılaştırılabilir bilgi sunar.

3.2.2. Veri Analiz Yöntemi

Araştırmada elde edilen veriler nitel veri analizi şekli olan betimsel analiz tekniği kullanılarak analiz edilmiştir. Betimsel analiz tekniğinde elde edilen veriler daha önceden belirlenen başlıklar altında özetlenir ve yorumlanır.

3.3. Araştırmanın Bulguları

Bu kısımda, Bilgi Güvenliği Yönetim Sistemi Belgelendirilmesi: Batı Karadeniz'de Bir Alan Araştırması çalışmasının bulgularına yönelik değerlendirmeler sunulmuştur. Bu araştırmada elde edilen verilerin analizi kapsamında bulgular BGYS Öncesi Hazırlık Süreci, BGYS Başvuru Aşaması, BGYS Sonrası, Düzeltici Faaliyetler Ve İyileştirme olarak dört başlık altında incelenmiştir.

3.3.1. Sistem Öncesine İlişkin Bulgular

Araştırma kapsamında Batı Karadeniz Bölgesinde ISO/IEC 27001 sertifikasına sahip dört kuruluş ile gerçekleştirdiğimiz görüşmeler sonucunda, BGYS öncesi hazırlık sürecinde kuruluşların **BGYS'yi kurma amaçları**; kritik bilginin korunması ve standardın yönlendirmeleri ile mevcut IT süreçlerini iyileştirmek, IT süreçlerinin daha kaliteli bir şekilde yürütülebilmesi, yasal mevzuatların ve şartların gereksinimlerini karşılayabilmek, uluslararası bir standart olması ve tüm dünyada geçerliliğinin olması, bilgi güvenliğinin sağlanması, işletmenin yürüttüğü genel faaliyetler ve yasal gereklilikler olarak ifade edilmiştir.

Danışmanlık firmasından destek alma; üç kuruluş bu süreçte bir danışmanlık firmasından destek almış, diğer kuruluş sahip olduğu yetkin bir IT departmanı sayesinde danışman firmaya gerek duymamıştır.

BGYS başvuru komitesinin yeterliliği; ISO/IEC 27001 standardının kurulması, uygulanması, yönetimi ve performansının değerlendirilmesi görevlerini yürüten BGYS komitesi; A ve Tat Metal kuruluşlarında BGYS hakkında bilgiye sahip değildi ve danışman firma tarafından eğitimler almışlardır. B kuruluşu ve C kuruluşlarında oluşturulan BGYS komitesi yeterli bilgiye sahipti ve komite üyelerinin eğitimi için herhangi bir destek almamışlardır.

BGYS hazırlık sürecinde karşılaşılan sorunlar; standart konusuna hakim, bilgisi ve tecrübesi yeterli düzeyde olmayan bir danışmanla çalışmanın zorluğu, denetçinin

kişisel yorumları sebebiyle kuruma özgü bilgi güvenliği yönetim sistemi uygulamalarını kavrayamama, doküman ve bilgi eksikliğinden kaynaklı zorluklar, yetkin bir IT departmanına sahip olması gerekliliği olarak belirtilmiştir.

Bu süreçte kuruluşların **önerileri,** bu alanda yetkin IT yetkilisi ile çalışmak, üst yönetimin desteğini alarak ISO/IEC 27001'in bütün kurumda benimsenmesini sağlamak, kuruma özgü bir BGYS oluşturmak ve daha önce bu sistemi uygulamış kuruluşlarla bilgi alışverişinde bulunmak olarak belirtilmiştir.

3.3.2. Sistemin Başvuru Evresine İlişkin Bulgular

BGYS kapsamını belirleme; bu aşamada A kuruluşu kapsamını Yetkilendirilmiş Yükümlü Statüsü (YYS) işlemlerinde görev alan departmanlar olarak belirlemiş diğer departmanları hariç tutmuştur. B kuruluşu, Bilgi Sistemleri Departmanı takip sorumluluğunda olan departmanları belirlemiştir. Tat Metal, İnsan Kaynakları, Bilgi İşlem, Muhasebe, Finans, İdari İşler, Satın Alma, Satış ve Pazarlama, Dış Ticaret (İthalat ve İhracat), Lojistik departmanlarını dahil etmiştir. C kuruluşu kapsamı ERP, IK, AR-GE, Satın Alma, Muhasebe, Sevkiyat, Satış ve Mali işler olarak belirlemiştir.

Yapılan değerlendirmede çoğu kuruluş bu sistemi tüm faaliyetlerinde uyguladığı sonucunu çıkarmakla birlikte bazı büyük organizasyonların sadece bir biriminde veya bilgi sistemleri takip sorumluluğunda olan bölümlerinde bu sistemi uyguladıkları belirlenmiştir.

Üst yönetimin katkısı; bütün kuruluşlar üst yönetimden tam destek görerek hiçbir zorlukla karşılaşmamıştır.

Varlıkları belirleme; kuruluşlar varlıklarını belirlerken gizliliği olan kritik bilgilerden başlayarak genele doğru bir sıralama yapmışlardır. Kuruluşun önemli bilgileri bilgi güvenliği açısından korunması gereken en önemli varlıklar olmuştur.

Politika ve prosedürleri belirleme; kuruluşların politika ve prosedürleri standardın gereklerine göre hazırladıkları görülmektedir.

Risk belirleme; kuruluşlar bilgi güvenliğini tehdit eden tehlikeleri belirledikten sonra varlık değeri, riskin etkisi, olma sıklığı değerleri ile oluşturulan bir tablo yardımıyla risklerini belirlemişlerdir. Riskler, kurum kültürü ve kurumun bilgi güvenliği açısından

mevcut durumu göz önünde bulundurularak, risk değerlendirme prosedürü baz alınarak, gizliliği, bütünlüğü, erişilebilirliği, olasılığı etkileyip etkilemediğine bakılarak belirlenmiştir.

Ek-A Kontrol maddeleri; verilen cevaplar doğrultusunda kuruluşlar riskleri azaltmak ya da ortadan kaldırmak için Ek-A maddelerinin bir çoğunu uyguladığı görülmektedir. B kuruluşu, A.9.4.5 Yazılım geliştirme ile ilgili maddeler ve A.10.1, A.10.2 Kriptografik Kontrollerle ilgili maddeleri uygulamadıklarını belirtmişlerdir.

İlk başvuruda belgeyi alabilme; A, B ve Tat Metal kuruluşları ilk başvuruda belgeyi alabilmişler, C kuruluşu ise bilgi işlem odasındaki kabinet yeri ile ilgili sorunlar sebebiyle ilk başvuruda belgeyi alamamıştır.

Bu aşamada yaşanan temel zorluklar;

Çalışanın bilgi güvenliği konusunda yeterli bilgiye sahip olmaması, yeni sistemin getirdiği yeni kurallar, daha kontrollü ve sistematik iş akışı sebebiyle çalışanların önyargısı ile karşılaşılmıştır. Standardın yeni olduğu ilk zamanlarda Türkiye'de Türkçe doküman yetersizliğinden dolayı bazı kavramların tam anlaşılamaması da bu aşamada yaşanılan zorluklardan olmuştur.

Öneriler;

Bu aşamada çalışanları sürece dahil ederek sistemin sahiplenilmesini, kendi kurumlarına özgü uygulama yöntemlerini geliştirmelerini, bilgi güvenliği konusunda yetkin bir IT departmanı kurulmasını önermektedirler.

3.3.3. Sistem Sonrası Evreye İlişkin Bulgular

BGYS Uygulama süreleri; Bilgi güvenliği yönetim sistemi Türkiye'de 2005 yılında uygulanmaya başlanmıştır.Tat Metal 5, A kuruluşu 8, C kuruluşu 9, B kuruluşu 11 yıldır uygulamaktadır. Buna göre kuruluşların uygulama yılı açısından oldukça önemli adımlar attığından söz edilebilir.

BGYS sonrası sistemin sağladığı faydalar; kritik bilgilerin güvenle korunması oluşturulmuş, çalışanların bilgi güvenliği farkındalığı oluşmuş ve karşılaşılan zorluklar standardın bir gerekliliği olarak ifade edildiğinde uygulamalar daha kolay kabul

görmüştür. Bu sistem ile borsada işlem gören şirketlerin tabi olduğu denetimler sırasında gelen soruların cevaplanmasında kolaylık sağlanmıştır.

Belgeye sahip olmanın kurumsal prestije katkısı; A kuruluşu, belgeyi aldıkları zaman Türkiye'de bu büyüklük ve ölçekte hiçbir kuruluşun belgeye sahip olmadığını bu durumun kuruma büyük bir prestij kazandırdığını ifade etmiştir. B kuruluşu, sektörde sertifikaya sahip ilk çimento fabrikası olduğunu belirtmiştir. Tat Metal ve C kuruluşu global çapta adımızı duyurarak rekabetçi pazar payında yerimizi almış olduk ifadelerini kullanmışlardır. Bu verilere göre bilgi güvenliği yönetim sistemi kuruluşların kurumsal prestijinin artmasına büyük katkı sağladığından söz edilebilir.

BGYS'nin uygunluğu ve etkinliğinin tespiti; kuruluşlar BGYS'nin uygunluğunu ve etkinliğini iç denetim, dış denetim, penetrasyon testleri ve risk işleme faaliyetlerini gerçekleştirerek yapmaktadırlar. İç denetim ve dış denetim kuruluşların verdiği ortak cevaplar olmuştur.

İç denetim; verilen cevaplar doğrultusunda kuruluşların hepsi iç denetimleri kurum içerisinden iç tetkik belgesi alan çalışan tarafından gerçekleştirmiştir. İç denetimleri saha, doküman, soru ve fiziksel şekilde gerçekleştirdiklerini belirtmişlerdir.

BGYS'nin kuruma ekstra iş yükü getirmesi; sistemin uygulanmasının kuruma ekstra iş yükü getirdiği verilen ortak cevap olmuştur. C kuruluşu; anlık yetkilendirme istekleri, çeşitli onaylardan geçerek yapıldığı için sürecin uzadığını, B kuruluşu ise kurum içerisinde BGYS' nin sadece IT'nin sorumluluğundaymış gibi görünmesi sebebiyle sistemin uygulanmasının kuruma olumsuz etkileri olabileceğini belirtmişlerdir. Ancak sonrasında standartı uygulamalarının çalışanlara getirdiği iş yükü, standardın sağladığı faydalar ile karşılandığında oldukça az ve kabul edilebilir duruma gelmiştir.

Destek alma; Tat Metal ve C kuruluşu bu süreçte danışmanlık firmasından destek almamışlardır. A ve B kuruluşları gerekli olduğunda destek aldıklarını belirtmişlerdir.

BGYS'nin diğer yönetim sistemleri ile uyumlaştırılması; görüşme gerçekleştirilen tüm kuruluşlara bakıldığında bünyelerinde ISO/IEC 27001 ile birlikte diğer yönetim sistemlerinin de mevcut olduğu görülmektedir. ISO/IEC 27001'in diğer yönetim sistemleri ile uyumlaştırılırken A kuruluşu, Tat Metal ve C kuruluşu hiçbir sorunla

karşılaşılmadığını belirtmişlerdir. A kuruluşu, risk yönetimi, bağlam, iç ve dış hususlar gibi konularda kurum içi öncü çalışmanın hep ISO/IEC 27001 standardı kapsamında gerçekleşmesinden ötürü diğer standartlar için gerekli alt yapıyı sağlamış, yaşanabilecek sorunları yaşamış hatta sorunlara ilişkin çözümleri de bulmuş olduğundan diğer yönetim sistemleri ile ilgili bir sorun yaşamadıklarını belirtmişlerdir. B kuruluşu Ek-A maddelerinden dolayı zorluk çektiklerini ifade etmişlerdir. Ayrıca kuruluş B kurumun petrol çimentosu üretebilmesi için API yönetim sistemi belgesinin alınmasında fayda sağladığını belirtmiştir.

Eğitim ve bilinçlendirme çalışmaları; kuruluşlar eğitim ve bilinçlendirme çalışmalarını belirli zaman aralıklarında oryantasyon eğitimi, farkındalık eğitimi, bilgi güvenliği bülteni, bilgi güvenliğine ilişkin duyurular ve bilgi güvenliği broşürleri düzenleyerek yaptıklarını belirtmişlerdir. Bilgi güvenliği yönetim sistemi tamamen çalışan odaklı yürütüldüğünden çalışanların sürekli eğitimlerle bilgilendirilmesi etkin bir bilgi güvenliği açısından önemlidir.

Çalışanlar üzerinde bıraktığı etki; Bilgi Güvenliği Yönetim Sisteminin uygulanmasının ardından çalışanlar üzerinde bıraktığı etki incelendiğinde A kuruluşu ve Tat Metal, yeni uygulamalar ile birlikte mevcut uygulamaların daha zorlayıcı hale gelmesi ile çalışanın olumsuz yönde etkilendiğini ifade etmiştir. B kuruluşu, veri güvenliği açısından çalışanların yüksek düzeyde bilinçlendiğini ifade etmiştir. C kuruluşu, çalışanların üzerinde çalıştıkları verilerin güvenli olduğunu bilmelerinin çok önemli olması sebebiyle çalışanın uyum içinde çalışarak hiçbir zorlukla karşılaşılmadığını belirtmiştir.

Sistemin kurum için getirdiği yük ve maliyete değecek kadar fayda sağlayıp sağlamadığı; A, B ve C kuruluşları katkı sağladığını Tat metal ise her ne kadar çok faydası olsa da bizim kuruluşumuz için öncesi ile sonrası arasında pek bir fark olmamıştır beyanında bulunmuştur.

Çalışanların BGYS'ye bakışı ve ilgisi; bu süreçte çalışanların BGYS' ye bakışı ve ilgisi sorgulandığında çalışanların hem kurum içinde hem de özel hayatlarında bilgi güvenliği farkındalıklarının arttığı görülmüştür.

Ara denetimlerde kuruluşların karşılaştığı sorunlar; Belgelendirme kuruluşunun yaptığı ara denetimlerde kuruluşların karşılaştığı sorunları incelediğimizde A kuruluşu,

denetçilerin kendi bakış açılarına ve daha önce görmüş / uygulamış oldukları sistemlerin birebir aynısını beklemesi ve bunların dışındaki uygulamalara karşı ön yargılı yaklaşmaları başlıca yaşadığımız sorundur beyanında bulunmuştur. B kuruluşu ise ara denetimlerde bir önceki yıl çıkan minör uygunsuzluklar için alınan aksiyonların yeterlilikleri sorgulandığından sorunlar yaşadıklarını ifade etmiştir. C kuruluşu ve Tat Metal ara denetimlerde sorun yaşamamıştır.

Karşılaşılan zorluklar; BGYS sonrası kurumlarda karşılaşılan zorlukları incelediğimizde A kuruluşu, işlerin daha kontrollü, prosedürdeki tüm adımların ve bunlara ilişkin bütün kayıtların tutularak oluşturulması yaşadığımız en büyük zorluklardandır, şeklinde ifade etmiştir. B kuruluşu, BGYS'nin sürecinin yönetimi sadece IT çalışanlarında olduğu için iş yükünü artırmaktadır ifadesinde bulunmuştur. Tat Metal, belgelerin devamlılığı ve takip iş yükünü artırdığından dolayı zorluklar yaşadık ifadesinde bulunmuştur. C kuruluşu ise hiçbir zorlukla karşılaşmamıştır.

Öneriler; kuruluşların bu aşamada; üst yönetimin iradesi ve çalışanların desteğini mutlaka yanlarına almaları, BGYS organizasyonunun (ekibinin) mutlaka BGYS kapsamını ilgilendiren birimlerden oluşması sağlanmalı, BGYS konusunda bilgili çalışan tarafından ekibin oluşturulması sağlanmalı, kuruluşların bünyelerinde IT departmanı kurarak, bu alanda en az 10 yıl çalışmış olan kişileri tercih etmeliler şeklinde tavsiyede bulunmuşlardır.

3.3.4. Düzeltici Faaliyet ve İyileştirme

Bu aşamada A kuruluşu ve Tat Metal, tüm uygunsuzluklar için; B kuruluşu, iç denetimler, dış denetimler ve risk değerlendirme sonucunda çıkan uygunsuzluklar için düzeltici faaliyet düzenlemiştir. C kuruluşu ise hiçbir uygunsuzluk yaşamamak için çok uç noktalarda önlem aldıklarını belirtmiştir. Karşılaşılan uygunsuzlukların tekrar edilmemesi için eğitim ve iyileştirilmelere yer verilmiştir.

Penetrasyon testi, işletmelerin ve kurumların güvenlik açıklıklarının ve risklerin uzman kişiler tarafından tespit edilip açıklıkların raporlanmasıdır. A, C ve B kuruluşları yıl içinde belirli aralıklarla penetrasyon testi yaptıklarını Tat Metal ise şimdiye kadar yapmadıklarını ama 2021 yılı içerisinde yapacaklarını ifade etmişlerdir. Penetrasyon testleri siber tehditlerin neden olacağı olumsuz sonuçları en aza indirmek açısından önemlidir.

Tablo 10. Bulgular Tablosu

Sorular	Cevaplar			
	Kuruluş A	**Kuruluş B**	**Kuruluş C**	**Tat Metal**
BGYS ÖNCESİ HAZIRLIK SÜRECİ				
1. Kurumunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini kurmaya neden ihtiyaç duydunuz?	Kritik bilginin korunması, standardın yönlendirmeleri ve mevcut IT süreçlerimizi iyileştirmek olarak ifade edilmiştir.	Mevcut IT süreçlerinin daha kaliteli bir şekilde yürütülebilmesi ve yasal mevzuatların ve şartların gereksinimlerini karşılayabilmek olarak ifade edilmiştir.	Uluslararası standart olması ve bütün dünyada kabul görmesi olarak ifade edilmiştir.	Bilgi güvenliğinin sağlanması, işletmenin yürüttüğü genel faaliyetler ve yasal gereklilikler olarak ifade edilmiştir.
2. Hazırlık için danışman firmadan yararlandınız mı? Eğer evetse bu süreç sizin için yararlı oldu mu? Hayırsa bu süreçte zorluk çektiniz mi? Bu yöntemi önerir misiniz?	Evet, danışman firmadan yararlanılmıştır. Yönetim sisteminin gerekliliklerini şirket süreçlerimize dâhil etme, iyi uygulamalar ve tecrübe paylaşımı konusunda, süre, standarda ilişkin çalışan yetkinliği gibi konularda kısıt mevcut ise danışmanlık alınması önerilmektedir.	Evet, danışman firmadan yararlanılmıştır. Sürecin daha kolay ilerlemesi için önerilmektedir.	Kuruluş danışman firmadan yararlanmadığını belirtmiştir.	Evet, danışman firmadan yararlanılmıştır. Süreçlerin daha kolay yürütülmesi açısından önerilmektedir.
3. Başvuru için oluşturduğunuz BGYS komitesi yeterli bilgiye sahip miydi? Bu konuda eğitim danışmanlık hizmeti aldınız mı?	BGYS Komitesi yeterli bilgiye sahip olmadığı için eğitim danışmanlık desteği alınarak ekibe eğitimler verildiği belirtilmiştir.	BGYS Komitesinin yeterli bilgiye olmadığı ifade edilmiştir.	BGYS Komitesi yeterli bilgiye sahipti ve eğitim almaya gerek duyulmamıştır.	BGYS Komitesi yeterli bilgiye sahip olmadığı için eğitim danışmanlık desteği alınarak ekibe eğitimler verildiği belirtilmiştir.

4. Bu aşamada karşılaşılan zorluklar nelerdir?	Konusuna hâkim IT süreçlerinde çalışmış tecrübeli danışman bulmanın zorluğu konusunda zorluk yaşanmıştır.	Denetçilerin yaklaşımlarında kişisel yorumlarını dayatmaları konusunda zorluk yaşanmıştır.	IT departmanı olarak yeterli bilgiye sahip olan kuruluş C zorluk yaşamamıştır.	Belge ilk zamanda alındığı için yeterli bilgi ve doküman eksiliğinden dolayı zorluk yaşanmıştır.
5. Hazırlık süreci için bir öneriniz var mı?	IT operasyonlarında görev almış danışmanlardan hizmet almak ve üst yönetimin desteğini almak, önerilmiştir.	Standardı iyi anlamak ve kuruma özgü yöntemler uygulanmalıdır önerisinde bulunmuşlardır.	Bu alanda uzun yıllar hizmet veren yetkin IT yetkilisi bulunmasını önerilmektedir.	Daha önce bu belgeyi almış bir firma ile keşif çalışması yapılmalı ve bilgi alışverişinde bulunulmalı önerisinde bulunmuşlardır.
BGYS BAŞVURU AŞAMASI				
1. Kurumunuzda oluşturduğunuz ISO/IEC 27001 BGYS' nin kapsamı nedir? Hariç tutmaları gerekçelendirdiniz mi?	Standard maddeleri hariç tutulamıyor. Belge anlamında kapsam, Yetkilendirilmiş Yükümlü Statüsü (YYS) işlemlerinde görev alan departmanlar olarak belirlenmiştir.	Kapsam; Bilgi Sistemleri Departmanı takip sorumluluğunda olan verilerin korunmasını kapsamaktadır. Standartın ana maddeleri hariç tutulamazken Ek -A maddelerinde kurumumuz için uygulanabilirliği olmayan maddeleri hariç tutulmuştur.	Kapsam olarak, ERP, IK, AR-GE, Satın Alma, Muhasebe, Sevkiyat, Satış ve Mali işler bulunmaktadır.	Kapsam; İnsan Kaynakları, Bilgi İşlem, Muhasebe, Finans, İdari İşler, Satın Alma, Satış ve Pazarlama, Dış Ticaret (İthalat ve İhracat), Lojistik departmanlarından oluşmaktadır.
2. Üst yönetim bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunup destekledi mi? Varsa yaşadığınız	Gerek kurulum aşamasında, gerekse sonrasında üst yönetimin desteğini görmüşlerdir. Bu konuda zorluk yaşamamışlardır.	Üst yönetimin desteğini görmüşler ve bir sıkıntı yaşamamışlardır.	Üst yönetimin desteğini görmüşler ve bu konuda zorluk yaşamamışlardır.	Üst yönetimin desteğini görmüşler ve bir sıkıntı yaşamamışlardır.

zorluklar nelerdir?				
3. Bilgi Varlıklarınızı belirlerken nelere dikkat ettiniz?	İlk olarak kurum için kritik öneme sahip bilgileri sonra bu bilgilerin tutulduğu, saklandığı ortamlar , transferinde görev alan sistem / cihazlar, kaynağı olan kişiler, işlendiği cihazlar, işleyen sistemler göz önüne alınmıştır.	Muhasebe, üretim, satış, satın alma, kalite, insan kaynakları vb. modüllerde oluşan bilgiler, kullanıcı dokümanları, arşivler, dolaplar, şirket web sitesi olarak belirlenmiştir.	Gizliliği olan bilgilerden başlayarak genel bilgilere doğru belirlenmiştir.	Firmanın sahip olduğu her şey varlık olarak belirlenmiştir.
4. Bilgi Güvenliği Politikası ve prosedürler neleri kapsıyor, nasıl bir sistemle bunları hazırladınız?	Standardın gerekli gördüğü doküman yapısını ve kuruma yön gösteren, yönlendiren yazılı kaynakları kapsayan bilgi güvenliği politikası ve ve prosedürler bir yazılım üzerinde hazırlanmıştır.	Standart maddelerine göre oluşturulan bilgi güvenliği politikası ve prosedürleri doküman yönetim sistemi yazılımı ile kullanıcılara duyurulmuş ve bu yazılım üzerinden doküman yönetimi gerçekleştirildiği ifade edilmiştir.	Kurum politikasının en önemli aşaması yetkilendirmelerdir. Yetki dahilinde olmayan bütün bölümlere erişimlerin kısıtlandığı ifade edilmiştir.	BGYS kapsamındaki her şeyi kapsadığı ifade edilmiştir.
5. Kurumunuzdaki riskleri belirlemek için hangi yöntemleri kullanıyorsunuz?	Kurumundaki riskler; risk puanını hesaplarken varlık değeri, riskin etkisi (finansal, operasyonel, paydaş açısından, yasal olmak üzere 4 kriter göz önünde	Bilgi güvenliğini tehdit eden tehlikeler tanımlandıktan sonra risk puanlaması yapılmaktadır. Bu riskin olasılığı, sıklığı ve şiddeti göz önünde bulundurularak aksiyon	Risk değerlendirme tablosu düzenleyerek riski belirlediklerini ifade etmişlerdir.	Varlık değeri, riskin etkisi ve olma sıklığı değerleri ile riske puan vererek risk analiz tablosu oluşturulmaktadır.

	bulundurulmaktadır.) ve olma sıklığı değerleri göz önünde bulundurularak belirlendiği ifade edilmiştir.	alınıp alınmayacağına karar verileceği belirtilmiştir.		
6. Kabul edilebilir veya risk iyileştirmesi gerektirecek seviyede öngörülmüş risk seviyesini nasıl belirlediniz?	Kurum kültürü ve kurumun bilgi güvenliği açısından mevcut durumu göz önünde bulundurularak kabul edilebilir risk seviyesi belirlenmiştir.	Risk değerlendirme Prosedürü oluşturularak belirlenmiştir.	Kurumun bilgi güvenliği durumunu baz alarak kabul edilebilir risk seviyesi belirlenmiştir.	Gizliliği, bütünlüğü, erişilebilirliği, olasılığı yani gerçekleştirme olasılığını etkiliyor mu diye risklere puan vererek belirlenmiştir.
7. Riskleri azaltmak ya da ortadan kaldırmak için ISO/IEC 27001 Ek – A maddelerinden hangisini seçtiniz?	ISO/IEC 27001 Ek – A maddelerinden birçoğunu kullandıklarını belirtmişlerdir.	A.9.4.5 Yazılım geliştirme ile ilgili maddeler, A.10.1, A.10.2 Kriptografik Kontrollerle ilgili maddeler haricinde diğer kontrol maddelerini seçtiklerini belirtmişlerdir.	Ek-A maddelerinin hepsini uyguladıklarını ifade etmişlerdir.	Ek-A maddelerinin hepsi uygulandığı ifade edilmiştir.
8. İlk başvurunuzda belgeyi alabildiniz mi? Eğer alamadıysanız neden alamadınız?	İlk başvuruda belgeyi aldıklarını ifade etmişlerdir.	İlk başvuruda belgeyi aldıklarını ifade etmişlerdir.	Bilgi işlem odasındaki kabinet yeri ile ilgili ufak sorunlar sebebiyle ilk başvuruda belgeyi alamadıklarını ifade etmişlerdir.	İlk başvuruda belgeyi aldıklarını ifade etmişlerdir.

9. Bu aşamada yaşadığınız temel zorluklar nelerdir?	Çalışanların yeniliklere karşı ön yargılı davranması olarak belirtmişlerdir.	Standardın Türkiye'de yeni olduğu ilk zamanlarda Türkçe doküman yetersizliği sebebiyle bazı kavramların anlaşılmasında, kurulum ve denetimler esnasında zorluklar yaşanılmıştır	Yetkin bir IT departmanına sahip oldukları için zorluk yaşanılmamıştır.	Çalışanların yeterli bilgiye sahip olmaması, yeni iş tarzı, uyulması gereken yeni kurallar, daha kontrollü çalışmak bu aşamada yaşanılan zorluklar olmuştur.
10. Bu aşamada önerileriniz nelerdir?	Çalışanları sürecin içine dahil ederek yapılan çalışmaların neden yapıldığını, bize getireceği faydaları kendileri ile paylaşmak konusunda öneride bulunmuşlardır.	Kuruma özgü uygulama yöntemleri belirlenmesi önerisinde bulunmuşlardır.	Yetkin bir IT departmanına sahip olmak ve çalışanlarda farkındalık oluşturularak sürece dahil etmek önerilerinde bulunmuşlardır..	Kuruma özgü uygulama yöntemleri belirleme önerisinde bulunmuşlardır.
BGYS SONRASI				
1. Bilgi Güvenliği Yönetim Sistemi kuruluşunuzda kaç yıldır uygulanmaktadır?	Kasım 2013 yılında alınmıştır.	2009 yılından 2020 yılına kadar uygulanmıştır.	Uzun süredir uygulanan BGYS sertifikamız 2019 yılında yenilenmiştir.	2016 yılından itibaren uygulanmaktadır.

2. Bu sistemin kurumunuzun bilgi güvenliği açısından temel yararları nelerdir?	Standart, kurum ve çalışanlar için bir rehber niteliğindedir. Kullanıcılar tarafından bilgi güvenliği faaliyetleri standardın bir gereği olarak görüldüğü için daha çabuk kabul gördüğü ifade edilmiştir.	Borsada işlem gören şirketlerin denetiminde bu belgenin olması kolaylık sağlamaktadır. kullanıcılar tarafından ön yargı ile karşılanan bazı bilgi güvenliği faaliyetleri standardın gerekliliği olarak ifade edildiğinde daha çabuk kabul gördüğü ifade edilmiştir.	Hem çalışan hem de yönetim açısından bilginin güvenle saklanması olarak ifade edilmiştir.	Farkındalık yaratıldığı, kullanıcıların daha dikkatli olmaya başladığı ve bilginin öneminin arttığı ifade edilmiştir.
3. İşletmenin kurumsal prestijine ne tür katkılar sağladı?	Kurum belgeyi aldığında Türkiye'de bu ölçek ve büyüklükte hiçbir kuruluşun bu belgeyi almamış olması kuruluş A için büyük bir prestij olmuştur.	Sektörde BGYS belgesi olan ilk çimento fabrikası olması nedeniyle kuruma prestij sağlamıştır.	Uluslararası geçerliliği olan bir standard olmasından dolayı kuruluşumuz global pazarda yerini almıştır.	Bu belge, ile global çapta tanınırlığımız ve pazardaki prestijimiz artmıştır.
4. Kurumunuzda BGYS' nin uygunluğunun ve etkinliğinin tespitini nasıl yapıyorsunuz?	İç ve dış denetimler, periyodik olarak yapılan penetrasyon testleri, risk işleme faaliyetleridir.	İç denetimler ve dış denetimlerle yapılmaktadır.	İç ve dış denetimlerle yapılmaktadır.	İç ve dış denetim ile yapılmaktadır.
5. Kurumunuzda iç denetimi kendiniz mi yoksa danışman firma mı yapıyor? İç denetimi nasıl yapıyorsunuz?	İç denetim, eğitim almış çalışanlar tarafından yılda en az 1 kez saha ve doküman bazlı olarak yapılmaktadır.	İç denetçi sertifikası alan kendi çalışanlarımız tarafından saha ve doküman içerikli gerçekleştirilmektedir.	IT departmanı yapmaktadır.	Kurum içinde iç tetkik belgesi olan çalışanlar ile her bölüme tek tek gidilerek saha, soru ve fiziksel denetim şeklinde yapılmaktadır.

6. Sistemin uygulanması kurum üzerindeki iş yükünü olumlu ya da olumsuz yönde etkiledi mi? Bunlar nelerdir?	İlk kurulum ekstra bir iş yükü getirmektedir. İş yükü, standardın sağladığı faydalar ile karşılandığında oldukça az ve kabul edilebilir bir durumda olduğu ifade edilmiştir.	Olumsuz yönü, kurum içerisinde BGYS'nin sadece IT' nin sorumluluğundaymış gibi görünmesi ve IT'deki çalışan sayısının az olması iş yükünü arttırdığı, olumlu yönü ise IT ihtiyaçlarını bilgi güvenliği kapsamında değerlendirerek daha kolay temin edebilmek olarak ifade edilmiştir.	Anlık yetkilendirme istekleri, çeşitli onaylardan geçerek yapıldığı için sürecin biraz uzadığını ve bunun da aksaklıklara yol açtığı ifade edilmiştir.	Kuşkusuz olumlu etkiliyor ama bu belgeler iş yükü çıkartıyor olarak ifade edilmiştir.
7. Uygulama sürecinde danışmanlık firmasından destek alıyor musunuz? Evetse bu oran ne kadardır?	Uygulama sürecinde zaman zaman belli konularda danışmanlık alınmıştır.	Akıllarına takılan sorular olduğu zaman düşük bir oranda yardım aldıklarını ifade etmişlerdir.	Danışman firmadan yardım alınmamıştır.	Belgeyi aldıktan sonra destek almamışlardır.
8. Kuruluşunuzda diğer yönetim sistemlerini kullanıyor musunuz? Eğer kullanıyorsanız bilgi güvenliği yönetim sistemi bunlarla uyumlaştırıldı mı? Uyumlaştırılırken nasıl sorunlarla karşılaştınız?	Kuruluşta 8 farklı yönetim sistemi mevcuttur ve uyumlaşma konusunda sorunla karşılaşılmamıştır.	Ek A maddelerinden dolayı uyumlaştırmada zorluk çekilmiştir.	BGYS haricinde Kalite Yönetim Sistemi mevcuttur. Sorun yaşanmamıştır.	Çevre Yönetim Sistemi, İş Sağlığı ve Güvenliği Sistemi Yönetimi, Kalite Yönetim Sistemi, Otomotiv Kalite Yönetim Sistemi, Enerji Yönetim Sistemi vardır ve hiçbir sorunla karşılaşılmamıştır.

9. Kurumunuzda eğitim ve bilinçlendirme çalışmalarını hangi aralıklarla, nasıl yapıyorsunuz?	Periyodik olarak oryantasyon eğitimi, farkındalık eğitimi, bilgi güvenliği bülteni, bilgi güvenliğine ilişkin duyurular ve bilgi güvenliği broşürleri şeklinde yapılmaktadır.	Belirli aralıklarla ve tüm çalışanlara farkındalık eğitimleri verilmektedir.	3 ayda bir farkındalık eğitimleri düzenlenmektedir. Ayrıca bilgi güvenliği ile ilgili broşürler hazırlanıp duyurular yapılmaktadır.	Yılda bir kez farkındalık eğitimi verilmektedir.
10. Kurumunuzda kontrol sürecini nasıl yaparsınız?	Gözden geçirme toplantıları, iç de dış denetimler, dış kaynak ile yapılan penetrasyon testleri ile yürütülmektedir.	İç tetkikler, yönetim gözden geçirme ve dış tetkiklerle gerçekleştirilmektedir.	Sunucu ve İstemci taraflı olarak kontrol işlemleri yapılmaktadır.	İç denetim ve dış denetim ile yapılmaktadır.
11. Bilgi Güvenliği Yönetim Sisteminin uygulanması çalışanları nasıl etkiledi? Karşılaşılan zorluklar ne oldu?	Yeni uygulamalar ve mevcut uygulamaların daha zorlayıcı hale gelmesi çalışanı olumsuz yönde etkilemiştir.	Çalışanın yüksek düzeyde bilinçli olmasını sağlamıştır.	Çalışanların üzerinde çalıştıkları verilerin güvenli olduğunu bilmeleri çok önemli olduğu için tam uyum içinde olduklarını ifade etmişlerdir.	Standart sonrası koyulan bazı kurallara (masaüstü temizliği, evrakların kırpılması, şifre zorunluğu, ekran kitleme gibi) çalışanın uymak zorunda kalması olumsuz tepkilere sebep olmuştur.
12. Bu sistem kurum için getirdiği yük ve maliyete değecek kadar fayda sağladı mı?	Getirdiği yük ve maliyetin çok üstünde bir faydası olduğunu belirtmişlerdir.	API denetimlerinde ve mali denetimlerde BGYS' nin olması fayda sağlamışır.	Çalıştığımız firmaların çoğu bu sertifikayı zorunlu tuttuğundan yük ve maliyet getirisi ne olursa olsun sistemin sürekliliği kaçınılmaz olmuştur. Bu yüzden yük ve maliyete değecek kadar fayda sağlamıştır.	Tabikî bu sistemin bir çok faydası vardır. Fakat bizim kuruluşumuzda öncesi ile sonrasın arasında pek bir fark olmamıştır.

13. İşleyiş sürecinde yönetimin bakışı ve desteği ne yönde değişti?	Hem kurulum hem de işleyiş sürecinde yönetim tarafından oldukça destek görülmüştür.	İşleyiş sürecinde YGG toplantılarında BGYS hedefleri için gerekli aksiyonlara kaynaklar sağlanıyordu.	Üst Yönetim sürecin başından beri tam destek vermiştir.	Yönetim her aşamada desteğini tam göstermiştir.
14. Uygulama sürecinde ilgili çalışanların BGYS' ye bakışı ve ilgisi ne yönde değişti?	Kullanıcı farkındalığının arttığı ve bakış açısının olumlu yönde değişti ifade edilmiştir.	Çalışanlarda sadece kuruluş için değil kendi kişisel verileri için de farkındalık oluştuğunu ifade etmişlerdir.	Bilgi güvenliği farkındalığının arttığını ifade etmişlerdir.	Bilgi güvenliği farkındalığının arttığını ifade etmişlerdir.
15. BGYS denetim aşamasında belgelendirme kuruluşunun yaptığı ara denetimlerde ne tür sorunla karşılaştınız?	Denetçilerin kendi bakış açılarını ve daha önce uygulamış oldukları sistemlerin aynısını beklemeleri ve ön yargılı yaklaşımları karşılaşılan sorunlardandır.	Önceki yıl çıkan minör uygunsuzluklar için alınan aksiyonların yeterliliklerinin sorgulanması karşılaşılan sorunlardandır.	Herhangi bir zorlukla karşılaşılmamıştır.	Hiçbir sorun ile karşılaşma olmamıştır.

16. Bilgi Güvenliği Yönetim Sistemi kurulduktan sonra kuruluşunuzda karşılaşılan zorluklar nelerdir?	İşlerin daha kontrollü yapılması, tüm adımları yerine getirilmesi ve bu adımlara ilişkin kayıtları oluşturulması yaşanan zorlukların başında gelmektedir.	IT çalışanlarında artan iş yükü karşılaşılan zorluklardandır.	Herhangi bir zorlukla karşılaşılmamıştır.	Belgelerin devamlılığı ve takip, bunlar iş yükü ve zaman kaybı getirmektedir.
17. Tavsiyeleriniz nelerdir?	Her aşamada üst yönetimin ve çalışanların desteğini almalırı tavsiyesinde bulunulmuştur.	BGYS ekibinin mutlaka BGYS kapsamını ilgilendiren birimlerden oluşması sağlanmalıdır.	Firmalar bünyelerine IT departmanı kurarak, bu alanda en az 10 yıl çalışmış olan kişileri tercih etmelidir şeklinde tavsiyede bulunmuşlardır.	Üst yönetimin desteği ile beraber BGYS konusunda bilgili çalışan tarafından ekibin oluşturulması tavsiyesinde bulunulmuştur.
DÜZELTİCİ FAALİYETLER ve İYİLEŞTİRME				

1. Hangi uygunsuzluklar karşısında düzeltici faaliyetler düzenlediniz? Tekrar edilmemesi için hangi önlemleri aldınız?	Tespit edilen tüm uygunsuzluklar için düzeltici faaliyet düzenlenmektedir.	İç denetimler, dış denetimler ve risk değerlendirme sonucunda çıkan uygunsuzluklara düzeltici faaliyetler düzenlenip yeniden risk değerlendirme yapılarak kontrol edilmiştir.	Olumsuzluk yaşanmamıştır, yaşamamak için çok uç noktalarda önlemler alınmıştır.	Uygunsuzluklar belirlenip Düzeltici Faaliyet açılarak kalıcı ve geçici önlemler alınıp tekrar edilmemesi için gerekli görülen yerlerde eğitim ve iyileştirmelere yer verilmektedir.
2. Belirlenen amaçlara ulaşmak için geçerli iyileştirmeler tespit ettiniz mi?	Belirlenen politika ve hedeflere uyulmadığı durumlarda kök neden araştırılıp gerekli iyileştirilmeler yapılmaktadır.	Yıllık BGYS hedefleri, süreç ölçümleri üzerine iyileştirmelerin olduğu ifade edilmiştir.	Bu bir süreç olduğu için sistemler sürekli takip edilerek gerekli iyileştirmeler yapılmaktadır.	Politika ve hedeflerin gerçekleştirilemediği durumlarda sorunun bulunarak geçerli iyileştirmelerin yapıldığını ifade etmişlerdir.
3. Bu süreçte açıklık ve sızma testleri yapıyor musunuz? Ne sıklıkta?	Dış kaynak ile her yıl en az 1 kez olmak üzere sızma testi yapılmaktadır. Yeni sistemlerin kurulması, mevcut sistemlerdeki değişiklikler durumunda da iç kaynaklar ile sızma testi yapılmaktadır.	Belirli aralıklarla sızma testi yapılmaktadır.	Sosyal mühendisliğimizi aksatmadan, yeni bilgi ve haberlerle, sürekli testler yapılmaktadır.	Şimdiye kadar yapılmamış ama 2021 içinde yapılacağını belirtmişlerdir.

SONUÇ ve ÖNERİLER

Günümüzde sadece kâğıt üzerinde olmamakla beraber birçok farklı alanda bulunan bilgi, çalışanları, müşterileri, iş ortakları ve tedarikçileri ile birlikte varlığını sürdüren kurumlarda çok değerli olup bilginin korunması büyük önem taşımaktadır. Teknolojinin hızlı bir şekilde gelişmesiyle beraber bilginin önemi daha da artmış, kurumlar sahip oldukları bilginin korunması, yönetilebilmesi, tehdit ve riskleri en az seviyede tutabilmek için en uygun bilgi güvenliği çalışmalarına, çözüm arayışlarına yönelmişlerdir. Böylece bilgi güvenliğinin sağlanması, kurumlarda standartlaşmış yönetim sistemlerinin kurulması ihtiyacını ortaya çıkarmıştır. Bu noktada bilgi güvenliği yönetim sistemini uygulamak isteyen kurumlar için en önemli kaynak tüm dünyada kabul görmüş ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'dir. ISO/IEC 27001 standardı, kurumların bilgi güvenliği ihtiyacına yönelik oluşturulmuş uluslararası bir standarttır. Fiziksel ve çevresel koşullara, müşteri ve tedarikçi anlaşmalarına, insan kaynaklarına, iş sürekliliği ve bilgisayar uygulamalarına yönelik kuralları ve uygulamaları vardır. Her sektörde büyüklüğüne, ihtiyaç ve amacına bakılmaksızın uygulanabilen esnek bir yapıya sahiptir. Kuruluşlar prosedürleri, politikaları, yönergeleri ve risk yönetimleri olan bu sistemi hayata geçirerek sahip oldukları bilgilerin korunmasını sağlarlar. Bu sistemle beraber kuruluşlar marka ve imaj değerlerini de arttırmış olurlar.

Bilgi güvenliği yönetiminin başarılı ve etkin olması için; üst yönetimin desteği, tüm çalışanların eğitimlerle kurumsal düzenlemelerle bilinçlendirilmesi, öncelikli risklerin tespit edilerek bu risklerin tamamen ortadan kaldırılması ya da minimum seviyeye indirilecek çözümlerin belirlenmesi, belirlenen çözümlerin kurumda uygulanması ile birlikte belirli aralıklarla denetlenerek gerekli iyileştirmelerin yapılarak sürekli gelişime açık olması gereklidir.

Sertifikanın alınması, BGYS' nin kurulması, uygulanması önemli adımlardandır ama BGYS' nin sürdürülebilir ve devamlı iyileştirilebilir olması çok daha önemlidir. Kurumların etkin bir BGYS yürütebilmesi için bazı başarı faktörlerini dikkate almalıdır:

- BGYS bir kurumda hayata geçirilmeden önce kurumun, üst yönetimin kararıyla ISO/IEC 27001 standardını alıp bu standarda uygun bir

şekilde çalışmaya "karar vermesi" gerekmektedir. Üst yönetimin kararlılığı ve liderliği, gerekli kaynakların sağlanması ve uygulayıcıların BGYS etkinliğini yönlendirmek ve desteklemek için çok önemlidir.

- Kurumda bilgi güvenliği faaliyetlerini yürütmek ve performansının izlenmesi için üst yönetim tarafından BGYS komitesi oluşturulmalıdır. Komite üyeleri bu iş için yeterli ve eğitimli olmalıdır. Ardından yönetim sisteminin temel ilkelerini, hedeflerini ve çalışanların sorumluluklarını içeren bilgi güvenliği politikası hazırlanarak üst yönetimin onayı ile çalışanlara ve üçüncü taraflara duyurulmalıdır. Bilgi güvenliği politikası ve amaçları, hedeflenen bilgi güvenliği ile uygun olmalıdır. Standardın hangi departmanı kapsayacağını, sınırlarını, süreçleri ve hangi işleri kapsayacağı kapsam dahilinde belirlenmelidir.
- Değişimlere ve gelişimlere ayak uyduran bir bilgi güvenliği yönetimi, sadece teknoloji ya da bilgisayar güvenliğinden ibaret değildir. Bilgi güvenliği; bireylerin, süreçlerin ve teknolojinin özel hayatta ve iş hayatında benimsenmesi, öğrenilmesi ve rutin bir şekilde uygulanması vurgulanmalıdır.
- Kurumda etkin bir bilgi güvenliği farkındalığı oluşturmak için eğitim, farkındalık ve alıştırma çalışmaları çalışanlarla beraber ilgili tarafların bilgisine sunulmalıdır. Bu farkındalık eğitimleri politikalar, prosedürler, rol ve sorumlulukları yeterince idrak etmek açısından sınıf içi yüz yüze uygulamalar şeklinde olsa daha iyi olur. Aksi taktirde bu eğitimlerin yeteri kadar etkisi olmayabilir.
- ISO/IEC 27001 standardında bilgilerin dokümante edilmesi çok önemlidir böylece bilgiler iyi bir şekilde dokümante edilmeli ve belirli zaman aralıklarında dokümanlar gözden geçirilmeli ve güncellenmelidir.
- Varlıkların sınıflandırması ve risk analizi en önemli çalışmalardan biridir. Kurumun sahip olduğu her şey hatta çalışan bile kurum varlığı kabul edildiğinden dolayı varlıkların sınıflandırılması ve varlık değerlendirmesi dikkatlice yapılmalıdır. Bütün varlıkların dökümünün çıkarılıp sınıflandırılmasının ardından risk analizi yapılmalıdır. Risk analizi sonucunda kurumun karşılaşabileceği tehditler ve olma

olasılıkları belirlenmelidir ve bunun sonucunda kurumda oluşturacağı etki hesaplanmalıdır.

- İç tetkikler ve YGG toplantıları belirlenen aralıklarla düzenli bir şekilde yapılmalıdır. BGYS' nin uygunluk, yeterlilik ve etkinliğinin devam ettiğinin üst yönetim tarafından belli aralıklarla denetlenmesi gerekmektedir.

Ülkemizde bilgi güvenliği yeni bir alan olduğundan bilgi güvenliği yönetim sistemlerini kurma ve uygulama esnasında kuruluşlar çeşitli zorluklarla karşılaşmıştır. Mülakat yapılan kuruluşların BGYS öncesi hazırlık aşamasında karşılaştıkları sorunların; standart konusuna hakim, bilgisi ve tecrübesi yeterli düzeyde olmayan bir danışmanla çalışmanın zorluğu, denetçinin kişisel yorumları sebebiyle kuruma özgü bilgi güvenliği yönetim sistemi uygulamalarını kavrayamama, standardın alındığı zaman doküman ve bilgi eksikliğinden kaynaklanan zorlukların yaşandığı gözlemlenmiştir. BGYS başvuru aşamasında, kuruluşlar, çalışanın bilgi güvenliği konusunda yeterli bilgiye sahip olmaması, yeni sistemin getirdiği yeni kurallar, daha kontrollü ve sistematik iş akışı sebebiyle çalışanların önyargısı ve Türkçe doküman yetersizliğinden dolayı bazı kavramların tam anlaşılamaması ile ilgili zorluklarla karşılaşıldığı gözlemlenmiştir. BGYS sonrası aşamasında; işlerin daha kontrollü, prosedürdeki tüm adımların ve bunlara ilişkin bütün kayıtların tutularak oluşturulması ve iş yükünün artması belirtilen zorluklardan olmuştur.

Bilgi güvenliği yönetim sistemi sertifikasına sahip dört kuruluş ile yapmış olduğumuz mülakat sonucunda; kuruluşların standart başvurusu yapmadan önce kendi sektörleri ile ilgili araştırma yapması ve bilgi alışverişinde bulunarak ortaya çıkan tecrübelerin paylaşımı, üst yönetimin desteğini her aşamada alarak kuruma özgü bir BGYS oluşturmaları, çalışanları sürece dahil ederek sistemin sahiplenmesini, kendi kurumlarına özgü uygulama yöntemlerini geliştirmelerini ve bilgi güvenliği konusunda bilinçli bir IT departmanı kurulmasını, BGYS komitesinin bilgili, mutlaka BGYS kapsamını ilgilendiren birimlerden oluşması önerilerinde bulunulması karşılaşılan zorlukların çözümü konusunda kolaylık sağlayacaktır.

Gelecek çalışmalarda çalışmanın kapsamı genişletilerek daha çok firma üzerinde yapılabilir ve bu çalışmada tespit edilemeyen farklı sorunlar ve çözüm yolları ortaya çıkarılabilecektir.

KAYNAKÇA

(2020, 05 25). https://en.wikipedia.org/wiki/Information_Age adresinden alındı

Adak, Ş. F., Çakır, H., & Tuğ, E. (2014). Bilişim Güvenliği Tedbirleri ve TKDK Kurumunda Uygulama Örneği. *Bilişim Teknolojileri Dergisi, 7*(1), 14.

Akay, İ. G. (2014). *Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama MülakatlarıI.* Bilecik Şeyh Edebali Üniversitesi, Sosyal Bilimler Enstitüsü işletme Anabilim Dalı, Bilecik.

Akgün, A. E., & Keskin, H. (2003). Sosyal Bir Etkileşim Aracı Olarak Bilgi Yönetimi ve Bilgi Yönetimi Süreci. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1*, 175–188.

Aktan, C. C., & Vural, İ. Y. (2005). *Bilgi Çağı, Bilgi Yönetimi ve Bilgi Sistemleri.* Konya: Çizgi Kitabevi.

Almeman, F., & Saymaz, Ö. (2018). *TS EN ISO/IEC 27001:2017 Denetçisi Ne (Görmek) İster? Uygulama Klavuzu, Vericert Yönetim Sistemi Serisi:4.* İstanbul: Bahri Mutlu Matbaası.

Alpay, B. N. (2008). *ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması.* Yüksek Lisans Tezi, İstanbul.

Altun, R. (2014). *Belirli Kısıtlara Göre Bilgi Güvenliği İhlallerinin Tespiti.* Yayınlanmamış Yüksek Lisans Tezi, Beykent Üniversitesi FBE, İstanbul.

Atılgan, D. (2009). Bilgi Yönetimi Kavramı ve Gelişimi. *Türk Kütüphaneciliği, 23*(1), 201-212.

Awad, E., & Ghaziri, H. (2004). *Knowledge Management.* New Jersey: Prentice Hall Publishing.

Aydoğan, H. (2011). *Mobil Haberleşme Sektörü İçin Örnek Bilgi Güvenliği Yönetim Sistemi (BGYS) Modeli.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Barquin, R. C. (2001). What is Knowledge Management? *Knowledge and Innovation: Journal of The KMCI, 1*(2), 129.

Barutçugil, İ. (2002). *Bilgi Yönetimi.* İstanbul: Kariyer Yayıncılık.

Başaranoğlu, E. (2016, 01 25). Bilgi Güvenliği Unsurları (CIA Ve Diğerleri). https://www.siberportal.org/blue-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/ adresinden alındı

Beydağlı, E., Kara, M., Bahşi, H., & Alparslan, E. (2009). Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler Standardı. *IV.Ulusal Yazılım Mühendisliği Sempozyumu*, (s. 11-17). İstanbul.

BGYS Danışmanlık DAS Smart. (2018). Risk Yönetimi Dokümanları.

Bilgin, B. Ö. (2016). *Bilgi Teknolojileri Denetimi ve Bir Uygulama.* İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Bingöl, U. (2010). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu.* Sakarya: Sakarya Üniversitesi Sosyal Bilimler Enstitüsü.

Boşal, S. (2017). *Kamuda Bilgi Güvenliği ve İller Bankası A.Ş. Örneği.* Ankara: İller BankasıI Anonim Şirketi.

Buckman, R. (2004). *Building a Knowledge – Driven Organization.* U.S.A: McGraw-Hill Companies.

Bureau Veritas Gözetim Hizmetleri. (2017). *ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi İç Denetçi Eğitimi Sunumu.*

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

Canbek, G., & Sağıroğlu, Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 33*(2), 1-12.

CEN/Cenelec ISO/IEC 27001:2017 Revizyonu. (2020, 07 4). https://blog.btyon.com.tr/2017/11/cencenelec-isoiec-270012017-revizyonu.html adresinden alındı

cybermag. (2018, 10 19). Şirketlerin Büyüklüğü Arttikça Şifre Güvenliği Azaliyor! 07 14, 2021 tarihinde https://www.cybermagonline.com/sirketlerin-buyukluguarttikca-sifre-guvenligi-azaliyor adresinden alındı

Çakır, H., & Tuygun, M. (2019). ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 3*(2), 59-78.

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

Çetinkaya, M. (2008). Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması. *Akademik Bilişim 2008* (s. 511-516). Çanakkale: Çanakkale Onsekiz Mart Üniversitesi.

Çiğdem, Y. (2009). *Telekominikasyon Sektöründe Firma İçindeki Bilgi Güvenliğini Etkileyen Faktörler ve Bu Faktörlerin Çalışanlar Üzerine Etkileri.* Gebze: Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü.

Çontar, F. (2013). *Ağ ve Yazılım Güvenliği.* İstanbul: Kodlab.

Çubukçu, F. (2018). *Bilgi Güvenliği Yönetim Sistemi ISO 27001:2013 Uygulama Klavuzu.* İstanbul: Pusula.

Demirok, E. (2016). *Kurumsal Bilgi Güvenliği Yönetim Sistemi Uygulaması; Vakıf Üniversitesi Örneği.* İstanbul: Okan Üniversitesi Bilişim Sistemleri.

Djapić, M., & Lukić, L. (2007). ISO/IEC 27000 Series Standards The Best Business Practice For Information Security. *1. International Quality Conference* (s. 124-128). Kragujevac: AOS.

Doğantimur, F. (2009). *ISO 27001 Standartı Çerçevesinde Kurumsal Bilgi Güvenliği.* Ankara: T.C. Maliye Bakanlığı Strateji Geliştirme Başkanlığı.

Ekşi, B. (2021, 02 14). *ISO 27001 Varlık Yönetimi – Varlıkların sorumluluğu.* https://www.burakeksi.com/iso-27001-varlik-yonetimi-varliklarin-sorumlulugu/ adresinden alındı

Eminağaoğlu, M., & Yılmaz, G. (2009). Bilgi Güvenliği Nedir, Ne Değildir? Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4), 1-15.

Emir Erdoğan, S. (Ocak, 2020). *Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC/ ISO 27001 Standartının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi.* İstanbul Kültür Üniversitesi, İşletme. İstanbul: Lisansüstü Eğitim Enstitüsü.

Ergen, C. (2010, 05 10). *Çözüm Park.* Çözüm Park: https://www.cozumpark.com/information-technology-infrastructure-library-itil-nedir/ adresinden alındı

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standartı Tanımlar ve Örnek Uygulamalar.* Ankara: Odtü Yayıncılık.

FFIEC. (2010). Information Security. Virginia, USA.

Ganbat, O. (2013). *Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması.* Yüksek Lisans Tezi, Ege Üniversitesi , Fen Bilimleri Enstitüsü, İzmir.

Gazdağı, O., & Çetinyokuş, T. (2020). Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301

Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme. *Journal of Humanities and Tourism Research, 10*(2), 475-491.

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

Gülmüş, M. (2010). *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği.* İstanbul: Yıldız Teknik Üniversitesi FBE.

Gündoğan, B. (2016). Bilgi Sistemleri Denetiminde ISO/IEC 27001 ve ISO/IEC 27002 Standartlarının Yeri. *Muhasebe ve Denetim Dünyası*, 15-28.

Güngör, M. (2015). *Ulusal Bilgi Güvenliği : Strateji ve Kurumsal Yapılanma.* Ankara: Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı.

Gürsel, T. (2019). *Sigorta Şirketlerinde Bilgi Güvenliği Yönetim Sistemi Ddenetimi.* İstanbul: Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Sigortacılık Anabilim Dalı.

Hacısüleymanoğlu, E. (2010). *Bilgi Teknolojileri Yönetişim Yöntemleri ve COBIT İle Ulusal Bir Bankada Uygulaması.* İstanbul: Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü.

Hariharan, M. R., & Khaneja, M. (2003). E-Knowledge Management Framework for Government Organizations. *Information Systems Management*, 38-48.

Harold, I. (2007). *Empire and Communications.* Toronto: Dundurn Press.

Henkoğlu, T. (2017). Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme. *Arşiv Dünyası Dergisi*, 46-56.

http://www.cagataycebi.com/security/bilgi_guvenligi.pdf. (tarih yok).

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report, 13*(4), 247- 255.

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

Ilgaz, B. (2018). *Küçük ve Orta Büyüklükteki İşletmeler İçin Veri Güvenliği ve Standartları.* Konya: KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü.

Irmak, H., & Baz, F. Ç. (23-25 Ağustos 2019). Kurumsal Bilgi Güvenliği, Tehditler ve Alınması Gereken Önlemler Üzerine Bir İnceleme. *2. Uluslararası Mardin Artuklu Bilimsel Araştırmalar,* (s. 333-341). Mardin.

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* USA: ISACA.

IsecT. (2020, June 28). “ISO/IEC 27001:2013 Information security management systems requirements”. New Zealand. https://www.iso27001security.com/html/27001.html adresinden alındı

ISO. (2018). *ISO/IEC 31000 Kurumsal Risk Yönetimi Standardı.* TSE.

ISO/IEC 31000. (2011). *Risk Management- Principles and Guidelines.* Switzerland: ISO.

isokalitebelgesi. (tarih yok). ISO 27001 Belgesi Kimler Hangi Sektörler Şirketler Firmalar alabilir Zorunlumudur. 07 14, 2020 tarihinde https://www.isokalitebelgesi.com/iso-27001-belgesi-kimler-hangi-sektroler-sirketler-firmalar-alabilir-zorunlumudur adresinden alındı

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2006). Information Security Standards and Global Business. *2006 IEEE International Conference on Industrial Technology* (s. 2091-2095). IEEE Institute of Electrical and Electronic Engineers.

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

Kılıç, M. Ç., & Gökçöl, O. (2010). Türkiye’deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi. 1-5.

Koç, F. (2008). *BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Klavuzu.* Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Koç, S., Şeker, S., & Şeker, F. (2019). Bilişim Teknolojileri (BT) Denetiminde Bilgi Güvenliği İle İlgili Uluslararası Standartlar ve Türkiye' de ki Uyum Çabalarının İncelenmesi. *Uluslararası Muhasebe ve Finans Araştırmaları Dergisi, 1*(2), 121-139.

Kum Eğitim Danışmanlık. (2019, 09 03). ISO 27001 BGYS'de İnsan Kaynaklarının Rolü. İstanbul, Türkiye.

Kumaş, E. (2009). *Bilgi Güvenliğinin Sağlanmasında Risk Yönetimi: E-Devlet Kapısı Uygulaması.* Kırıkkale: Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü.

Malhotra, Y. (1998). Deciphering the Knowledge Management Hype. *Journal of Quality & Participation, 21*(4), 58-60.

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

Mitnick, K. D., & Simon, W. L. (2016). *Aldatma Sanatı* (6. Basım b.). Ankara: ODTÜ Yayınları.

Muharremoğlu, G. (2013). *Kurumsal Bilgi Güvenliğinde Zaafiyet, Saldırı ve Savunma Ögelerinin İncelenmesi.* Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi FBE.

Ok, K. (Ekim 2013). *Bilgi ve Bilgi Yönetimine Giriş.* İstanbul, İstanbul: Papatya Yayıncılık Eğitim.

Öğüt, A. (2001). *Bigi Çağında Yönetim.* Ankara: Nobel Yayın Dağıtım.

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

Önel, D., & Dinçkan, A. (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Önel, Dinçer; Dinçkan, Ali. (2007). *Bilgi Güvenliği Yönetim Sistemi Kurulumu.* Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Örnek, C. K. (2003). Bilişim Güvenliği Denetimlerinde Yapılan Hatalar. *Türkiye İç Denetim Enstitüsü E-DERGİ, 8*, 43-44.

Ötegen, M. (2018). *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini Kurumsal Geçiş Süreci ve Uygulaması.* Ankara: İller Bankası Anonim Şirketi.

Öztemiz, S., & Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası Dergisi, 14*(1), 87-100.

Peker, D. (2008). *Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005.* TBD Kamu-BİB Kamu Bilişim Platformu X Çalışma Grubu Raporu .

Perendi, Ü. (2008). *BGYS Kapsamı Belirleme Kılavuzu.* Kocaeli: Tübitak-UEAKE.

Perendi, Ünal. (2008). *BGYS Kapsamı Belirleme Kılavuzu.* Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Plunkett, P. (2001). Managing Knowledge@Work: An Overview of Knowledge Management. *Knowledge Management Working Group of the Federal Chief Information Officers Council*, 7.

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

Richardson, R. (2008). *2008 CSI/FBI Computer Crime & Security Survey.* CSI.

Seferoglu, S. S., Karaoğlan Yılmaz, F. G., Yildiz- Durak, H., & Yılmaz, R. (October 2018). *Bilgi Güvenliği Farkındalığı ve Bilgi Güvenliği Politikalarıyla İlgili Bir İnceleme.* Sakarya: TOJET ve Sakarya Üniversitesi.

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. *Akademik Bilişim 2013* (s. 677-681). Antalya: XV. Akademik Bilişim Konferansı Bildiriler Kitabı.

Şentürk, B. (2008). *Türkiye Büyük Millet Meclisi'nde Bilgi Yönetimi Anlayışı ve Belge Yönetimi. Yüksek Lisans Tezi.* Yüksek Lisans Tezi, Ankara Üniversitesi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı, Ankara.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132-137.

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook.* New York: Auerbach Publicaions.

TSE. (Mart 2006). *TS ISO/IEC 27001,Bilgi Teknolojisi,Güvenlik Teknikleri, Bilgi güvenliği Yönetim Sistemleri, Gereksinimler.* Ankara: TSE.

TSE, T. S. (2013). *TS ISO/IEC 27001:2013 Bilgi teknolojisi – Güvenlik teknikleri– Bilgi güvenliği yönetim sistemleri – Gereksinimler* (2. Baskı b.). İsviçre: ISO Telif Ofisi.

Ünal, H. (2019). *Dijitalleştirme ve Kurumsal Elektronik Arşiv Yönetimi Sistemlerinin Yapılandırılması.* Yüksek Lisans Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Bilgi ve Belge Yönetimi Ana Bilim Dalı, Ankara.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik - Mimarlık Fakültesi Dergisi, 23*(2), 507-522.

Vural, Yılmaz; Sağıroğlu, Şeref. (2007). Kurumsal Bilgi Güvenliği: Güncel Gelişmeler. *X. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 191-199). Ankara: Bilgi Güvenliği Derneği.

Wenger, A., Mauer, V., & Cavelty, M. D. (2008). *International CIIP Handbook.* Switzerland: ETH Zurich.

Whitman, M., & Mattord, H. (2014). *Principles of Information Security* (Fourth Edition Course Techonology b.). Mason, OH, United States: Cengage Learning, Inc.

Yıldırım, S. (2017). *Bilgi Sistemleri Denetim Süreçleri Yeterlik Etüdü.* İstanbul: Sermaye Piyasası Kurulu Denetleme Dairesi.

Yıldız, B. (2007). *Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması.* Kocaeli: Gebze Yüksek Teknoloji Enstitüsü SBE.

Yıldız, M. (2014). *Siber Suçlar ve Kurum Güvenliği.* Ankara: Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Dairesi Başkanlığı.

Yılmaz, H. (2010). Bilgi Yönetimi Sürecinde Performans Yönetim Modellerinin Uygulanması. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 0*(2), 59-76.

Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standartı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Denetişim*(15), 45 - 59.

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

Yusufovna, F. S., & Kim, T.-H. (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering, 2*(2), 17-32.

Zaim, H. (2005). *Bilginin Artan Önemi ve Bilgi Yönetimi.* İstanbul: İşaret Yayınları.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

ÖZGEÇMİŞ

Tuğba ÇELİK Kalaba Lisesi'nden mezun olduktan sonra Selçuk Üniversitesi Karaman Meslek Yüksekokulu Bilgisayar Teknolojisi ve Programlama Bölümü'nde öğrenime başlayıp 2004 yılında mezun oldu. Ardından Anadolu Üniversitesi İşletme Bölümüne geçiş yaparak Lisans derecesi ile mezun oldu.

EKLER

KURULUŞ A İLE YAPILAN GÖRÜŞME

BGYS ÖNCESİ HAZIRLIK SÜRECİ

1. **Kurumunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini kurmaya neden ihtiyaç duydunuz?**

   Kritik bilginin korunması ve standardın yönlendirmeleri ile mevcut IT süreçlerimizi iyileştirmek adına sistemin kurulmasına karar verilmiştir.

2. **Hazırlık için danışman firmadan yararlandınız mı? Eğer evetse bu süreç sizin için yararlı oldu mu? Hayırsa bu süreçte zorluk çektiniz mi? Bu yöntemi önerir misiniz?**

   Yönetim sisteminin kurulum aşamasında danışmanlık hizmeti aldık. Özellikle yönetim sisteminin gerekliliklerini şirket süreçlerimize dâhil ederken danışmanın yönlendirmesi bizim için faydalı oldu. Ayrıca standart ile ilgili çalışmalara başladığımızda Türkiye'de bizim ölçek ve büyüklüğümüzde hiçbir üretim tesisi bu konuda çalışmalara henüz başlamamıştı. Bu sebeple sektör, en iyi uygulamalar, tecrübe paylaşımı konusunda danışmanlığın faydasını gördük. Süre, standarda ilişkin çalışan yetkinliği gibi konularda kısıt mevcut ise mutlaka danışmanlık ile sürecin yönetilmesini öneriyorum.

3. **Başvuru için oluşturduğunuz BGYS komitesi yeterli bilgiye sahip miydi? Bu konuda eğitim danışmanlık hizmeti aldınız mı?**

   Sistem kurulumuna başlandığında, BGYS Komitesi'nin (bizdeki uygulamaya göre Bilgi Güvenliği Yönetim Sistemi Ekibi) konu hakkında bilgisi yoktu. Danışmanlık kapsamında ekip üyelerine eğitimler (ISO 27001 BGYS Standardı Temel Eğitimi, İç Denetçi Eğitimi) de verildi.

4. **Bu aşamada karşılaşılan zorluklar nelerdir?**

   Kurulum sırasında standart Türkiye için çok yeni olduğundan konusuna hâkim, IT süreçlerinde çalışmış danışman bulmak oldukça zordu. Bizim çalıştığımız danışmanda ISO 9001 Kalite Yönetim Sistemi kökenliydi ve IT operasyonlarında tecrübesi yeterli düzeyde değildi. Bu sebeple süreçlerimizi kendisine anlatırken ve süreçleri standardın istediği çerçeve getirmek için önerdiği aksiyonlar üzerinde çalışırken zaman zaman sorunlar yaşadık. Daha net anlaşılması için bir örnek verecek olursam; sunucuların bakımlarını

konuşurken danışmanımız bir bakım planı olmasını ve plana göre sunucuların belli periyotlarla kapatılarak içindeki toz vb. maddelerin temizliğinin yapılmasını önerdi. Bu önerinin kökeninde daha öncede belirttiğim gibi ISO 9001 Kalite Yönetim Sistemi temelli olmasından kaynaklı sunucu bakımını her hangi mekanik bir cihaz bakımı ile paralel düşünmesiydi muhtemelen. Kendisine sunucularımızın 7/24 çalıştığını, zorunlu olmadıkça kapatılmadığını, sunucu fanlarının belli aralıklarda çok güçlü çalışarak zaten içindeki tozların dışarı attığını anlatmak / kabul ettirmek durumunda kalmıştık.

5. **Hazırlık süreci için bir öneriniz var mı?**

   Firmalar, süreci danışmanlık ile yürütecekler ise mutlaka daha önce IT operasyonlarında görev almış danışmanlardan hizmet almaları ortak dili konuşmak ve hızlı ilerlemek adına faydalı olacaktır.

   Diğer bir tavsiyemde; ISO 27001 BGYS sistemini kurumun benimsemesi için üst yönetimin bu konudaki yaklaşımı, bakış açısı oldukça önem arz etmektedir. Üst yönetim konu ile ilgili ne kadar hassas ise çalışanlarında desteği o kadar güçlü olmaktadır. Bu sebeple üst yönetimin desteği her süreçte olduğu gibi bu tip yeni ve kapsamlı süreçlerde de çok önemlidir.

BGYS BAŞVURU AŞAMASI

1. **Kurumunuzda oluşturduğunuz ISO/IEC 27001 BGYS' nin kapsamı nedir? Hariç tutmaları gerekçelendirdiniz mi?**

   Standart maddeleri anlamında bir hariç tutmamız yoktur.

   Belge anlamında kapsamımız ise Yetkilendirilmiş Yükümlü Statüsü (YYS) işlemlerinde görev alan departmanlar olarak belirlenmiş, diğer departmanlar hariç tutulmuştur.

2. **Üst yönetim bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunup destekledi mi? Varsa yaşadığınız zorluklar nelerdir?**

   Üst yönetim süreci oldukça destekleyici yaklaştı. Gerek kurulum aşamasında, gerekse sonrasında sürece katkı sundu.

3. **Bilgi Varlıklarınızı belirlerken nelere dikkat ettiniz?**

   İlk olarak kurum için kritik öneme haiz bilgileri (çalışan, satın alma, üretim, kalite verileri vb.) belirledik.

   Bu bilgileri belirledikten sonra;

- Bu bilgilerin tutulduğu ortamları (kağıt, sunucu, veri tabanı)
- Bu bilgilerin saklandığı ortamları (arşiv, sistem odası vb.)
- Bu bilgilerinin transferinde görev alan sistem / cihazları (kablo, ftp sunucusu vb.)
- Bu bilgilerin kaynağı olan kişileri (çalışan, 3. taraf, hizmet sağlayıcı vb.)
- Bu bilgilerin korunmasında görevli cihazları (firewall vb.)
- Bu bilgilerin işlendiği cihazları (PC, yazıcı vb.)
- Bu bilgileri işleyen sistemleri (yazılımlar vb.)

göz önünde bulundurarak varlıklarımızı belirledik.

4. **Bilgi Güvenliği Politikası ve prosedürler neleri kapsıyor, nasıl bir sistemle bunları hazırladınız?**

   Bilgi güvenliği politika ve prosedürlerimiz standardın gerekli gördüğü doküman yapısını ve işleyişimizde bize yön gösterecek, yönlendirecek yazılı kaynakları kapsamaktadır.

   Bu dokümantasyonu şirketimizin yönetim sistemleri dokümantasyonunu takip ettiği bir yazılım üzerinde hazırladık.

5. **Kurumunuzdaki riskleri belirlemek için hangi yöntemleri kullanıyorsunuz?**

   Kurumumuzda riskler hem bilgi varlığı hem de süreç bazlı olarak değerlendirilmektedir.

   Risk yönetim metodolojimiz; risk puanını hesaplarken varlık değeri, riskin etkisi (finansal, operasyonel, paydaş açısından, yasal olmak üzere 4 kriter göz önünde bulundurulmaktadır.) ve olma sıklığı değerleri göz önünde bulundurmaktadır.

6. **Kabul edilebilir veya risk iyileştirmesi gerektirecek seviyede öngörülmüş risk seviyesini nasıl belirlediniz?**

   Kurum kültürü ve kurumun bilgi güvenliği açısından mevcut durumu göz önünde bulundurularak kabul edilebilir risk seviyesi belirlenmiştir.

   Kabul edilebilir risk seviyesi her yıl mevcut durum ışığında Yönetimin Gözden Geçirmesi Toplantısı'nda yeniden değerlendirilmektedir.

7. **Riskleri azaltmak ya da ortadan kaldırmak için ISO/IEC 27001 Ek – A maddelerinden hangisini seçtiniz?**

   ISO/IEC 27001 Ek – A maddelerinden birçoğunu risk iyileştirme faaliyetlerimizde referans olarak kullandık.

   Ayrıca; hangi risk iyileştirme aksiyonu için hangi EK-A maddesini kullandığımızı da takip açısından risk analizlerine ilişkin dokümanlar üzerinde belirtiyoruz.

8. **İlk başvurunuzda belgeyi alabildiniz mi? Eğer alamadıysanız neden alamadınız?**

   Belgeyi ilk başvurumuzda almaya hak kazandık.

9. **Bu aşamada yaşadığınız temel zorluklar nelerdir?**

   İnsan doğası gereği yeniliklere önyargılıdır. Özellikle bu yenilikleri; iş yapış tarzınızı eskiye göre daha kontrollü, daha sistematik ve kurallar üzerine yapmayı gerektiriyor ise… Bizde bu aşamada çalışanlarımızda bu ön yargının yansımalarını sıklıkla gördük.

10. **Bu aşamada önerileriniz nelerdir?**

    Çalışanları olabildiğince sürecin içine dahil etmek, yapılan çalışmaların neden yapıldığını, bize getireceği faydaları kendileri ile paylaşmak oldukça önemli. Bu paylaşımın bir kez ya da tek bir kanal üzerinden değil, birden fazla kere ve farklı yollar ile yapılması sürecin sahiplenilmesi ve kurulan sistemin sürdürülebilirliği adına oldukça önemli.

    Belirlemiş olduğumuz parola kurallarına ilişkin bir örnek verecek olursak;

    - Parola politikasının öneminin yapılan üst düzey bir toplantıda Genel Müdür tarafından paylaşılması
    - Parolanın güçsüz olması durumunda yaşanabilecek sorunların bir eğitimde çalışanlara aktarılması
    - Parola güvenliği ile ilgili bir karikatürün kurum portalında yayınlanması

    gibi bir çok kanaldan gelen bildirimler çalışanların yeni parola politikasına hızlı bir şekilde adapte olmasını daha da önemlisi bunun tercihe bağlı değil bir zorunluluk olduğunu anlayarak günlük hayatlarının bir parçası haline getirmelerini sağlayacaktır.

BGYS SONRASI

1. **Bilgi Güvenliği Yönetim Sistemi kuruluşunuzda kaç yıldır uygulanmaktadır?**

   ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nin kurumumuzda kuruluş kararı Şubat. 2013'dir. İlk belge Kasım 2013 yılında alınmış olup bu tarihten itibaren yönetim sistemine ilişkin faaliyetlerimiz kesintisiz devam etmektedir.

2. **Bu sistemin kurumunuzun bilgi güvenliği açısından temel yararları nelerdir?**

   Bilgi güvenliği faaliyetlerine sadece ilgili çalışanın kişisel bakış açısı, vizyonu ve tecrübesi ile bakmak yerine standart bir perspektif ile bakabilmekte olanak sağlamıştır. Standart kurum için bir rehber niteliğinde olmuştur.

   Ayrıca normalde kullanıcılar tarafından ön yargı ile karşılanan bazı bilgi güvenliği faaliyetleri standardın gerekliliği olarak ifade edildiğinde daha çabuk kabul görmektedir.

3. **İşletmenin kurumsal prestijine ne tür katkılar sağladı?**

   Daha öncede belirttiğim gibi belgenin ilk alındığında Türkiye'de henüz bizim ölçek ve büyüklüğümüzde hiçbir üretim tesisi belgeyi almamıştı. Bu sebeple oldukça büyük bir prestij kaynağı olmuştur.

4. **Kurumunuzda BGYS' nin uygunluğunun ve etkinliğinin tespitini nasıl yapıyorsunuz?**

   Kurulan sistemin etkinliği ve etkililiğini tespit etmek için kullandığımız temel enstrümanları; iç ve dış denetimler, periyodik olarak yapılan penetrasyon testleri, risk işleme faaliyetleri olarak sıralanabilir.

5. **Kurumunuzda iç denetimi kendiniz mi yoksa danışman firma mı yapıyor? İç denetimi nasıl yapıyorsunuz?**

   Kurumumuzda iç denetim faaliyetleri eğitim almış çalışanlarımız tarafından yani iç kaynaklar ile yapılmaktadır.

   İç denetimler, kurumun sahip olduğu diğer yönetim sistemleri ile entegre olarak planlamakta ve yılda en az 1 kez planlı olarak iç denetim faaliyeti gerçekleşmektedir.

   Denetim faaliyetleri saha ve doküman bazlı olarak yapılmaktadır.

6. **Sistemin uygulanması kurum üzerindeki iş yükünü olumlu ya da olumsuz yönde etkiledi mi? Bunlar nelerdir?**

   Özellikle ilk kurulum, versiyon geçişi, kapsama yeni dahil olma durumlarında kuruma ekstra bir iş yükü getirmektedir. Ancak sonrasında uygulamaların çalışanlara getirdiği iş yükü, standardın sağladığı faydalar ile karşılandığında oldukça az ve kabul edilebilir duruma gelmiştir.

7. **Uygulama sürecinde danışmanlık firmasından destek alıyor musunuz? Evetse bu oran ne kadardır?**

   Uygulama sürecinde zaman zaman belli konular özelinde danışmanlık hizmeti alınmıştır. Bu ilk belgenin alınmasından bu yana geçen yaklaşık 7 senede 2 kezdir.

   Şu aşamada her hangi bir danışmanlık hizmeti alınmamaktadır.

8. **Kuruluşunuzda diğer yönetim sistemlerini kullanıyor musunuz? Eğer kullanıyorsanız bilgi güvenliği yönetim sistemi bunlarla uyumlaştırıldı mı? Uyumlaştırılırken nasıl sorunlarla karşılaştınız?**

   Kuruluşumuzda ISO 27001 BGYS dışında 8 farklı yönetim sistemi mevcuttur. ISO 27001 faaliyetleri; bu yönetim sistemleri ile entegre olarak yürütülmektedir.

   Kurumda Annex SL Yüksek Seviye Yapı'ya geçen ilk standart ISO 27001 olmuştur. Bu sebeple; risk yönetimi, bağlam, iç ve dış hususlar gibi konularda kurum içi öncü çalışma hep ISO 27001 standardı kapsamında gerçekleşmiştir. Bu açıdan BGYS'nin uyumlaştırma da öncü bir rol üstlendiğini söylemek yanlış olmaz. Öncü olmanın getirdiği handikapları yaşayan ISO 27001 sonrasında kurum içinde Yüksek Seviye Yapı'ya diğer standartlar için gerekli alt yapıyı sağlamış, yaşanabilecek sorunları yaşamış hatta sorunlara ilişkin çözümleri de bulmuş durumdaydı. Bu sebeple ISO 27001 açısından diğer yönetim sistemleri uyumlaşma konusunda sorunla karşılaşılmamıştır.

9. **Kurumunuzda eğitim ve bilinçlendirme çalışmalarını hangi aralıklarla, nasıl yapıyorsunuz?**

   Kurumumuzda eğitim ve bilinçlendirme çalışmaları periyodik olarak yapılmaktadır.

Çalışmanın periyodu faaliyette göre değişmekte olup Kurumumuz ’da yürütülen temel eğitim ve bilinçlendirme faaliyetleri aşağıdaki şekilde listeleyebiliriz:

- Oryantasyon Eğitimi
- Farkındalık Eğitimi
- Bilgi Güvenliği Bülteni
- Bilgi Güvenliği ’ne İlişkin Duyurular
- Bilgi Güvenliği Broşürleri

10. Kurumunuzda kontrol sürecini nasıl yaparsınız?

Kontrol süreci; gözden geçirme toplantıları, iç de dış denetimler, dış kaynak ile yapılan penetrasyon testleri ile yürütülmektedir.

Ayrıca sistemlere ilişkin periyodik bakım ve kontroller tanımlanmış olup ilgili kişiye otomatik görev olarak düşerek gerekli kontrolü yapması beklenmektedir.

11. Bilgi Güvenliği Yönetim Sisteminin uygulanması çalışanı nasıl etkiledi? Karşılaşılan zorluklar ne oldu?

Yeni uygulamalar ve mevcut uygulamaların daha zorlayıcı hale gelmesi çalışanı olumsuz yönde etkiledi. Örneğin; Temiz Masa Temiz Ekran Politikası, Parola sistematiğinin güvenli düzeye çekilmesi vb.

12. Bu sistem kurum için getirdiği yük ve maliyete değecek kadar fayda sağladı mı?

Yetkilendirilmiş Yükümlülük Statüsü başvuru yapabilmek için başvuru şartlarında ISO 27001 belgesinin olma zorunluluğu sebebiyle ISO 27001 belgesi bir yerden sonra Kurum için tercih değil zaten yasal olarak zorunluluk haline gelmiştir. Bu sebeple; yük ve maliyeti ne olursa olsun sistemin devamlılığı kaçınılmazdır.

Sistemin yasal zorunluluklar öncesinde kurulmuş olması mevzuata uyum açısından oldukça hızlı yol kat edilmesine olanak vermiştir. Örneğin; 6698 sayılı Kişisel Verilerin Korunması Kanunu teknik önlemleri açıklandığında, açıklanan önlemlerin bir çoğu zaten ISO 27001 kapsamında zaten Kurumumuzda yapılmaktaydı.

Bu açılardan baktığımızda; getirdiği yük ve maliyetin kat be kat üstünde bir faydası vardır.

13. İşleyiş sürecinde yönetimin bakışı ve desteği ne yönde değişti?

Hem kurulum hem de işleyiş sürecinde yönetim tarafından oldukça destek görüldü / görülmektedir.

14. **Uygulama sürecinde ilgili çalışanların BGYS' ye bakışı ve ilgisi ne yönde değişti?**

    Standarda ilişkin kullanıcı farkındalığı arttıkça "Bu konunun bilgi güvenliği açısından da değerlendirilmesi gerekmez mi? Bilgi güvenliği açısından bu bir risk teşkil eder mi?" gibi geri dönüşler almaya başladık. Ki bence bu da kullanıcı bakış açısının olumlu yönde değiştiğinin en güzel örneklerinden.

15. **BGYS denetim aşamasında belgelendirme kuruluşunun yaptığı ara denetimlerde ne tür sorunla karşılaştınız?**

    Denetçilerin kendi bakış açılarına ve daha önce görmüş / uygulamış oldukları sistemlerin birebir aynısını beklemesi ve bunların dışındaki uygulamalara karşı ön yargılı yaklaşmaları başlıca yaşadığımız sorundur.

16. **Bilgi Güvenliği Yönetim Sistemi kurulduktan sonra kuruluşunuzda karşılaşılan zorluklar nelerdir?**

    İşlerimizi daha kontrollü, prosedürdeki tüm adımları yerine getirerek ve bunlara ilişkin kayıtları oluşturarak yapmak yaşanan zorlukların başında gelmektedir.

17. **Tavsiyeleriniz nelerdir?**

    Sistem kurulumu sırasında üst yönetimin iradesi ve çalışanların desteğini mutlaka yanlarına alsınlar.

DÜZELTİCİ FAALİYETLER ve İYİLEŞTİRME

1. **Hangi uygunsuzluklar karşısında düzeltici faaliyetler düzenlediniz? Tekrar edilmemesi için hangi önlemleri aldınız?**

    Tespit edilen tüm uygunsuzluklar için düzeltici faaliyet düzenlenmektedir.

    Düzeltici faaliyetlerin tekrar edilebilir olup olmadığı düzeltici faaliyeti kapatırken yönetim temsilcisi tarafından değerlendirilmiş ve tekrarlı bir durum olması halinde yeni iyileştirmeler planlanmıştır.

2. **Belirlenen amaçlara ulaşmak için geçerli iyileştirmeler tespit ettiniz mi?**

    Politika ve stratejik plan kapsamında amaçlarımıza ulaşmak için hedefler belirliyor ve bu hedefleri takip ediyoruz. Hedeflere uyamadığımız durumlarda

kök nedenin araştırıp gerekirse iyileştirmeler yaparak amaca ulaşmanın yollarını arıyoruz.

3. **Bu süreçte açıklık ve sızma testleri yapıyor musunuz? Ne sıklıkta?**
   Dış kaynak ile her yıl en az 1 kez olmak üzere sızma testi yaptırıyoruz. Ayrıca yeni sistemlerin kurulması, mevcut sistemlerdeki değişiklikler durumunda da iç kaynaklar ile sızma testi yapıyoruz.

KURULUŞ B İLE YAPILAN GÖRÜŞME

BGYS ÖNCESİ HAZIRLIK SÜRECİ

1. **Kurumunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini kurmaya neden ihtiyaç duydunuz?**
   Mevcut IT süreçlerinin daha kaliteli bir şekilde yürütülebilmesi ve yasal mevzuatların ve şartların gereksinimlerini karşılayabilmek için ihtiyaç duyduk.
2. **Hazırlık için danışman firmadan yararlandınız mı? Eğer evetse bu süreç sizin için yararlı oldu mu? Hayırsa bu süreçte zorluk çektiniz mi? Bu yöntemi önerir misiniz?**
   Evet danışmanlık firmasından yararlandık. Bu süreç bizim için daha kolay oldu ve öneririm.
3. **Başvuru için oluşturduğunuz BGYS komitesi yeterli bilgiye sahip miydi? Bu konuda eğitim danışmanlık hizmeti aldınız mı?**
   Yeterli bilgiye sahipti. IT deki BGYS yöneticisi danışmandan aldığı bilgilerle BGYS Takımına eğitim vererek bilinçlendirme sağladı.
4. **Bu aşamada karşılaşılan zorluklar nelerdir?**
   Zorlukların önüne geçebilmek için BGYS Takımına da üst yönetim sponsor yapılarak yönetim desteği sağlandı. Kurulum esnasında planlı çalışıldığı ve üst yönetim desteği alındığı için iç zorluklarla karşılaşmadık. Yalnız dış denetimlerde denetçi yaklaşımları kişisel yorumlara dayanabildiği için mevcut uygulanan yöntemlerimizi kavrayamama durumu söz konusu durumlar oldu.
5. **Hazırlık süreci için bir öneriniz var mı?**
   Standartı iyi okuyup anlamalı ve kurum kendi yöntemlerini uygulamalı. Biz kurum olarak bu açıdan baktıktan sonra denetimlerde yöntemlerimizi kabul ettirebildik.

BGYS BAŞVURU AŞAMASI

1. **Kurumunuzda oluşturduğunuz ISO/IEC 27001 BGYS' nin kapsamı nedir? Hariç tutmaları gerekçelendirdiniz mi?**

   Bilgi Sistemleri Departmanı takip sorumluluğunda olan verilerin korunması. Standartın ana maddelerini hariç tutamıyorsunuz. Ek -A maddelerinde bizim için uygulanabilirliği olmayan maddeleri hariç tuttuk. Kriptografik kontrolleri örnek verebiliriz.

2. **Üst yönetim bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunup destekledi mi? Varsa yaşadığınız zorluklar nelerdir?**

   Üst yönetimin desteğini gördük ve bir sıkıntı yaşamadık.

3. **Bilgi Varlıklarınızı belirlerken nelere dikkat ettiniz?**

   Şirket ERP sürecinde (muhasebe, üretim, satış, satın alma, kalite, insan kaynakları vb. modüllerde oluşan bilgiler) işlem gören bilgiler. Kullanıcıların dokümanları, arşivler, dolaplar, şirket web sitesi buralarda bulunan bilgiler sınıflandırılmıştır. Bilgi varlıklarımız buradaki bilgileri kapsar.

4. **Bilgi Güvenliği Politikası ve prosedürler neleri kapsıyor, nasıl bir sistemle bunları hazırladınız?**

   BGYS el kitabı prosedürler ve politikalar standart maddelerine göre oluşturuldu. Dokümanlarımız doküman yönetim sistemi yazılımı ile kullanıcılara duyuruldu ve bu yazılım üzerinden doküman yönetimi gerçekleştirildi.

5. **Kurumunuzdaki riskleri belirlemek için hangi yöntemleri kullanıyorsunuz?**

   Risk değerlendirmesi bilgi güvenliğini tehdit eden tehlikeler tanımlandıktan sonra risk puanlaması ile yönetiliyor. Varlıklarımızın bir bilgi değeri bulunmaktadır. Riskin önem derecesini belirlerken bu riskin olasılığı sıklığı ve şiddeti göz önünde bulundurularak aksiyon alınıp alınmayacağına karar verilir.

6. **Kabul edilebilir veya risk iyileştirmesi gerektirecek seviyede öngörülmüş risk seviyesini nasıl belirlediniz?** Risk değerlendirme Prosedürü oluşturularak belirlenmiştir. Tablolar aşağıdaki gibidir.

4.3.1.2. Sıklık :

SIKLIK	PUAN
Çok seyrek(yılda bir defa veya daha seyrek)	0.5
Seyrek (yılda birkaç defa)	1.0
Sık değil (ayda bir defa veya birkaç defa)	2.0
Arada sırada (haftada bir veya birkaç defa)	3.0
Sık (günde bir veya birkaç defa)	6.0
Hemen hemen sürekli (birkaç saatte bir defa)	10

4.3.1.3. Şiddet:

Açıklığın gerçekleşmesi durumunda Etkinin Şiddeti: Üçü durum için ayrı değerlendirilir ve puanlanır. (Gizlilik+Bütünlük+Erişilebilirlik)

ETKİNİN ŞİDDETİ	ETKİ PUANI
Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur, süreçlerin durmasına sebep olabilir,	10
Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir, kurum büyük mali zarara uğrayabilir, süreçlerde aksamaya neden olabilir	6
Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir, kurum mali zarara uğrar, süreçler etkilenir	3
Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrayabilir, süreçler kısmen etkilenebilir	2
Kurumun bazı varlıkları etkilenir	1
Önemsiz	0,5

4.4. Varlık / Bilgi Değeri: Varlık bilgi değeri belirlenirken BG.F-08 Bilgi Sınıflama Formundaki bilgiler dikkate alınmıştır.

VARLIK / BİLGİ DEĞERİ	VARLIK PUANI	*BİLGİ DEĞERİ*
Kurumun ana işlevlerini büyük ölçüde tek başına üstlenen veya kurum için çok kritik bilgileri içeren veya maddi değeri yeniden bir bütçe tahsisi yapılamayacak kadar yüksek olan veya yeniden temini çok zor olan Bunlar sadece varlık sahibi tarafından yetkilendirilmiş, belirli bir birim veya kişilerin erişim ve kullanım yetkisi olan varlıklardır. Kişisel ve kurumsal bilgileri içeren veya kanunlar ile korunması gereken varlıklardır. Bir olay karşısında delil niteliğinde	Çok Yüksek - 50	***Çok Gizli***

bilgiler içeren varlıklardır. Bu varlıklar güvenli ortamlarda korunur ve bunlara yapılan erişimler kayıt altına alınır.		
Kurum ana işlevlerini kesintiye uğratabilecek veya kurum için kritik bilgileri içeren veya maddi değeri yüksek olan veya yeniden temini zor olan varlıklar. Bunlar sadece varlık sahibi tarafından yetkilendirilmiş kişilerin erişim sağlayacağı bilgileri içeren varlıklardır. Bu varlıklar güvenli ortamlarda korunur ve bunlara yapılan erişimler kayıt altına alınır.	Yüksek - 30	***Gizli***
Kurumun ana işlevlerinde bir kesintiye neden olabilecek veya kurum dışından görülmesi tercih edilmeyen verileri içeren veya yeniden satın alımının bütçe ve prosedür açısından bir miktar zaman aldığı varlıklardır, yerine koyması zaman alabilen ve kurumun ana işlevlerinde bir kesintiye neden olabilecek veya kurum dışından görülmesi tercih edilmeyen bilgileri içeren varlıklardır. ***Bilgiye erişim kurum içerisindeki belirli çalışanlara açıktır.***	Orta - 15	***Hizmete Özel***
Kurumun ana işlevlerini doğrudan etkilemeyen veya hassas bir veri içermeyen ancak yeniden satın alımının bütçe ve prosedür açısından bir miktar zaman aldığı ve Erişim denetimi ve kaydı gerektirmeyen bilgileri içeren varlıklardır.	Düşük - 5	***Şirket İçi***
Kurumun ana işlevlerini doğrudan etkilemeyen veya hassas bir veri içermeyen veya yeniden satın alımının kurumun bütçesi ve satın alma prosedürleriyle kolayca gerçekleştirilebildiği veya kolay temin edilebilen ve kurum dışındaki kullanıcı ve kişilerinde erişimine açık olan bilgileri de içeren varlıklardır.	Çok Düşük - 1	***Kamuya Açık***

4.5. Risk Büyüklüğü : Risk + Varlık Bilgi Değeri

RİSKİN ÖNEM DERECESİ	**RİSK BÜYÜKLÜĞÜ**
Tolerans gösterilemez risk, Hemen gerekli önlemler alınmalı	500 < R
Kritik risk, Kısa dönemde iyileştirilmelidir(bir kaç ay içinde)	300 < R < 500
Önemli risk, Orta dönemde iyileştirilmelidir (bir yıl içinde)	100 < R < 300
Olası risk, Kabul edilebilir risk Gözetim altında uygulanmalıdır	20 < R < 100
Önemsiz risk, Kabul edilebilir risk Önlem öncelikli değildir	R < 20

Riskin önem derecesine göre standardın Ek-A kısmında belirtilen kontrol yöntemlerinden uygun olanlar ilgili riski kontrol altına almak için uygulamaya konulur.

4.5.1. Riskin kontrol altına alınmasına yönelik alınan tedbirlerin etkinliği, tedbir alındıktan sonra yapılan risk değerlendirme sonucuna göre yapılır. Risk değerlendirme sonucu kabul edilebilir seviyelerde çıkarsa alınan tedbirin etkin olduğu anlamına gelir. İkinci risk değerlendirmeden sonra risk sonucu kabul edilebilir seviyenin üzerinde ise alınan tedbir etkin değildir anlamına gelir. Bu durumda yeni tedbirleri öngörmek gereklidir.

4.5.2. Artık Risk : Belirlenmiş olan kontrol yöntemleri etkin şekilde uygulamaya konulduktan sonra elde edilen sonuçlar dikkate alınarak yeniden risk değerlendirme faaliyeti yapılır. Risk değerlendirme sonucunda kalan riske artık risk denir.

4.5.3. Risk sorumlusunun (sahibinin) onayı: Bilgi güvenliğini tehdit eden tehlikelerin risk değerlendirme sonuçları, önem dereceleri, riskin azaltılmasına yönelik alınan tedbirler ve artık riskler konusunda risk sahibinin onayı alınır. Risk değerlendirmenin bütünü hakkında yönetim temsilcisinin onayı alındıktan sonra B.Ç Varlık Risk Analizi Risk Değerlendirme Tablosu ilgili tarafların bilgisine sunulur.

4.6. Risk değerlendirme güncellemeleri: BGYS kapsamında ve uygulamalarında hiçbir değişiklik olmadığı zaman yılda en az bir kere risk değerlendirme kayıtları gözden geçirilir. Bunun yanında kapsamda, uygulamalarda önemli değişiklikler olduğu zaman potansiyel tehlikeler dikkate alınarak risk değerlendirme kayıtları güncellenip gerekli kontrol yöntemleri belirlenerek uygulamaya konulur.

7. **Riskleri azaltmak ya da ortadan kaldırmak için ISO/IEC 27001 Ek – A maddelerinden hangisini seçtiniz?**

   Sadece çıkardıklarımızı söyleyeyim. A.9.4.5 Yazılım geliştirme ile ilgili maddeler, A.10.1, A.10.2 Kriptografik Kontrollerle ilgili maddeler bu üç madde haricinde diğer kontrol maddeleri seçtik.

8. **İlk başvurunuzda belgeyi alabildiniz mi? Eğer alamadıysanız neden alamadınız?**

   Belgeyi ilk başvuruda alabildik.

9. **Bu aşamada yaşadığınız temel zorluklar nelerdir?**

   İlk kurulumda Türkiye'de yeni olduğu için standardla ilgili Türkçe doküman bulunmuyordu. Bu nedenle standarttaki bazı kavramların anlaşılmasında hem kurulum hem denetimler esnasında zorluklar yaşanabiliyordu.

10. **Bu aşamada önerileriniz nelerdir?**

    Kurum kendi uygulama yöntemlerini kendisi belirlemeli. Danışman desteği alınırken buna dikkat etmeliler.

BGYS SONRASI

1. **Bilgi Güvenliği Yönetim Sistemi kuruluşunuzda kaç yıldır uygulanmaktadır?**

   Kuruluşumuzda 2009 yılından 2020 yılına kadar uygulandı.

2. **Bu sistemin kurumunuzun bilgi güvenliği açısından temel yararları nelerdir?**

   Borsada işlem gören şirketler mevzuat gereği dış denetimlere tabi tutulurlar. Belgenin olması bu tip denetimlerde gelen soruların cevaplanmasında kolaylık sağladı. Bilgi güvenliği, Bilgi Sistemleri departmanı ve ilgili diğer birimlerin veri akış yöntemlerine standard bir açıdan bakılmasına olanak sağlamıştır.

   Ayrıca normalde kullanıcılar tarafından ön yargı ile karşılanan bazı bilgi güvenliği faaliyetleri standardın gerekliliği olarak ifade edildiğinde daha çabuk kabul görmektedir.

3. **İşletmenin kurumsal prestijine ne tür katkılar sağladı?**

   Belgenin olması ve sektörde BGYS belgesi olan ilk çimento fabrikası olması nedeniyle kuruma prestij sağlamıştır.

4. **Kurumunuzda BGYS' nin uygunluğunun ve etkinliğinin tespitini nasıl yapıyorsunuz?**

   İç denetimler ve dış denetimlerle yapıyoruz.

5. **Kurumunuzda iç denetimi kendiniz mi yoksa danışman firma mı yapıyor?**

   İç denetimi nasıl yapıyorsunuz? İç denetimi kendimiz yapıyoruz. Kurum içerisinde çalışanlara iç denetçi sertifikası alınarak kendi çalışanlarımız tarafından gerçekleştiriyoruz. Saha ve doküman içerikli gerçekleştiriyoruz.

6. **Sistemin uygulanması kurum üzerindeki iş yükünü olumlu ya da olumsuz yönde etkiledi mi? Bunlar nelerdir?**

   Olumsuz yönü, kurum içerisinde BGYS' nin sadece IT' nin sorumluluğundaymış gibi görünmesi ve IT' deki çalışan sayısının az olması iş yükünü arttırmaktadır. Olumlu yönü ise IT ihtiyaçlarını bilgi güvenliği kapsamında değerlendirerek daha kolay temin edebiliyorduk.

7. **Uygulama sürecinde danışmanlık firmasından destek alıyor musunuz? Evetse bu oran ne kadardır?**

   Uygulama sürecinde aklımıza takılan sorular olduğu zaman yardım aldık. Çok düşük bir oran.

8. **Kuruluşunuzda diğer yönetim sistemlerini kullanıyor musunuz? Eğer kullanıyorsanız bilgi güvenliği yönetim sistemi bunlarla uyumlaştırıldı mı? Uyumlaştırılırken nasıl sorunlarla karşılaştınız?**

   Diğer yönetim sistemleri kullanılmaktadır. Bütün yönetim sistemleri Entegre Yönetim Sistemi (EYS) kapsamında değerlendirildiği için birlikte yürütüldü. BGYS standartları aynı zamanda Ek A maddelerini de içerdiği için diğer yönetim sistemlerinden farklılık göstermektedir. Kurum EYS el kitabı oluştururken mecburen BGYS yi ayrı tutmak zorunda kalmış ve BGYS El Kitabı oluşturmuştur. Ek A maddelerinden dolayı uyumlaştırmada zorluk çektik. Çimento sektöründe API (Amerikan Petrol Enstitüsü) yönetim sistemi vardır. Bu yönetim sistemi kurumun petrol çimentosu üretebilmesine olanak sağlamaktadır. BGYS' nin kurumda olması bu belgenin alınmasında fayda sağlamıştır.

9. **Kurumunuzda eğitim ve bilinçlendirme çalışmalarını hangi aralıklarla, nasıl yapıyorsunuz?**

   Belirli aralıklarla ve tüm çalışanlara farkındalık eğitimleri verilmektedir.

10. **Kurumunuzda kontrol sürecini nasıl yaparsınız?**

    BGYS' nin kontrolü iç tetkikler, yönetim gözden geçirme ve dış tetkiklerle gerçekleştirilir.

11. **Bilgi Güvenliği Yönetim Sisteminin uygulanması çalışanı nasıl etkiledi? Karşılaşılan zorluklar ne oldu?**

    Veri güvenliği açısından çalışanın yüksek düzeyde bilinçli olmasını sağladı.

12. **Bu sistem kurum için getirdiği yük ve maliyete değecek kadar fayda sağladı mı?**

    Katkı sağladı. API denetimlerinde ve mali denetimlerde BGYS' nin olması fayda sağlar.

13. **İşleyiş sürecinde yönetimin bakışı ve desteği ne yönde değişti?**

İşleyiş sürecinde YGG toplantılarında BGYS hedefleri için gerekli aksiyonlara kaynaklar sağlanıyordu.

14. **Uygulama sürecinde ilgili çalışanların BGYS' ye bakışı ve ilgisi ne yönde değişti?**

    Çalışanların bilgi güvenliği konularında sadece şirket için değil kendi kişisel verileri için de farkındalıkları oluştu.

15. **BGYS denetim aşamasında belgelendirme kuruluşunun yaptığı ara denetimlerde ne tür sorunla karşılaştınız?**

    Ara denetimlerde özellikle önceki yıl çıkan minör uygunsuzluklar önem arz ediyor. Bu uygunsuzlar için aldığımız aksiyonların yeterlilikleri bazen sorgulanabiliyordu

16. **Bilgi Güvenliği Yönetim Sistemi kurulduktan sonra kuruluşunuzda karşılaşılan zorluklar nelerdir?**

    BGYS' nin sürecinin yönetimi sadece IT çalışanlarında olduğu için iş yükünü arttırabiliyordu.

17. **Tavsiyeleriniz nelerdir?**

    BGYS organizasyonunun (ekibinin) mutlaka BGYS kapsamını ilgilendiren birimlerden oluşması sağlanmalıdır.

DÜZELTİCİ FAALİYETLER ve İYİLEŞTİRME

1. **Hangi uygunsuzluklar karşısında düzeltici faaliyetler düzenlediniz? Tekrar edilmemesi için hangi önlemleri aldınız?**

   İç denetimler, dış denetimler ve risk değerlendirme sonucunda çıkan uygunsuzluklara düzeltici faaliyetler düzenlenmiştir. Düzeltici faaliyetin etkinliği yeniden risk değerlendirme yapılarak kontrol edilmiştir.

2. **Belirlenen amaçlara ulaşmak için geçerli iyileştirmeler tespit ettiniz mi?**

   Yıllık BGYS hedefleri, süreç ölçümleri üzerine iyileştirmeler mevcuttur.

3. **Bu süreçte açıklık ve sızma testleri yapıyor musunuz? Ne sıklıkta?**

   Belirli aralıklarla sızma testi yapılıyordu.

KURULUŞ C İLE YAPILAN GÖRÜŞME

BGYS ÖNCESİ HAZIRLIK SÜRECİ

1. **Kurumunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini kurmaya neden ihtiyaç duydunuz?**
   Uluslararası standart olmasından ve tüm dünyada geçerliliği kabul edildiğinden dolayı BGYS' yi kurmaya karar verdik.
2. **Hazırlık için danışman firmadan yararlandınız mı? Eğer evetse bu süreç sizin için yararlı oldu mu? Hayırsa bu süreçte zorluk çektiniz mi? Bu yöntemi önerir misiniz?**
   Danışman firmadan yararlanmadık. Süreç zor değildi.
3. **Başvuru için oluşturduğunuz BGYS komitesi yeterli bilgiye sahip miydi? Bu konuda eğitim danışmanlık hizmeti aldınız mı?**
   BGYS Komitesi yeterli bilgiye sahipti ve eğitim almadık.
4. **Bu aşamada karşılaşılan zorluklar nelerdir?**
   Zorluk yaşamadık. IT departmanı olarak bilgi birikimimiz yeterliydi bu sebeple zorluk yaşamadık.
5. **Hazırlık süreci için bir öneriniz var mı?**
   Şirket bünyesinde uzun yıllar bu alanda hizmet veren IT yetkilisi varsa, bu gibi süreçler daha rahat aşılabiliyor.

BGYS BAŞVURU AŞAMASI

1. **Kurumunuzda oluşturduğunuz ISO/IEC 27001 BGYS' nin kapsamı nedir? Hariç tutmaları gerekçelendirdiniz mi?**
   Kapsam olarak, ERP, IK, AR-GE, Satın Alma, Muhasebe, Sevkiyat, Satış ve Mali işler bulunmaktadır.
2. **Üst yönetim bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunup destekledi mi? Varsa yaşadığınız zorluklar nelerdir?**
   Firmamızda bulunan IT altyapısı, Üst Yönetimin telkinleriyle oluşturulmuştur. Eğer bilinçli üst yönetime sahip olmasaydık, yatırım maliyetlerini IT departmanının istediği seviyede tutamazdık.
3. **Bilgi Varlıklarınızı belirlerken nelere dikkat ettiniz?**

Şirketimiz için gizliliği olan bilgilerden başlayarak genel bilgilere doğru sıraladık.

4. **Bilgi Güvenliği Politikası ve prosedürler neleri kapsıyor, nasıl bir sistemle bunları hazırladınız?**

   Politikalarımızın en önemli aşaması yetkilendirmelerdir. Şirket CEO'sundan, en küçük birimine kadar yetkilendirerek, kişilerin ilgi alanı dahilinde olmayan bütün bölümlere erişimleri kısıtlıdır.

   Kurumunuzdaki riskleri belirlemek için hangi yöntemleri kullanıyorsunuz?

   Risk değerlendirme tablosu düzenliyoruz. Risklere puan vererek derecelerini belirliyoruz. Ayrıca kurumlardaki riskler büyük oranda insan faktörlüdür. Eğitimler vererek riskleri minimuma indirmeyi amaçlıyoruz. Dijital olarak azaltmış olsak bile, insan faktörü her zaman risk taşıyacaktır.

5. **Kabul edilebilir veya risk iyileştirmesi gerektirecek seviyede öngörülmüş risk seviyesini nasıl belirlediniz?**

   Kurumun bilgi güvenliği durumunu baz alarak kabul edilebilir risk seviyesi belirlenmiştir. Bu durum her yıl Yönetim Gözden Geçirme toplantısında bu risk seviyeleri güncellenmektedir.

6. **Riskleri azaltmak ya da ortadan kaldırmak için ISO/IEC 27001 Ek – A maddelerinden hangisini seçtiniz?**

   EK-A maddelerini hepsini uyguluyoruz.

7. **İlk başvurunuzda belgeyi alabildiniz mi? Eğer alamadıysanız neden alamadınız?**

   İlk başvurumuzda alamadık. Çünkü bilgi işlem odasındaki kabinet yeri ile ilgili ufak sorunlar çıkmıştı. Sonrasında iyileştirmeler yaparak sorunu çözdük.

8. **Bu aşamada yaşadığınız temel zorluklar nelerdir?**

   Daha önce de belirttiğim gibi güçlü bir IT departmanımız olduğu için bir zorluk yaşamadık.

9. **Bu aşamada önerileriniz nelerdir?**

   Hazırlık sürecinin 4. Maddesinde belirttiğim gibi, iyi bir IT departmanı olması şart. Firma bünyesinde IT departmanı var ise, bu gibi sistemler zaten olması gerekenler. Ayrıca çalışanlarda farkındalık yaratarak sürece dahil etmek bu süreci daha kolay kılmaktadır.

BGYS SONRASI

1. **Bilgi Güvenliği Yönetim Sistemi kuruluşunuzda kaç yıldır uygulanmaktadır?**
   Uzun süredir uygulanan BGYS sertifikamız 2019 yılında yenilenmiştir.
2. **Bu sistemin kurumunuzun bilgi güvenliği açısından temel yararları nelerdir?**
   Hem çalışan hem de yönetim açısından bilginin güvenle saklanması en önemli yarar bizler için.
3. **İşletmenin kurumsal prestijine ne tür katkılar sağladı?**
   Bu standart uluslararası geçerliliği olan bir standard olduğu için firmamız global pazarda yerini almıştır. Çalıştığımız firmaların bir çoğu zaten bu sertifikayı zorunlu tutuyor.
4. **Kurumunuzda BGYS' nin uygunluğunun ve etkinliğinin tespitini nasıl yapıyorsunuz?**
   İç ve dış denetimlerle yapmaktayız. Ayrıca IT departmanı sürekli ve rutin olmak üzere iki çalışma yapmaktadır. Sürekli olarak sunucuların güvenlik kontrolü, rutin olarak ise çalışanlarımızın PC kontrolleri.
5. **Kurumunuzda iç denetimi kendiniz mi yoksa danışman firma mı yapıyor?**
   IT departmanımız yapmaktadır.
6. **Sistemin uygulanması kurum üzerindeki iş yükünü olumlu ya da olumsuz yönde etkiledi mi? Bunlar nelerdir?**
   Yetkilendirme beklemeleri gereken süreçte tabi ki aksaklıklar olmaktadır. Anlık yetkilendirme istekleri, çeşitli onaylardan geçerek yapıldığı için süreç biraz uzuyor.
7. **Uygulama sürecinde danışmanlık firmasından destek alıyor musunuz? Evetse bu oran ne kadardır?**
   Almıyoruz.
8. **Kuruluşunuzda diğer yönetim sistemlerini kullanıyor musunuz? Eğer kullanıyorsanız bilgi güvenliği yönetim sistemi bunlarla uyumlaştırıldı mı? Uyumlaştırılırken nasıl sorunlarla karşılaştınız?**
   Yönetim sistemi olarak BGYS haricinde Kalite Yönetim Sistemi mevcut. KVKK (Kişisel Verileri Koruma Kurumu) uyumu sürecinde, BGYS'nin çok faydasını gördük. Hatta IT olarak hiç sorun yaşamadık.

9. **Kurumunuzda eğitim ve bilinçlendirme çalışmalarını hangi aralıklarla, nasıl yapıyorsunuz?**

   3 ayda bir farkındalık eğitimleri düzenliyoruz. Ayrıca bilgi güvenliği ile ilgili broşürler hazırlayıp duyurular yapıyoruz.

10. **Kurumunuzda kontrol sürecini nasıl yaparsınız?**

    Sunucu ve İstemci taraflı olarak kontrol işlemlerini yapmaktayız.

    Bilgi Güvenliği Yönetim Sisteminin uygulanması çalışanı nasıl etkiledi? Karşılaşılan zorluklar ne oldu?

    Çalışanlarımız tam uyum içindeydi. Zira çalışanın, üzerinde çalıştıkları verilerin güvenli olduğunu bilmeleri çok önemli.

11. **Bu sistem kurum için getirdiği yük ve maliyete değecek kadar fayda sağladı mı?**

    Çalıştığımız firmaların çoğu bu sertifikayı zorunlu tuttuğundan yük ve maliyet getirisi ne olursa olsun sistemin sürekliliği kaçınılmaz olmuştur. Bu yüzden yük ve maliyete değecek kadar fayda sağlamıştır.

12. **İşleyiş sürecinde yönetimin bakışı ve desteği ne yönde değişti?**

    Üst Yönetim sürecin başından beri tam destek vererek IT departmanını sağlamlaştırdı.

13. **Uygulama sürecinde ilgili çalışanların BGYS' ye bakışı ve ilgisi ne yönde değişti?**

    Bilgi güvenliği açısında çalışma şartlarına adapte olan çalışanların özel hayatlarında da bilgi güvenliği farkındalıkları artmıştır. Biz eğitimler esnasında bu konulara da yer veriyoruz.

14. **BGYS denetim aşamasında belgelendirme kuruluşunun yaptığı ara denetimlerde ne tür sorunla karşılaştınız?**

    Herhangi bir zorlukla karşılaşmadık.

15. **Bilgi Güvenliği Yönetim Sistemi kurulduktan sonra kuruluşunuzda karşılaşılan zorluklar nelerdir?**

    Hiçbir zorlukla karşılaşmadık.

16. **Tavsiyeleriniz nelerdir?**

    Firmalar bünyelerine IT departmanı kurarak, bu alanda en az 10 yıl çalışmış olan kişileri tercih etmelidir. BGYS'nin asıl kanayan yarası da burasıdır. Bir

çok orta-büyük ölçekteki firmanın henüz bünyesinde IT departmanı bile yok. Bu sebeple dışarıdan alınan hizmetler bana kalırsa zaten bir güvenlik açığıdır.

DÜZELTİCİ FAALİYETLER ve İYİLEŞTİRME

1. **Hangi uygunsuzluklar karşısında düzeltici faaliyetler düzenlediniz? Tekrar edilmemesi için hangi önlemleri aldınız?**
   Olumsuzluk yaşamadık, yaşamamak için çok uç noktalarda önlemler almıştık.
2. **Belirlenen amaçlara ulaşmak için geçerli iyileştirmeler tespit ettiniz mi?**
   Bu bir süreç zaten. Yaptım bitti olayı IT alanında imkansızdır. Bugün yaparsınız yarın yeni bir saldırı mekanizması ile kırılır. IT departmanı sistemleri sürekli takip etmekle zorunludur. Aksi taktirde, bugünü kurtarsanız bile yarınınız sürekli tehlikededir.
3. **Bu süreçte açıklık ve sızma testleri yapıyor musunuz? Ne sıklıkta?**
   Yapıyoruz. Sosyal mühendisliğimizi aksatmadan, yeni bilgi ve haberlerle, sürekli takip ediyor ve testlerimizi yapıyoruz.

TAT METAL İLE YAPILAN GÖRÜŞME

BGYS ÖNCESİ HAZIRLIK SÜRECİ

1. **Kurumunuzda ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemini kurmaya neden ihtiyaç duydunuz?**
   Bilgi güvenliğinin sağlanması, işletmemizin yürüttüğü genel faaliyetlerinden ve yasal gerekliliklerden dolayı yönetim sistemini kurmaya gerek duyduk.
2. **Hazırlık için danışman firmadan yararlandınız mı? Eğer evetse bu süreç sizin için yararlı oldu mu? Hayırsa bu süreçte zorluk çektiniz mi? Bu yöntemi önerir misiniz?**
   Evet bir firmadan danışmanlık alındı. Süreçlerin daha kolay bir şekilde yürütülmesi açısından yararlı gördüğüm için öneriyorum.
3. **Başvuru için oluşturduğunuz BGYS komitesi yeterli bilgiye sahip miydi? Bu konuda eğitim danışmanlık hizmeti aldınız mı?**
   BGYS ekibinin bilgisi yoktu. Danışmanlık desteği alarak ekibe eğitimler verildi.
4. **Bu aşamada karşılaşılan zorluklar nelerdir?**

Biz belgeyi ilk zamanlarda alan bir firmayız. Bu sebeple doküman ve bilgi eksikti, kimsenin bilgisi yoktu bu konularda zorluklar yaşandı.

5. **Hazırlık süreci için bir öneriniz var mı?**
   Daha önce bu belgeyi almış bir firma ile keşif çalışması yapılmalı ve bilgi alışverişinde bulunulmalı.

BGYS BAŞVURU AŞAMASI

1. **Kurumunuzda oluşturduğunuz ISO/IEC 27001 BGYS' nin kapsamı nedir? Hariç tutmaları gerekçelendirdiniz mi?**
   Kapsam; İnsan Kaynakları, Bilgi İşlem, Muhasebe, Finans, İdari İşler, Satın Alma, Satış ve Pazarlama, Dış Ticaret (İthalat ve İhracat), Lojistik departmanlarından oluşmaktadır.
2. **Üst yönetim bilgi güvenliği yönetim sisteminin etkinliğine katkıda bulunup destekledi mi? Varsa yaşadığınız zorluklar nelerdir?**
   Üst yönetim gerekli desteği vermiştir. Bu konuda hiçbir sıkıntı yaşamadık.
3. **Bilgi Varlıklarınızı belirlerken nelere dikkat ettiniz?**
   Firmanın sahip olduğu her şeyi varlık olarak belirledik.
   Bilgi Güvenliği Politikası ve prosedürler neleri kapsıyor, nasıl bir sistemle bunları hazırladınız?
   BGYS kapsamındaki her şeyi kapsıyor. BGYS' nin gerekli kıldığı doküman ve yazılı kaynakları kapsamaktadır. Bu konuda 53 tane dosya hazırladık.
4. **Kurumunuzdaki riskleri belirlemek için hangi yöntemleri kullanıyorsunuz?**
   Varlık değeri, riskin etkisi ve olma sıklığı değerleri ile riske puan vererek risk analiz tablosu oluşturduk.
   Kabul edilebilir veya risk iyileştirmesi gerektirecek seviyede öngörülmüş risk seviyesini nasıl belirlediniz?
   Risklere puan veriyoruz. Gizliliği, bütünlüğü, erişilebilirliği, olasılığı yani gerçekleştirme olasılığını etkiliyor mu diye risklere puan verip riski hesaplıyoruz.

RİSK DEĞERİ	EYLEM
80-125	KRİTİK RİSK Acil olarak müdahale edilir
26-79	ÖNEMLİ RİSK Mümkün olduğunca çabuk müdahale edilir
3-25	KABUL EDİLEBİLİR RİSK Acil aksiyon planlanmaz

5. **Riskleri azaltmak ya da ortadan kaldırmak için ISO/IEC 27001 Ek – A maddelerinden hangisini seçtiniz?**
   Hepsini uyguladık.
6. **İlk başvurunuzda belgeyi alabildiniz mi? Eğer alamadıysanız neden alamadınız?**
   Evet, ilk başvurumuzda belgeyi aldık.
7. **Bu aşamada yaşadığınız temel zorluklar nelerdir?**
   Bilgi güvenliği konusunda çalışanların yeterli bilgiye sahip olmaması, yeni iş tarzı, uyulması gereken yeni kurallar, daha kontrollü çalışmak bu aşamada yaşadığımız zorluklardandır.
8. **Bu aşamada önerileriniz nelerdir?**
   BGYS için bir ekip oluşturmaları ve işletmeye özgü uygulama prosedürlerini belirlemeleri.

BGYS SONRASI

1. **Bilgi Güvenliği Yönetim Sistemi kuruluşunuzda kaç yıldır uygulanmaktadır?**
   2016 yılından itibaren uygulanmaktadır.
2. **Bu sistemin kurumunuzun bilgi güvenliği açısından temel yararları nelerdir?**
   Farkındalık yaratıldı, kullanıcılar daha dikkatli olmaya başladı, bilginin önemi arttı. Standart, bilgi güvenliğine kişisel olarak değil de standart açısından bakabilmeyi sağlamıştır.
3. **İşletmenin kurumsal prestijine ne tür katkılar sağladı?**

Firma genel olarak yönetim sistemlerine önem vermektedir. Bu belge, global çapta tanınırlığımızı artırmış ve pazardaki prestijimizi artırmıştır.

4. **Kurumunuzda BGYS' nin uygunluğunun ve etkinliğinin tespitini nasıl yapıyorsunuz?**

   Denetimlerde belli oluyor, iç ve dış denetim ile yapıyoruz.

5. **Kurumunuzda iç denetimi kendiniz mi yoksa danışman firma mı yapıyor? İç denetimi nasıl yapıyorsunuz?**

   Kurum içinde iç tetkik belgesi olan çalışanlar ile iç denetim yapılmaktadır. İç denetim planına göre her bölüme tek tek gidilerek saha, soru ve fiziksel denetim şeklinde yapılıyor.

6. **Sistemin uygulanması kurum üzerindeki iş yükünü olumlu ya da olumsuz yönde etkiledi mi? Bunlar nelerdir?**

   Kuşkusuz olumlu etkiliyor ama bu belgeler iş yükü çıkartıyor. Uygulama sonrasında ise sistemin faydaları iş yükünü gözle görülür derecede aza indirgemiştir.

7. **Uygulama sürecinde danışmanlık firmasından destek alıyor musunuz? Evetse bu oran ne kadardır?**

   Hayır. Belgeyi aldıktan sonra destek almayı bıraktık.

8. **Kuruluşunuzda diğer yönetim sistemlerini kullanıyor musunuz? Eğer kullanıyorsanız bilgi güvenliği yönetim sistemi bunlarla uyumlaştırıldı mı? Uyumlaştırılırken nasıl sorunlarla karşılaştınız?**

   Çevre Yönetim Sistemi, İş Sağlığı ve Güvenliği Sistemi Yönetimi, Kalite Yönetim Sistemi, Otomotiv Kalite Yönetim Sistemi, Enerji Yönetim Sistemi' ne sahibiz. Bunlar sonuçta iç içe olan sistemlerdir herhangi bir sorun yaşamadık.

9. **Kurumunuzda eğitim ve bilinçlendirme çalışmalarını hangi aralıklarla, nasıl yapıyorsunuz?**

   Yılda bir kez farkındalık eğitimi verilmektedir.

10. **Kurumunuzda kontrol sürecini nasıl yaparsınız?**

    İç denetim ve dış denetim ile yapıyoruz.

Bilgi Güvenliği Yönetim Sisteminin uygulanması çalışanı nasıl etkiledi? Karşılaşılan zorluklar ne oldu?

Tabi bazı kurallar koyularak çalışanların bu kurallara uymak zorunda kalması olumsuz tepkilere sebep oldu. Örneğin; Masaüstü temizliği, evrakların kırpılması, şifre zorunluğu, ekran kitleme gibi kurallar koyuldu.

11. **Bu sistem kurum için getirdiği yük ve maliyete değecek kadar fayda sağladı mı?**

    Tabikî bu sistemin bir çok faydası vardır. Fakat bizim kuruluşumuzda öncesi ile sonrasın arasında pek bir fark olmamıştır.

12. **İşleyiş sürecinde yönetimin bakışı ve desteği ne yönde değişti?**

    Yönetim her aşamada desteğini tam gösterdi.

13. **Uygulama sürecinde ilgili çalışanların BGYS' ye bakışı ve ilgisi ne yönde değişti?**

    Olumlu olmuştur. Çalışanların özel hayatında da çalışma hayatında da bilgi güvenliği farkındalığının olumlu açıdan değişmesine sebep oldu.

14. **BGYS denetim aşamasında belgelendirme kuruluşunun yaptığı ara denetimlerde ne tür sorunla karşılaştınız?**

    Hiçbir sorun ile karşılaşma olmamıştır.

15. **Bilgi Güvenliği Yönetim Sistemi kurulduktan sonra kuruluşunuzda karşılaşılan zorluklar nelerdir?**

    Belgelerin devamlılığı ve takip, bunlar iş yükü ve zaman kaybı getiriyor.

16. **Tavsiyeleriniz nelerdir?**

    Üst yönetimin desteği ile beraber BGYS konusunda bilgili çalışan tarafından ekibin oluşturulması sağlanmalı. Belgeyi almış olmak için almamalı uygulamak için almalıyız.

DÜZELTİCİ FAALİYETLER ve İYİLEŞTİRME

1. **Hangi uygunsuzluklar karşısında düzeltici faaliyetler düzenlediniz? Tekrar edilmemesi için hangi önlemleri aldınız?**

   Uygunsuzluklar belirlenip Düzeltici Faaliyet açılarak kalıcı ve geçici önlemler alınıp tekrar edilmemesi için gerekli görülen yerlerde eğitim ve iyileştirmelere yer verilmektedir.

2. **Belirlenen amaçlara ulaşmak için geçerli iyileştirmeler tespit ettiniz mi?**

Tabi iyileştirmeler olmasa belge boş duruyor demektir. Belgenin çalışması için her zaman iyileştirme olur. Politika ve hedeflerimizi gerçekleştiremediğimiz durumlarda sorunu bulup çözüm yolları bulmaya çalışıyoruz.

3. **Bu süreçte açıklık ve sızma testleri yapıyor musunuz? Ne sıklıkta?**

   Şimdiye kadar yapmadık ama 2021 içinde yapılacak. Esasında en az yılda bir kere yapılması gerekiyor.