İLLER BANKASI ANONİM ŞİRKETİ

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNE KURUMSAL GEÇİŞ SÜRECİ VE UYGULAMASI

Mehmet ÖTEGEN

UZMANLIK TEZİ

HAZİRAN 2018


İLBANK
TÜRKİYE'NİN YAPICI GÜCÜ

İLLER BANKASI ANONİM ŞİRKETİ

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNE KURUMSAL GEÇİŞ SÜRECİ VE UYGULAMASI

Mehmet ÖTEGEN

UZMANLIK TEZİ

Tez Danışmanı (Kurum)
Namık ÇETİNER

Tez Danışmanı (Ankara Üniversite)
Dr. Öğr. Üyesi Mustafa DOĞAN

Mehmet ÖTEGEN tarafından hazırlanan "ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNE KURUMSAL GEÇİŞ SÜRECİ VE UYGULAMASI" adlı tez çalışması aşağıdaki Yeterlik Sınav Kurulu tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile UZMANLIK TEZİ olarak kabul edilmiştir.

	Unvanı	Adı ve Soyadı	İmzası
Başkan	Genel Müdür Yardımcısı	Salih YILMAZ	
Üye	Daire Başkanı	Hüseyin TÖREN	
Üye	Daire Başkanı	Hakkı ÇIRAK	
Üye	Daire Başkanı	Orhan IŞIK	
Üye	Daire Başkanı	Doç. Dr. Birol KAYRANLI	

Tez Savunma Tarihi: 19.06.2018

ETİK BEYAN

"İLLER BANKASI ANONİM ŞİRKETİ Uzmanlık Tezi Yazım Kuralları"na uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Mehmet ÖTEGEN
19 Haziran 2018

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemine Kurumsal Geçiş Süreci Ve Uygulaması

(Uzmanlık Tezi)

Mehmet ÖTEGEN

İLLER BANKASI A.Ş.

Haziran 2018

ÖZET

Modern çağın en mühim niteliklerinden olan hız faktörü ticarette, eğitimde, haberleşmede, ulaşımda kısacası her alanda hissedilir bir şekilde etkisini göstermeye başlamıştır. Kimilerine göre bilgi çağı olarak adlandırılan modern çağda bilginin iletimi, erişimi, paylaşımı hızlanmış ve kolaylaşmıştır. Ancak bilgiye kolay erişebilenler yalnızca bilginin sahipleri değildir. Art niyetli kişiler de piyasadan kolayca edinilen yazılımlarla dev kurumların en mahrem bilgilerine erişebilmekte ve kurumlarda yüklü miktarda zarara sebebiyet verebilmektedirler. Bu girişimler bilgiyi elinde bulunduranları bilgi güvenliği üzerine çalışma yapmaya sevk etmiştir. Bu çalışmalar sonucunda ISO 27001 Bilgi Güvenliği Yönetim sistemi ortaya çıkmıştır. ISO 27001, herhangi bir faaliyet sınırı olmaksızın bilgi güvenliği endişesi taşıyan tüm kurumlara kendi bilgi güvenlik sistemlerini inşa etmeleri için rehberlik sağlayan bir standarttır. Bu tez çalışmasında bilginin, bilgi güvenliğinin ve risk kavramının muhteviyatına değinildikten sonra ISO 27001 Bilgi Güvenliği Yönetim Sisteminin tanıtımı yapılmıştır. Nihai olarak ISO 27001 Bilgi Güvenliği Yönetim Sistemine geçiş yapacak kurumların atması gereken adımlara yer verilmiş ve ISO 27001 sertifikası edinmiş kurumlardan örnekler verilerek anlatım zenginleştirilmeye gayret gösterilmiştir.

Anahtar Kelimeler	:	Bilgi, ISO/IEC 27001, BGYS, Risk Yönetimi, Bilgi Güvenliği
Sayfa Adedi	:	111
Tez Danışmanı	:	Namık ÇETİNER (Kurum)
Tez Danışmanı	:	Dr. Öğr. Üyesi Mustafa DOĞAN (Ankara Üniversitesi)

ISO / IEC 27001 Informatıon Securıty Management System Instıtutıonal Transıtıon Process And Implementatıon

(Expertise Thesis)

Mehmet ÖTEGEN

İLLER BANKASI ANONIM SIRKETI

June 2018

ABSTRACT

Speed factor which is the most important feature of modern era, demonstrate its effect on trade, education, telecommunication, transportation as matter of fact every single field. In the modern age, which according to some people is called the information age, the transmission, access and sharing of information is accelerated and facilitated. Unfortunately owners of the information are not the only one who can access information. Vicious people can also access the most intimate information of giant corporations with software that is easily acquired from the market and they can cause a serious damage on the institutions. These initiatives have encouraged those who hold information to work on information security. As a result of these studies, ISO 27001 Information Security Management System has emerged. ISO 27001 is a standard that provides guidance to all institutions with information security concerns without any operational limitations to build their own information security systems. In this thesis study, ISO 27001 Information Security Management System was introduced after the contents of information, information security and risk concept were mentioned. Ultimately, the steps to be taken by the institutions that will transition to the ISO 27001 Information Security Management System are mentioned and efforts have been made to enrich the narration by giving examples from the institutions that have obtained ISO 27001 certificate.

Key Words	:	Information, ISO / IEC 27001, ISMS, Risk Management, Information Security
Page Number	:	111
Supervisor	:	Namık ÇETİNER (Corporate)
Supervisor	:	Asst. Prof. Mustafa DOĞAN (Ankara University)

TEŞEKKÜR

Uzmanlık tezimin yazım sürecinde yardımlarını esirgemeyen kurum danışmanım Sayın Namık ÇETİNER' e ve üniversite danışmanım Sayın Yrd. Doç. Dr. Mustafa DOĞAN ' a;

Verdikleri değerli bilgiler ve yardımları sebebiyle kurum arkadaşlarım Sayın Sedat GÖKDOĞAN' a ve Fırat KAYA' ya;

Dualarını esirgemeyen aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış olan kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

BGYS	Bilgi Güvenliği Yönetim Sistemi
BS	British Standard
BSI	British Standard Institute
BT	Bilgi Teknolojileri
CEO	Chief Executive Office
GASCO	Abu Dhabi Gas Industries Ltd
GSMH	Gayri Safi Milli Hasıla
IDPS	Intrusion Detection and Prevention Systems
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
JTC	Joint Technical Committee
NATO	North Atlantic Treaty Organization
PUKÖ	Planla-Uygula-Kontrol Et-Önlem Al
TDK	Türk Dil Kurumu
TSE	Türk Standartları Enstitüsü
TURKAK	Türk Akreditasyon Kurumu
UKAS	United Kingdom Accreditation Service
VPN	Virtual Private Network
WEF	World Economic Forum
WG	Working Group

GİRİŞ

Asırlardır ihtiyaçlarının peşinden koşan insanoğlu, bu uğurda elindeki kaynakları cömert bir şekilde kullanmıştır. Kimi zaman ihtiyaçlarını tatmin etmek için sahip olması gereken unsur cilalı taş iken kimi zaman demir olmuştur. Bu unsurlar zamanın gelişimi üzerinde o kadar belirleyici rol oynamışlardır ki çağlara adını vermiştirler. Kimi bilim adamlarına göre içinde bulunulan çağa adını veren unsur ise bilgidir. Bağımsız danışmanlık firması Brand Finance' ın yaptığı araştırmanın sonucuna göre 2017 yılının en değerli markasının, bir '' bilgi'' arama motoru olan ''Google'' olması son dönemde bilgiye olan talebi gözler önüne sermektedir.

İnsanoğlu peşinden koştuğu ihtiyaçlarını tatmin etmek için her zaman ahlaki yolları tercih etmemiştir. Hırsızlık, yağma, dolandırıcılık bu gayriahlaki yollardan sadece birkaçıdır. Bir ticari mala atfedilen değer arttıkça onu yasal olmayan yollardan elde etmek isteyenlerin yaptıkları hazırlıklar en az o ölçüde artmaktadır. Buna karşılık ticari malını korumak isteyen mülk sahibi de bir o kadar çaba sarf etmek durumunda kalmıştır. Koyun sürüsü sahibi bir çiftçi için kurtarıcı kangal köpeği iken altınlarını muhafaza etmek isteyen bir tacir için çelik kasalar bu rolü üstlenmiştir. Günümüzün en önemli ticari metalarından biri olan bilginin muhafazası ise kurumları çok daha uzun vadeli ve sürekli kendini güncelleyen çözümler aramaya itmiştir zira bilgi paylaşımının, kopyalanmasının ve yayımlanmasının kolaylaşması beraberinde göz ardı edilemeyecek güvenlik problemleri getirmiştir.

Genel olarak siber saldırı veya bilgi dolandırıcılığı olarak isimlendirilen bilgi suçları Türk Ceza Kanunu' nda '' Bilişim sistemine girme'', '' Sistemi engelleme, bozma, verileri yok etme veya değiştirme'', '' Banka veya kredi kartlarının kötüye kullanılması'' olarak Bilişim Alanındaki Suçlar bölümünde yer almaktadır. Bilginin güvenliğini sağlamak adına 2001 yılında Avrupa Konseyi bünyesinde hazırlanan "Avrupa Siber Suç Sözleşmesi" imzalanmıştır. North Atlantic Treaty Organization (NATO) 'da ise Estonya'nın 2007'de maruz kaldığı saldırıdan sonra "NATO Siber Savunma Politikası" kabul edilmiş ve Lizbon'da yapılan zirve sonrası siber savunma konusunun gündemde sürekli olarak tutulması kararı alınmıştır (Budak, 2015). Türk Silahlı Kuvvetleri ise Genelkurmay Karargâhı' nda 'Siber Savunma Komutanlığı'nı 2013 yılında kurmuştur. Uluslararası topluluklar ve ülkeler bilgi güvenliği adına bu tip adımlar atarken, firmalar da kendilerince

savunma mekanizmaları geliştirmişlerdir. Önceleri bilgi güvenlik birimleri, firmalar tarafından yeterli görülürken ilerleyen zamanlarda üst yönetimden en alt düzey çalışana kadar uzanan, kurumu bütüncül olarak ele alan Bilgi Güvenliği Yönetim Sistemlerinin (BGYS) alternatifsizliği kabul görmüştür.

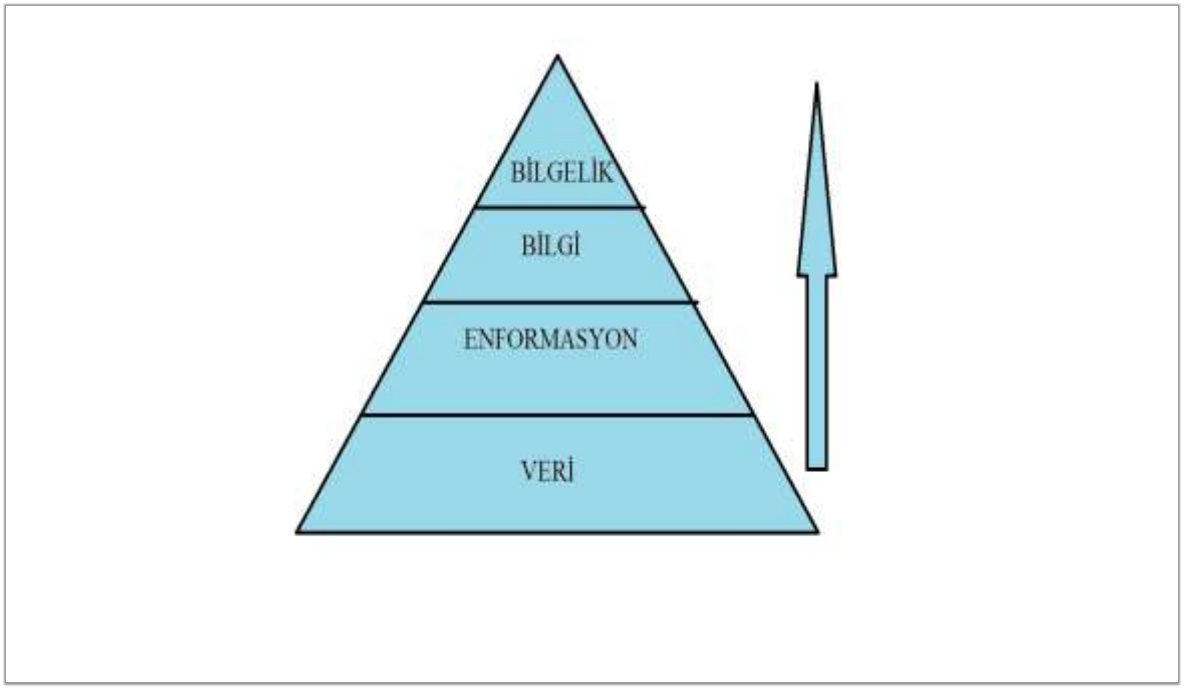
20. Yüzyılın sonlarında British Standard Institute (BSI) tarafından geliştirilen ISO 27001 BGYS standardı, uygulama ve denetleme kolaylığı açısından tekel konumunda yer almaktadır (Özbilgin ve Özlü). ISO 27001 kurumların BGYS kurması için güvenlik gereksinimlerini belirler ancak atılması gereken adımları kuruma bırakmaktadır. Türk Standartları Enstitüsü (TSE)' nin yayımlamış olduğu TS ISO/IEC 270001 adlı kitapçıkta bu standardın hazırlanış amacı; BGYS kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmak olarak açıklanmıştır (Yılmaz, 2014). ISO 27001 BGYS bilgi güvenliğinin yönetimini sağlarken sürekli gelişen ve değişen günümüz piyasasında rekabet avantajı da kazandırmayı hedeflemektedir.

1. BİLGİ VE BİLGİ GÜVENLİĞİ NEDİR?

1.1. Bilginin Oluşum Süreci

Nefes alıp verdiğimiz çağa adını vermesine rağmen bilgi kavramı üzerinde günümüz düşünür ve bilim insanlarınca bir uzlaşı sağlanamadığı gibi, geçmişten günümüze insanlığa yol gösterme çabası içerisindeki düşünürlerin ekseriyeti bu kavramı farklı ele alıp farklı değerlendirmiştir. İletişimin zaman ve mekan sınırlarını zorladığı bu dönemde, bilgiye ulaşımın maliyetinin neredeyse ortadan kalkmıştır. Ortalama bir yetişkinin sabah uyanıp hazırlanırken, evden işe giderken, öğle arasında yemek yerken işten eve dönerken, akıllı telefonunda oyun oynarken kısacası uyanık olarak geçirdiği saatlerin büyük çoğunluğunda billboardlar, afişler, TV, durak reklamları. vb. vasıtasıyla yüzlerce mesaja maruz kaldığı bu dönemde bilgi kavramını tanımlamak daha çok önem arz ekmektedir. Bilginin tanımına geçmeden önce sık sık karıştırılan veri, enformasyon, bilgelik gibi kavramların netleştirilmesi gerekmektedir.

Esasen bir kavramdan çok süreç olarak nitelendirmek bilgi kavramını özümsemek için katkı sağlayacaktır. Sürecin başlıca unsurları ise sırasıyla veri, enformasyon, bilgi, bilgeliktir. Şekil 1.1' de bu süreç resmedilmiştir.



Şekil 1.1. Bilgi hiyerarşisi

Bilginin oluşum süreci bir örnek yardımıyla anlatılmak istenirse yemeklerde servis edilen pirinç pilavı örnek verilebilir. Tedarikçiden alınan bir kamyon pirinç alınmıştır. Lakin bu pirinç hemen kullanıma hazır değildir. Zira kendi içinde baldo pirinç, dolmalık pirinç, osmancık pirinç gibi türleri barındıran ham pirinçten istenilen verimin elde edebilmesi için önce sınıflandırma yapıp kullanım alanına göre pirinçler sınıflara ayrılır. İhtiyaç duyulmayan pirinç türleri elemine edilir. Bir sonraki aşamada ise içindeki taşlar elenen pirinç kullanıma hazırdır. Son olarak pişirme işlemi sonucunda ortaya servise hazır pilav ortaya çıkar. Veri den bilgeliğe doğru bir yolculuk olan bilgi de buna benzer bir süreçten geçer. Piyasada sürekli artan bir şekilde veri yığını vardır. Bilgiye erişmek isteyen kişi önce edindiği ham veriyi sınıflara ayırmalı ardından zararlı ve gereksiz olanları ayıklamalıdır. Tüm gereksiz yanları devre dışı bırakılan gerçek bilgiyi edinen kişi onu amaçları doğrultusunda kullanabilir.

Veri**:** Türk Dil Kurumu (TDK) veriyi ‘’ Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done’’ olarak tanımlamaktadır. İngilizce ‘’Data’’ kelimesinin dilimizdeki karşılığıdır. Data kelimesi Latince “datum” kelimesinden (çoğul şekli “data” ve “vermeye cesaret etmek” fiilinin geçmiş zamanı, dolayısıyla “verilen şey”) gelmektedir. Dilimizde pratik bir şekilde ‘’verilen şey’’ anlamına gelen ‘’veri’’ kelimesinde kendine karşılık bulmuştur. (Canberk ve Sağıroğlu, Cilt: 9 Sayı: 3 , 2006). Veri çerisinde yorum barındırmaz, nesneldir ve hamdır. Semboller, sinyaller, sayılar, kelimeler veya işaretlerden oluşabilir.

Enformasyon**:** Bilgi kelimesi yerine de kullanılan[1] ‘’enformasyon’’ sözcüğü Fransızca ‘’information’’ kelimesinin Türkçedeki karşılığıdır. TDK enformasyonu danışma, tanıtma olarak tanımlamıştır. Enformasyon eldeki verilerin belirli kaideler çerçevesinde süzgeçten geçirilmesi sonucunda elde edilir. İşlenmiş veri olarak da ifade edilebilecek enformasyon, kim, ne, nerede sorularının cevabını verir. Ortak özellikleri haiz verilerin kümelenmiş hali olan enformasyon, bilginin oluşum sürecinde bir sonraki faza geçmeye hazırdır.

[1] BSTS/ İktisadi Terimleri Sözlüğü 2004

Bilgi**:** Enformasyonun önceden belirlenmiş bir hedef doğrultusunda yorumlanması ve analiz edilmesiyle ortaya çıkar. Bilgi enformasyonun doğuş noktasını irdeler ve kullanım alanlarına yönelik seçenek sunar. Enformasyon duyularımızla algıladığımız olaylar hakkında bir fikir verirken, bilgi sebep sonuç bağlamında bu olguları tartışmaktadır. Tecrübe, değerler ve öngörüden etkilenen bilgi özneldir.

Bilgelik(Hikmet)**:** Bilgi hiyerarşisinde ‘’Wisdom’’ kelimesinin karşılığıdır. Bilgi hiyerarşisinde çeşitli safhalardan geçen verinin nihai halidir. Bilgelik doğru, yanlış, ahlaki ve gayriahlaki kavramlarını içerir. Kendi değer yargılarını ve var oluşunu tanımlar. Neden sorusunu cevabını vermeye çalışan bilgelik, olay ve olguları farklı açılardan değerlendirerek bir bütün olarak ele almaya çalışır. Elde edilen bilgiyi geçmişten gelen tecrübeyle ve muhakeme, ileri görüşlülük, yorumlama gibi becerilerle harmanlayıp ortaya eldeki bilgiden tamamen bağımsız yeni bir ürün ortaya çıkarmayı amaçlar.

1.2. Bilgi Kavramı

TDK bilgiyi ‘’ öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf ’’ olarak tanımlamıştır. İnsanı insan yapan en mühim özellik düşünme yetisidir. O kadar ki Medeni Kanunun 405. Maddesine göre cezai ehliyete sahip olamama nedenlerinden birisi ‘’akıl hastalığı veya akıl zayıflığı’’ yani sağlıklı düşünme becerisidir. Her ne kadar insanın dünya ile bağlantısını göz, burun ve kulak gibi duyu organlarıyla kurduğu iddia edilse de insanoğlu gezegenimizle asıl bağlantısını duyu organlarından edindiği verileri aklıyla muhakeme ve analiz ederek kurmaktadır. Bu bağlantı sonucunda varılan yargıya ise bilgi denmektedir. Bilgi alınan mecra nesne ise bilgiyi alan öznedir. Bu bağlamda bilgi özne ile nesne arasındaki ilişkiden peydahlanmaktadır. Ekonomik olarak ele alınırsa bilgi, ekonominin 3 sacayağı olan emek, sermaye ve müteşebbisi doğrudan etkilemekte hatta 4. faktör olarak adlandırılabilmektedir. Asya’ da üretilen bir ürünün kargo masrafı olmadan son tüketici tarafından satın alınabildiği klişe tabirle küresel bir köy haline gelen günümüz dünyasının rekabet ortamında bilginin dengeler üzerindeki etkisi dikkate şayandır. Peter Drucker’ a göre bilgi kavramı son 250 yılda değişime uğramakla kalmamış toplumu ve ekonomiyi de beraberinde değiştirmiştir. Günümüzde ise değer ifade eden tek kaynak haline gelmiştir. Drucker ayrıca 1980 yılından sonra dünyanın aldığı durumu ve bilginin ekonomi üzerindeki iktidarını ‘’ enformasyon kapitalizmi’’ olarak ifade etmektedir. (Bingöl, 2010)

Sokrates “İyi olan tek şey bilgi, kötü olan tek şey bilgisizliktir” demiştir. Farabi ise “Erdemlerin en büyüğü bilimdir, bilgeliktir. Bilgi uçsuz bucaksız ve kıyısız bir denizdir. Doğru bilgi insanca yaşamanın temelidir” diyerek bilginin önemine vurgu yapmıştır (Atılgan, 2009).

Günümüz düşünce insanlarının görüşlerine yer verilmek istenirse (Enginoğlu, 2013);

Mark Allen’ a göre bilgi; ‘’Spesifik gerçekler, prosedürler ve birey ya da işletmenin sahip olabileceği, tipik olarak öğrenmenin sağladığı değişim süreci sonunda elde edilen becerileri ifade eder’’.

Baker’a göre bilgi; ‘’Fikirlerde, kararlarda, yeteneklerde, ilişkilerde, bakış açılarında ve görüşlerde ortaya çıkar. Bilgi; müşteriler, ürünler, süreçler, kültür, beceriler, deneyimler ve know-how ile ilgili olabilir’’.

Joy Liebowitz ve Wilcox Lyle’ a göre bilgi; ‘’Doğruları ve gerçekleri göz önünde tutan ve bu nedenle insanların düşüncelerine, davranışlarına ve ilişkilerine yol gösteren, anlayışlar, deneyimler ve yöntemler bütünüdür’’.

Peter Senge’ e göre bilgi; ‘’Enformasyondan farklıdır, etkili hareket edebilme kapasitesidir ve satın alınamaz’’.

Amrit Tiwana’ ya göre bilgi; ‘’Yeni deneyimleri ve enformasyonu değerlendirmek, içselleştirmek için bir ortam ve çevre sağlayan, tecrübe, değerler, sözel enformasyon, uzmanlık kavrayışının bir karışımıdır. Bilenlerin zihinlerinde doğar ve yine orada uygulanır. Kuruluşlarda bilgi, çoğu kez yalnızca belgelerde ya da sır gibi saklanan evraklarda değil, organizasyonun günlük işleyişinde, süreçlerde, pratiklerde ve normlarda gizlidir’’.

Bu görüşler ışığında basit bir tanım yapılmaya çalışılırsa; gözlem, araştırma ve öğrenme vasıtalarıyla elde edilen şeylerin deneyim ve zihin değirmeninden geçerek aksiyon aldıran bir olgu haline gelmesine bilgi denir.

Bireysel açıdan bilgi; insanın herhangi bir vasıta ile edindiği verilerin tecrübeleriyle alaşımıdır. İnsanlar arası iletişimle ortaya çıkan enformasyon aklın süzgecinden geçerek bilgiyi meydana getirir. Tecrübe, yargı, değerler, inançlar ve sezgi; bilginin bileşenlerini oluşturmaktadır.

Organizasyonlar için ise bilgi; ürünler, diğer firmalar, demografik ve çevresel faktörler, ekonomik değerler hakkında elde edilen enformasyondu. Ele geçen enformasyonun uzmanlarca uzun ve kısa vadeli planlama amacıyla kullanılması ve organizasyona bir yol haritası çıkarılması ise bilgiyi ortaya çıkarmaktadır. Bu perspektife göre organizasyonlar için bilgi:

- Verimli karar almada,
- Geleceğe yönelik tahminlerde bulunmada,
- İletişim kalitesinin yüksek tutulmasında,
- Ürün/hizmet standardizasyonunun gerçekleştirilmesinde,
- Hâlihazırda karşılaşılan veya gelecekte karşılaşılabilecek olay ve problemlere kalıcı çözüm üretilmesinde; kullanılan bir araçtır (Atılgan, 2009).

Literatürde yaygın kullanılan ve izah edilmesinde fayda görülen bilgi sınıflandırmalarından biri açık bilgi ve örtülü bilgi sınıflandırmasıdır.

Örtülü Bilgi**:** Bilgi sahibi kimsenin bilgiyi karşı tarafa aktarmakta güçlük çektiği bilgidir. Bilgi hakkında ve bilgiyi oluşturan unsurlar hakkında birçok şey bilinmesine rağmen kelimelere dökülemeyebilir. Yahut kelimelerle ifade edilse bile tam olarak ifade edilemez ve bilgi aktarılmak istenen tarafa transfer gerçekleşemez. Deneyime dayanan bir bilgidir, kişiseldir. Örnek vermek gerekirse 80 yaşında bir babaanneye yemek tarifi sorulduğunda ‘’göz kararı salça’’ veya ‘’bir tutam kekik’’ gibi tabirler kullanacaktır. İşte uzun bir tecrübi birikime dayanan ve ancak ‘’göz kararı’’ olarak dış dünyaya yansıması bulunan bilgi türüne örtülü bilgi yahut örtük bilgi denir.

Açık Bilgi**:** Rakamlarla ifade edilebilen bu sayede karşı tarafa aktarımında sorun yaşanmayan bilgidir. Deneylerle doğruluğu ispatlanabilir bilgi türüdür. Örneğin; çemberin çevresinin yarıçapına oranı 3,14 tür. Açık bilgi belirli bir formül düzenine sokulabilir,

bilimseldir. Ulaşılması, saklanması, dokümante edilmesi ve dolayısıyla arzu edilen tarafa iletilmesi oldukça zahmetsizdir.

Herhangi bir bilginin değer taşıyabilmesi için aşağıdaki niteliklere sahip olması gerekmektedir (Enginoğlu, 2013):

- Doğruluk: Bilgilerin doğru olması hem itibar açısından hem de alınacak aksiyonun geri dönülemeyecek etki ve maliyetlerinden kaçınmak için elzemdir. Lakin her ulaştığımız bilginin yüzde 100 doğru olma ihtimali düşüktür.
- İlgililik: Konu ile elde edilen bilgi arasında ilgi olması gerekmektedir. Aksi takdirde bilgi edinme maliyeti zarar hanesindeki yerini alacaktır.
- Tamlık: Bilginin amaca verimli hizmet edebilmesi için eksiksiz olması gerekmektedir. Uzun mesafeli hedef alan bir okçu nişan alırken 1 cm yanlış hedef aldığında okun isabet noktası metrelerce değişeceği gibi eksik bilgiyle yola çıkan bir işletme varoluş amacına doğru hareket ettiğinde amacından telafi edilemeyecek düzeyde sapma yaşayabilir
- Doğru Zamanlılık: Bilginin önem arz eden özelliklerinden birisi de doğru zamanda elde edilmesidir. Menkul kıymet piyasalarındaki herhangi bir değişimin aynı anda tüm dünya izlenebildiği günümüz ekonomi konjonktüründe geç elde edilen bir bilgi büyük zararlara neden olabilmektedir.
- Ulaşılabilirlik: Arzu edilen bilgiye ulaşım hem maliyet açısından hem de zaman açısından en uygun olmalıdır.
- Etkin Maliyet: Bilgiyi elde etmek için sarf edilen tutar o bilgi kullanılarak kazanılan getiriyi aşıyorsa orada etkin bir maliyet söz konusu olamaz. Maliyet etkinliği olmayan getirinin de hiçbir değeri yoktur

İster uluslararası arenada sahip olduğu bilgiler ışığında pozisyon alan devletler ele alınsın ister firma değeri kimi devletlerin GSMH' sini aşabilen ve hatalı karar aldığında kaybı milyonları bulan firmalar ele alınsın bilginin değeri ve önemi su götürmez bir gerçektir. Birey perspektifinden bakıldığında ise yegâne sermayesi olan hayatına yön veren kararları edindiği bilgilerle alır. Bu bağlamda bilgiye atfedilen önem arttıkça onun muhafazasına olan önem de o şiddette artmaktadır.

1.3. Bilgi Güvenliği Kavramı

Bilgi güvenliği insanoğlunun gündemine yeni giren bir konu değildir. Bilginin sağlıklı bir şekilde saklanması ve güvenliğinin sağlanması insanlığın Milattan önceki dönemlerden beri endişe kaynağıdır. Hatta yazının keşfi Mezopotamyalı tüccarların ticari bilgilerin saklanması gerektiğini düşünmesi üzerine gerçekleşmiştir (Rossi, 2009). Yazıdan önce şifahen iletilen bilginin güvenliği sağlamak bireye endeksliydi. Bilgiye ulaşmak isteyen şahsın veya devletin tek hedefi bireyden herhangi bir şekilde bilgiyi edinmekti. Saklanılması gereken bilgi rüşvetle, ödülle yahut işkenceyle elde edilebiliyordu. Ancak yazıya dökülen bilgi bireyden bağımsız bir sorun teşkil etmeye başlamıştır. Yazılı bilginin güvenliği kimi zaman şifreli mesajlar kullanılarak sağlanmaya çalışılmış kimi zaman görünmez mürekkep bu konu için tercih sebebi olmuştur. Ancak bilgi transferinin bilgisayar ağları üzerinden sağlandığı dönemde bilgi güvenliğinin sağlanması için alınan tedbirler tamamen sınıf atlamıştır.

Küresel çapta bir ağ bağlantısı olarak kabul edilen internet kendine tam anlamıyla 7' den 70' e bir kullanıcı kitlesi bulmuştur. Günümüzde bir anne çocuğunun okul ihtiyaçlarını internetten sipariş ederken uluslararası bir kurum ihracat işlerini yine internet üzerinden yürütmektedir. İnternet bankacılığı, sosyal medya, uzaktan eğitim internetin kullanım alanlarından sadece birkaçıdır. Kullanım alanlarının bu kadar çeşitlenmesi bireylerin ve kurumların bilgilerinin de ulaşılabilirliğini o ölçüde artırmaktadır.

Bilgi güvenliği kavramı üzerine literatürde pek çok tanımlama yer almaktadır;

Michael E. Whitman ve Herbert Mattord' a göre bilgi güvenliği '' Bilgiyi kullanan, ileten ve saklayan kritik elemanların korunmasıdır" (Boşal, 2017).

Bilgi güvenliğinin diğer bir tanımı Solms' a aittir. Solms bilgi güvenliğini "Kurumsal teknolojilerin bilginin üç temel özelliği olan gizlilik, bütünlük ve erişilebilirliğin sebebiyet verdiği riskleri azaltarak düzenlemesidir" şeklinde tanımlamıştır. (Boşal, 2017).

Bilgi güvenliği, elektronik ortamlarda yer alan bilgilerin muhafazası ve iletilmesi sırasında bütünlüğü bozulmadan, izinsiz erişimlere yer vermemek adına, güvenli bir bilgi

işleme platformu meydana getirme çalışmalarına verilen isimdir. (Allahverdi ve Alagöz, 2011-3).

Bilgi güvenliği, kurumların sahibi olduğu varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini tehdit eden risklerin ortaya konup, bu konuda risk yönetimi adına alınması gereken aksiyon alınmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olasılık değerine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir:

- Riskin azaltılması,
- Riskin kabul edilmesi,
- Bütün halinde üçüncü bir tarafa devredilmesi (sigorta etmek gibi),
- Risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir (Kandemirli, 2012).

Gizlilik, bütünlük ve erişilebilirlik biri olmadan diğerinin çok ehemmiyeti kalmayan, birbirleriyle iç içe geçmiş 3 temel unsurdur. Bu 3 temel unsur bilgi güvenliğinin oluşumunu ve sürekliliğini sağlar. Bu unsurların detaylı incelenmesi bilgi güvenliğinin kavramının yerleşmesi açısından önem taşımaktadır.

Gizlilik, bilginin sadece erişmesi zorunlu olan kişi ve kişiler tarafından erişilmesidir. Erişmesi izin verilmeyen hiç kimse bilgiye erişmemelidir. Bilginin gizliliği gerek kişisel gerekse kurumsal açıdan en çok üstünde durulan özelliktir. Aynı zamanda saldırganların da en çok elemine etmek istediği özellik bilginin gizliliğidir. Türkiye'de bu özelliğin önemine binaen yasama organı Kişisel Verilerin Korunması Kanunu'nu yürürlüğe koymuş, bilgi gizliliğinin önemine verdiği değeri sergilemiştir.

Bütünlük, oluşum sürecinden geçip nihai haline eren bilginin arzu edilmeyen bir değişime uğramadan sürekli bir şekilde muhafaza edilmesi, kendine has yapısını garanti altına alınmasıdır. Bilginin az da olsa bozulması veya değiştirilmesi bütünlüğünün sağlanamadığına delalettir. Bütünlüğü sağlanamayan bilgi istenmeyen sonuçlara mahal verir. İstenmeyen sonuçlar ise hem kurumsal hem bireysel bazda zarara sebep olabilir. Bu yüzden bilginin asıl halinin muhafazası mühimdir.

Erişilebilirlik, bilgiye erişmesine izin verilen kişi ve kişilerin erişmek istediği anda bilgiyi elde etmesidir. İstenilen bilgiye istenilen anda ulaşılamazsa bilginin erişilebilirliği zarar görmüş olur. Kurumsal bazda iş sürekliliğinin sağlanması erişilebilirlik seviyesine bağlıdır. (Boşal, 2017).

Bu üç temel unsurdan herhangi birinde yaşanan aksaklık bir diğerine sirayet etmekte olduğu gibi herhangi birinde seviyeyi yukarı çekerken diğer bir unsurun görevini yerine getirmesine de engel olunabilir. Bilginin gizliliğinin muhafaza edilmesi o bilginin erişilebilirliğine halel vermemelidir. Aynı zamanda erişilebilen bilginin bütünlüğünün de ihmal edilmemesi gerekmektedir. Gizliliği üst seviyede sağlanan bilginin erişilebilirliği aksadığı zaman kullanılamayan bilgi bir değer ifade etmeyecektir. Yine aynı şekilde erişimi sağlanan bilginin bütünlük yönünden bir noksanlığı mevcut ise eksik bilgi edinen birey ve kurum yanlış aksiyon alacak ve maddi manevi zarara sebep olabilecektir. Bu bağlamda bu üç temel yapıtaşı birbirinden bağımsız değerlendirildiğinde aksaklıkların yaşanması kaçınılmazdır. (Doğantimur, 2009).

1.3.1. Bilgi güvenliğinin sağlanması için temel prensipler

Bilgi güvenliğini sağlamak için pek çok güvenlik unsurunun birlikte yürütmek gerekmektedir. Bilginin güvenliği için gereksinim duyulan araçlar kurumun yaptığı işe göre, kapasitesine göre farklılık gösterebilir ancak genel bir yol haritası çizmek için bir takım temel prensipler sıralanabilir (Boşal, 2017).

<u>En az yetki</u>

Tüm departmanlarda, sistemlerde ve ağlarda kullanıcı hesabı yahut rolüne yetki verilirken sadece ilgili alanda işlem yapılabilecek seviyede yetki verilmesi önemlidir. Bu yetkilerin dışında kalan hiçbir alan üzerinde işlem yapmaya mahal verilmemesi gerekmektedir.

<u>İzinsiz her şey yasak</u>

Sistemde gereksiz yetki verilmemesi adına kullanıcı hesabına ya da rolüne sadece kendine müsaade edilen alanlarda işlem yapabilir halde olması ehemmiyeti yüksek bir

unsurdur. Bu yüzden yetki verilirken göz ardı edilmemesi gereken husus, tüm personel için ön tanımlı değerin her şeyi yasakla yaklaşımıyla tanımlanması gerekir.

Görevler ayrılığı

Bir iş yapılırken görevi üstlenen, aksiyon alan kişi ile onay merciinin farklı olması gerekmektedir. Zira işi yapan kişi onay yetkisine sahip olursa suiistimal ve kaytarma yaşanabilir. Böylece hem bilgi sahibi kişi ortaya konmuş olur hem de sorumlulukların ayrımı gerçekleşmiş olur.

Kullanılmayanların çıkarımı

Yaşamın her alanında olduğu gibi bilgi güvenliğinin sağlanmasında da sadelik yani gereksiz unsurların ortadan kaldırılması zaman ve mekan açısından verimlilik sağlar. Yaşanabilecek zafiyet anında ortaya sahip olmaya dair risklerin en aza indirilmesine katkıda bulunur. Uygulamalarda da kullanılmayan menülerin, ekranların, tuşların kaldırılması hareket kabiliyetini artırırken yapılan işlemin daha efektif hale gelmesini sağlar.

Kullanılabilirlik-güvenlik dengesi

Sistemlerin kullanılabilirliğinin ve işlem hacminin artması zafiyet yaşama olasılığını artırabilmektedir. Saldırılar tercih edilen ekranlar, kullanıcının daha çok ziyaret ettiği ekranlar olmaktadır. Bu yüzden üzerinde daha çok işlem yapılan sistemlerin güvenliği üzerine eğilmek gerekmektedir.

Bilgi güvenliğini sadece internet eksenli düşünmek hatalı olabilir. Çünkü bilgi bugün bir kurum bünyesinde çok farklı formlarda kendine yer bulabilmektedir. Bir dosya içerisinde veyahut bir telefon görüşmesinde kıymetli bir bilgi yer alabilirken; kurumların özel sistem odaları kayıt görüntüleri veya depolarında yer alan malzeme bilgileri o kurum için büyük önem taşıyabilmektedir. Dolaysıyla bilgi güvenliği sadece bilgi sistemlerinin güvenliği olarak ele alamamak gerekmektedir. Bilgi güvenliği bir bütün olarak ele alınmalı kurumun bütün bölümlerini kapsamalıdır. Herhangi bir bölümde yaşanacak güvenlik zafiyeti tüm kurumu etkileyebilmektedir (Allahverdi ve Alagöz, 2011-3).

1.3.2. Bilgi güvenliği farkındalığı

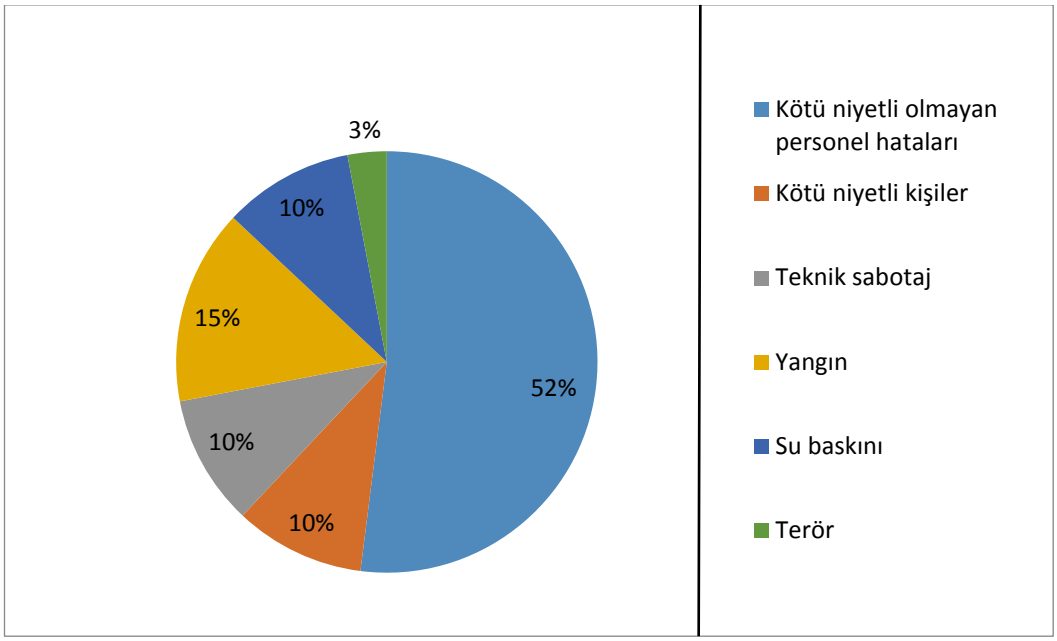
Herhangi bir kuruma, topluluğa hatta ülkeye bir yeni sistem entegre edilmeye çalışıldığı zaman genellikle o konuyla ilgili prosedürler, ilkeler, kanunlar ortaya çıkarılır eksikler varsa hazırlanır gerekirse profesyonel destek alınır. O branşa dair sertifikalar, belgeler alınır. Derneklere, vakıflara varsa ulusal, uluslararası cemiyetlere, topluluklara üye olunur. Edinilen bu ilkeler ve prosedürler duvarlara asılır, mail olarak atılır, gerekli duyurum yapılmaya çalışılır ancak entegre edilmek istenen sistem hakkında topyekûn bir farkındalık kazanılamadığı zaman yapılan bu çalışmalar enerji ve kaynak israfından öteye gidemez.

Bilgi güvenliği insan faktörü, teknoloji, eğitim gibi birçok etmen bir arada değerlendirilip gerekli tedbirlerin alındığı ve denetimler sağlandığı zaman ayakta tutulabilir. Kurumun her bir çalışanın katkısı ve katılımı olmadan bir daire veya departmanın gayretiyle bilgi güvenliğinde başarı sağlanamaz. Kurum kültüründe kökten bir değişim gerektirdiğinden ötürü öncelikle ve özellikle üst yönetimin onayı, katılımı ve desteği şarttır. Zira personel her daim üst yönetimi bu anlamda takip eder. Uyulması gereken bir kurala üst yönetim uymadığı zaman personelin her zaman kuraldan kaytarmak için hazır bir nedeni vardır. Dilimizde yaygın olarak kullanılan ‘’ Balık baştan kokar’’ atasözü bu anlamı ihtiva etmektedir. Bu sebepten bilgi güvenliği sistemini üst yönetimin her anlamda desteklemesi ve öncelikle kendisinin tatbik etmesi gerekmektedir. Bilgi güvenliğini emniyet kemerine benzetirsek; emniyet kemerini ilk önce sürücünün takması gerekir.

Kurumca saptanan güvenlik çözümleri, politika ve prosedürler kurum kültürüne yansıtılmadığı takdirde umulan etkiyi sağlayamayacaktır. Gerekli farkındalık sağlanmazsa çalışanlar şifrelerini korumakta dikkatsiz, hassas bölgelerde gördükleri yabancı kimselere karşı umursamaz, kâğıt çöpüne attıkları dokümanların imhasına özen göstermedikleri anda kurumun karşılaşabileceği tehditlerden bihaber olabileceklerdir. Bu durum yapılan yatırımların güvenliğe hiçbir katkı sağlamamasına neden olmakla kalmayıp mevcut zafiyetlerin güçlenerek varlıklarını devam ettirmesini sağlayacaktır (Şen ve Yerlikaya, 2013).

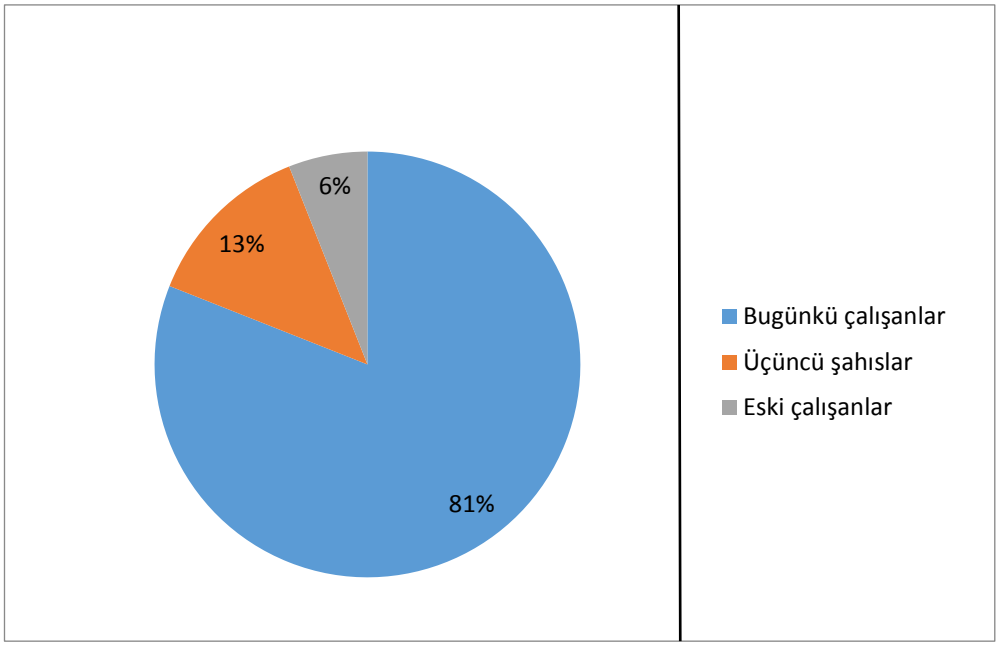
Bir kuruma bilgi güvenliğinin sağlanması için yazılımsal ve donanımsal önlemler insan faktörü göz ardı edildiğinde her zaman eksik kalmaktadır. Bilgi güvenliğinde en zayıf halka olarak addedilen insan faktörü güçlü sistemlere nazaran çok daha kolay atlatılabilir. Art niyetli kişiler sürekli testleri yinelenen sistemleri aşmak yerine kullanıcı rolünü üstlenen insan faktörünü hedef olarak belirlediğinde çok daha kolay netice alabilmektedir. Ulusal siber güvenlik tatbikatı sonuç raporuna göre (Usgt, 2011); Türkiye de kurumların yaşanan güvenlik olaylarına karşı yalnızca teknik önlemler aldıkları, güvenlik zincirinin en kritik halkası olan insanı göz ardı ettiği tespit edilmiştir. Raporda ayrıca kurumların çalışanlarına sosyal mühendislik saldırılarına karşı farkındalık eğitimlerini düzenli hale getirmedikleri, bu tip saldırıları engellemek amacıyla e-posta göndermek veya bilgilendirme afişleri vasıtasıyla bilgi güvenliği farkındalığı oluşturmaya yönelik tedbirlerin alınmadığına yer verilmiştir. Kısaca insanlara gerçek hayatta tanımadıkları bir başkası için asla yapmayacakları iş ve işlemleri yaptırtma eylemi olarak tanımlanan sosyal mühendislik, ekseriyetle ikna ve etkileme metotları kullanılarak icra edilir. Sıradan bir e- mail veya kısa mesaj olarak hedefine ulaşan art niyetli kişi ve kişiler kurum içinden veya dışından olabilir. Tek bir kullanıcının gafletinden ötürü açığa çıkan bilgi kurumu derinden sarsan mali zarara neden olabilirken piyasadaki güvenilirliğini ve itibarını zedeleyerek manevi hasara da neden olabilmektedir.

Bir araştırma şirketince gerçekleştiren bir araştırma yapılan saldırıların kimler tarafından icra edildiğini ortaya koymaktadır. Bilgi güvenliği farkındalığı gelişmediği takdirde kurumların yaşayacağı zafiyetleri gözler önüne seren araştırmaya göre kurumların saldırılardaki en yumuşak karnı kendi çalışanıdır. Şekil 1.2’ de bu konu hakkında hazırlanan bir grafik gösterilmiştir.



Şekil 1.2. Güvenlik saldırılarının nedenleri (Kandemirli, 2012)

Aynı raporda yer alan bir başka konu ise saldırganlar kimliği hakkında daha detaylı bilgi vermektedir. Bilgi güvenliğine dair işlenen suçlarının ana müsebbibinin işletmenin cari personeli olduğu iddia eden rapor bilgi güvenliğinde asıl yatırım yapılması gereken unsurun altını çizmektedir. Bir ordunun Görevini başarıyla yerine getirmesi için modern teçhizat ve donanıma sahip olması gerekir. Başarılı bir ordu için en az bu kadar önemli bir unsur da mühimmatın güvenliğinin sağlanmasıdır. Aynı şekilde firma da mühimmatını yani en mühim varlığı olan bilgi varlıklarını muhafaza eden personeli gerektiği şekilde eğitmez ve bu bağlamda onlara farkındalık kazandırmazsa saldırılardan kaçınamayacaktır. Şekil 1.3' de ki grafik anlatılanları destekler niteliktedir.



Şekil 1.3. Güvenlik saldırılarını gerçekleştirenler (Kandemirli, 2012)

Görüldüğü üzere bilgi güvenliğini sağlamak adına yazılım ve donanım tedbirleri eksik kalmakta, kurumlarda çalışan personele güvenlik bilincinin aşılanması gerekmektedir. Güvenlik farkındalığını yerleştirmek için ilk hamle uygulanabilir, sürekli güncellenen ve konjonktüre uyumlu prosedürlerin yönetim tarafından hazırlanması, uygulanması ve takibidir. Farkındalık hususunda aslan payı yönetime düşmektedir. Balık baştan kokar misali yönetim farkındalık konusunda gerekli dikkati göstermez ya da gösterdiği dikkati kurum geneline aksettirmezse farkındalık konusunda gerekli ilerlemeyi kat edemeyecektir. Yönetim kendi belirlediği veya ithal ettiği prosedürlere, standartlara, mevzuata en alt düzeydeki personeline kadar uyum sağlanmasını talep ediyorsa öncelikle kendisi bu kuralları uygulamaya ve çalışma hayatının temel prensipleri haline getirmeye gayret göstermelidir. Aksi takdirde kurum geneli bir farkındalık bilinci oluşmasını beklemesi yerinde bir davranış olmaz.

İkinci olarak personel seçiminden başlayan ve düzenli eğitimiyle devam eden bir süreç söz konusudur. Personel alırken ki şartnamede güvenlik sorumluluklarının yer alması gerekirse bu sebepten eleme yapılması, hali hazırda çalışan personel için sorumluluklar arasına bilgi güvenliğine dair maddelerin eklenmesi, yeni başlayan personel için gizlilik veya kapalılık anlaşmaları imzalatılması gibi önlemler alınmalıdır. Bunun yanı sıra kurumun bütün çalışanları ve hatta üçüncü taraf kullanıcılar organizasyona dair prosedür ve politikalarla ilgili doğru seviyede eğitim ve düzenli güncelleme almalıdırlar. Bu

eğitimlerin içeriğinde güvenlik gereklilikleri, olası saldırı senaryoları ve tehdit unsurları, yasal sorumlulukları, iş denetimleri, oturuma giriş yöntemlerine ek olarak yazılım paketlerinin kullanımı gibi bilgi işleme araçlarının doğru kullanımı bilgileri yer almalıdır. Eğitim verilmesi gereken bir başka alan ise sosyal medya kullanımı olmalıdır. Kurum içinde neredeyse her personelin kullandığı sosyal medya araçlarının hatalı kullanımı sonucu kullanıcı bilgileri ele geçirilebilmektedir. Birçok saldırgan bu bilgileri kullanarak kurumlara ciddi saldırılar düzenlemektedir.

Son olarak değinilmesi gereken nokta ise zaman tanıma konusudur. Yıllar içinde kazanılan kültürün oluşması belirli bir zamana, maliyete ve emeğe mal olduğu gibi yeni bir kültür oluşturmak, bir kuruma genel bir farkındalık kazandırmak, eski alışkanlıkları terk etmek de zaman tanınması gereken bir süreçtir. Bu süreçte de başrol yine üst yönetime düşmektedir. Uyulması gereken kuralları beyan edip gerisini personel inisiyatifine bırakmak, geri bildirimlerin takibini yapmamak ve bu kısa süreç sonunda bilgi güvenliği kültürünün oluşmasının beklemek yönetimde yeterli farkındalığın oluşmadığını göstermektedir. Gerçeğe yakın tatbikatlarla belki ödüllendirmelerle personelin sürekli teşvik edilmesi ve farkındalığın oluşması adına tekrar tekrar güvenlik gerekliliklerinin altının çizilmesi gerekmektedir. (Sagıroğlu, Ersoy, ve Alkan, 2007)

Kurumların veya devletlerin bilgi güvenliğini bir bütün olarak ele almadığı veya belirli ilkeler üzerine bina etmediği zaman ortaya çıkan neticelerin kimi zaman telafisi mümkün olmayabilmektedir. Yaşanan vakalardan birkaç örnek vermek gerekirse aşağıdaki örnekler sıralanabilir.

1.3.3. Güncel bilgi güvenliği vakaları

Bilgininin piyasalara yön verme gücü arttıkça onu elde etmek için harcanan çaba da doğru orantılı olarak artmıştır ve artmaya devam edecektir. Dünya Ekonomik Forumun (WEF) yayımladığı bir rapora göre siber suçların dünya ekonomisine etkisi 445 milyar $' dır (WEF, 2016). Bu rakamın 2021 yılında 6 trilyon $ olacağı tahmin edilmektedir. 2017-2021 arasında dünya genelinde bilgi güvenliği için harcanacak tutarın 1 trilyon $ olacağı öngörülmektedir (Cybersecurity Ventures, 2016).

Twitter, SoundCloud, Spotify saldırısı

Türkiye' nin de içinde yer aldığı birçok ülkede 21 Ekim 2016 da çeşitli internet site ve servislerinde erişim aksaklıkları gözlemlendi. Twitter, SoundCloud, Spotify ve Shopify gibi popüler site ve servislerde gözlemlenen yavaşlık veya erişilememe aksaklıkların ABD merkezli DYN adında DNS firmasına yapılan DDoS saldırıları sonucunda gerçekleştiği ortaya çıktı. Dyn DNS, ziyaretçi sayısı göz dolduran birçok web sitesi tarafından tercih edilen bir servis. Bu tür siteler arasında yukarıda sayılanlar dışında SaneBox, Reddit, Box, GitHub, Zoho CRM, PayPal, Airbnb, Freshbooks, Pinterest, Heroku ve Vox Media gibi diğer önemli hizmetler de bulunuyor. (STM, 2016)

Yahoo saldırısı

ABD'nin teknoloji devlerinden Yahoo, 2013 yılında gerçekleşen bir siber saldırıda takriben 1 milyar kullanıcısının hesap bilgilerinin çalındığını duyurdu. Müşterilerin gizli bilgileri, iletişim bilgileri, doğum tarihleri çalınırken finansal bilgilerin zarar görmediği bildirildi. Yine 2014 yılında yaşadığı bir saldırıda Yahoo 500 milyon kullanıcısının bilgilerinin ele geçirildiğini duyurmuştu (STM, 2016).

ABD İle Rusya Arasında Siber Saldırı Krizi

2016 yılındaki ABD başkanlık seçimlerine yönelik siber saldırının arkasında Rus siber korsanlarının olduğu iddiası iki ülke arasında diplomatik krize sebep oldu. ABD yönetimi başkan adaylarından Hillary Clinton' ın seçim kampanyasına yapılan saldırıyı gerçekleştiren siber korsanların ardında Rusya'nın olduğunu iddia etti. Hillary Clinton'un seçim ekibinin e-postlarının sızdırılmasına sebep olan siber saldırının, Cumhuriyetçi aday Donald Trump' ın seçim zaferine katkı sağladığını iddia eden ABD istihbaratına göre saldırının arkasında, Rusya devletine bağlı bilgisayar korsanlarının olduğuna dair sağlam kanıtlar mevcut. Rusya yönetimi ise suçlamaları kabul etmiyor.

ABD siber korsanlık yoluyla başkanlık seçimlerinin etkilendiği iddiaları nedeniyle Rusya devleti adına çalışan 35 diplomatı sınır dışı etme kararı aldı. ABD Dışişleri Bakanlığı söz konusu diplomatların ''statülerine uygun olmayan faaliyetler'' e dâhil olduklarını duyurdu. Washington yönetimi yaşanan süreçte karşılık olarak Maryland ve

New York’ da istihbarat amacıyla kurulan Rus merkezlerinin kapatılacağını bildirdi (STM, 2016).

WannaCry saldırısı

Uluslararası çapta yaşanan en büyük yazılım saldırısı geçtiğimiz dönemde meydana geldi. Dünyada 100’ den fazla ülke ve 200 bine yakın sistem 12 Mayıs 2017 tarihinde “WannaCry’’ adında zararlı yazılımın saldırısına maruz kaldı. En ağır hasarı bine yakın bilgisayarı saldırıya uğrayan Rusya İçişleri Bakanlığının aldığı siber saldırıdan çoğunlukla kurumlar etkilendi. İngiltere’nin sağlık sistemi tamamen çöktü. Yapılan değerlendirmeler ise saldırının arkasında Kuzey Kore’nin yer aldığı yönünde yoğunlaşıyor.

Yaşanan bu olaylar, siber saldırıların ülkeleri ve kurumları telafisi mümkün olmayan zararlara ve maddi kayıplara yol açabileceğini bir kez daha gözler önüne seriyor. Türkiye dünya da en çok siber saldırıya maruz kalan ülkeler arasında 9. Sırada yer almaktadır (STM, 2015). Gerek dünya da gerek Türkiye’ deki gelişmeler ve saldırılar göz önünde bulundurulduğunda, sürekli kendini yenileyen bir bilgi güvenliği sisteminin üst yönetimi de kapsamak kaydıyla tüm yönetime nüfuz etmesi artık bir zorunluluk haline gelmiştir.

2. RİSK YÖNETİMİ VE KAVRAMLAR

Modern çağda insanların; insanlar gibi güçlü, zayıf, başarılı ve başarısız tarafları bulunan kurumların; büyük kurumlar gibi yönetilen, finansmanı ve pazarlaması yapılan devletlerin hayatında önemli bir yer kaplayan bilişim teknolojileri ekonomik ve sosyal alışverişin vazgeçilmez araçları olmuştur.

Tüketici tatminini sağlayan, sürekli kendini yenileyen ve güvenilir hizmetlerin sağlanması için amaca yönelik hedeflerin belirlenmesi ve bu hedeflere göre de süreçlerin doğru yönetilmesi gerekmektedir. Kurumların uzun vadeli planlarında başarıya ulaşması için bilgi yönetimi konusunda yetkinliğe olması gerekmektedir. O yüzden kurumlarda bilgi işlem sistemleri ve bilgi işlem çalışanlarının ehemmiyeti hat safhadadır. Kurumların bilgi işlem konusunda gerekli seviyeye ulaşması için sürekliliğini sekteye uğratabilecek, hizmetlerini aksatabilecek ve itibarını leke sürebilecek faktörlerin tespit edilmesi ve en aza indirilmesi gerekmektedir. Bu hayati ihtiyacı karşılamak için ‘’Risk Yönetimi’’ kavramı ortaya çıkmıştır (Kahraman, 2006).

Risk yönetimi kavramını etraflıca kavrayabilmek için risk yönetiminin genel yapısının ve unsurlarının tetkiki ve BGYS ile ilişkisinin ortaya konması gerekmektedir. Bu sebepten ötürü risk yönetim modeli incelenmeden önce risk yönetiminin genel yapısı, kavramları ve BGYS ile ilişkisi açıklanmalıdır.

2.1. Risk Yönetiminin Konusu

Riskin konusu üzerine örnek verilmeye çalışıldığında çok zorlanılmayacağı aşikârdır. Zira hayatın riskten arındırılmış herhangi bir mekânı yahut zaman dilimi yoktur. Çok basit bir hafta sonu tatili dahi fazlasıyla risk barındıran bir eylemdir. Otobüsle yolculuk zaman kaybı olabilir. Hava yolu tercih edildiğinde ise seyahat için ayrılan bütçe yetersiz kalabilir. Özel araçla gidildiğinde ise fiziksel yorgunluk sebebiyle tatilden verim alamama durumu ortaya çıkabilir. Elbette hava durumu, kat edilecek mesafe, yolun düz veya engebeli oluşu yine karar mekanizması üzerinde söz sahibi olan unsurlardır. Bütün unsurlar göz önüne alınıp hangi tercihin hangi riskleri barındırdığı ortaya konulduğunda karar almak kolaylaşır. Örnekte otobüs yolculuğu hava şartlarına, yol durumuna göre güvenlik riski barındırmaktadır. Uçak yolculuğu ise mali risk barındırmaktadır. Bütün

alternatifleri ve içerdikleri riskleri değerlendiren karar merci kendi değer yargılarına göre seçimimi yapmak durumundadır.

Kurumlarda uzun vadeli başarı için dikkat edilmesi gereken hususların başında zafiyet yaşanabilecek alanları tespit edip, zafiyet yaşanmadan önlem almasıdır. Yani reaktif değil proaktif bir hareket tarzının benimsenmesidir. Hasta olduktan sonra ilaç almak yerine hasta olmayacak bir yaşam ve beslenme tarzı geliştirmeye benzetilebilir. Kışın hava şartları, salgınlar, kişinin yaşam koşulları ..vb. durumlar nedeniyle hasta olma ihtimalinin arttığı iddia edilebilir. Hasta olduktan sonra hem sağlık hizmetleri hem ilaç maliyetine katlanılır. Hem de iş veya eğitimden belli bir süre uzak kalınıp adaptasyon sorunları yaşanabilir. Bunun yerine sağlık yaşamaya ve beslenmeye özen gösterilerek; doğru yerde doğru kıyafetler giyilerek kış hasta olunmadan atlatılabilir. Buda kişinin eğitim veya iş yaşamında yaşadığı kaybın önüne geçer. Ayrıca tedavi masraflarına da katlanılmamış olur. Bir firmanın risk yönetimi de tıpkı bireyin sağlık yönetimine benzer. Kurumlarında insanlar gibi potansiyel risk içeren dönemleri veya zaafa uğrayabileceği zayıf tarafları vardır. Kurumların yapması gereken kendi risk unsurlarını ve onların kuruma verebileceği zararları doğru tespit edip gerekli tedbirleri alarak riski ve sebep olacağı zararı en aza indirmektir.

Risk yönetimi kuruma 2 temel fayda sunmaktadır. Birincisi yaşanabilecek potansiyel zararın önüne geçerek performans, zaman ve maliyet kaybı yaşamamak. Verimli işleyen bir risk yönetiminin bir diğer faydası ise bir alanda gözlemlediği risk unsurunu doğru değerlendirip, tabiri caizse krizi fırsata çevirip, rakiplerine karşı rekabet üstünlüğü sağlayabilmesidir. Örneğin teknolojik bir atılım veya üretim tarzında bir değişiklik söz konusu olduğunda kurum cüzi olmayan bir maliyet karşılığında bu atılımı gerçekleştirmeyi düşünebilir. Yapılan bu atılım piyasanın tepkisine göre firmayı rakiplerinin önüne geçirebileceği gibi bulunduğu pozisyonu dahi muhafaza edemeyip pazar payını büyük ölçüde kaybetmesine de vesile olabilir. Ayrıca bazı durumlarda gerekli atılımı yapmamak da piyasanın gerisinde kalınacağı için risk unsuruna dönüşebilir.

Riskin incelendiği durum giriftleştikçe, değişkenler, etkilenenler arttıkça karar almak daha zor bir hale gelir. Karar verme mekanizmalarının çoğu karar verirken önsezilerini ya da yargılarını kullanır. Ancak bu iki unsur riski en aza indirmede noksan kalabilir. Riski en aza indirmede sezgilerden ve yargılardan daha kapsamlı hareket

edebilmek için risk yönetiminin sistematikleştirilmesi ve süreklileştirilmesi gerekmektedir. Riskin kritiklik derece ortaya konup sonuca etkisi tespit edilmelidir. Risk, telafisi mümkün olmayan zararlara sebep olacaksa etkisiz hale getirilmeli veya zararın minimum düzeye çekilmesi için riske yönelik gerekli çalışmalar ortaya konmalıdır (Kahraman, 2006).

2.2. Risk Yönetimi Kavramları

Risk yönetimi tabiri ilk defa 1950'li yılların sonlarında ABD' de kullanılmaya başlanmıştır. Risk yönetimi olasılık planlamasını da kapsayan bir kavramdır. Sürekli olarak "eğer olursa ne olur", "ya olursa" sorularının tekrarlanmasıdır (Emhan, 2009). Çevresel, siyasal, sosyal ve ekonomik faktörler hakkında yeterince bilgi edinilemeyen, içerisinde bulunulan konjonktürü doğru okunamadığı ve hatta kurum bünyesindeki zayıflıklar ve güçlü yönlerin yeterince değerlendirilmediği bir ortam da karar vermek rakımı yüksek, virajları sert ve sisli bir yol güzergâhında süratle araç kullanmaya benzetilebilir. Sağlıklı kararlar alabilmek uzun ve kısa vadeli yol haritaları çizebilmek için tüm risk faktörlerinin doğru tespit edilmesi gerekmektedir. Elbette bahsi geçen değişenler ve daha fazlası hakkında yeterli bilgiye sahip olunsa dahi piyasa koşullarında her zaman tespit edilemeyen risk faktörü mevcuttur ve mevcut olmaya devam edecektir. Tüm bu riskleri en aza indirgemek yahut kontrol altında tutmak için risk yönetimine ihtiyaç vardır. Risk yönetimini tam idrak edebilmek için aşağıdaki kavramları doğru tanımlamak gerekmektedir:

Risk kavramı

Farklı dillerde farklı karşılıkları bulunan ''Risk'' kavramı İtalyancada ''Risco'' Almanca da ''Risiko'' İngilizce de ise '' Risk'' sözcüklerinde kendine yer bulmuştur. Türk dilinde önceleri risiko olarak kullanılmış ve bu şekilde yerleşmiştir. Zarara ve kayba neden olabilecek risk, bu duruma sebebiyet verecek durumun ortaya çıkma ihtimali anlamına da gelmektedir. Risk yer yer tehlike kelimesi yerine de kullanılabilmektedir. Herhangi bir alan sınırlandırılması yapılamayacak geniş bir mevcudiyet alanı olan risk faktörü her sektörde hesaba katılan bir değerdir. Risk faktörünün oluştuğu yahut oluşabileceği durumlarda geleceğe dair belirsizlik ortaya çıkmakta olup, buna yönelik çözüm önerileri kurum içi veya dışı birimlerce öne sürüldüğünde riskin en aza indirgenmesi sağlanmış olur (Yahyaoğlu, Korkmaz, ve Akman, 2011).

Geçmişten günümüze aktarılan deneyimler, iflas eden dev firmalar, başarı hikâyeleri, ekonomik krizler geriye sadece rakamlardan ve tablolardan oluşan bir yığın bırakmamış aynı zamanda kişilerin ve kurumların bakış açılarında olayları algılama tarzlarında değişikliğe neden olmuştur. Bu durumdan risk kavramı da nasibini almıştır. Çizelge 2.1' de geleneksel ve modern bakış açıları yansıtılmıştır.

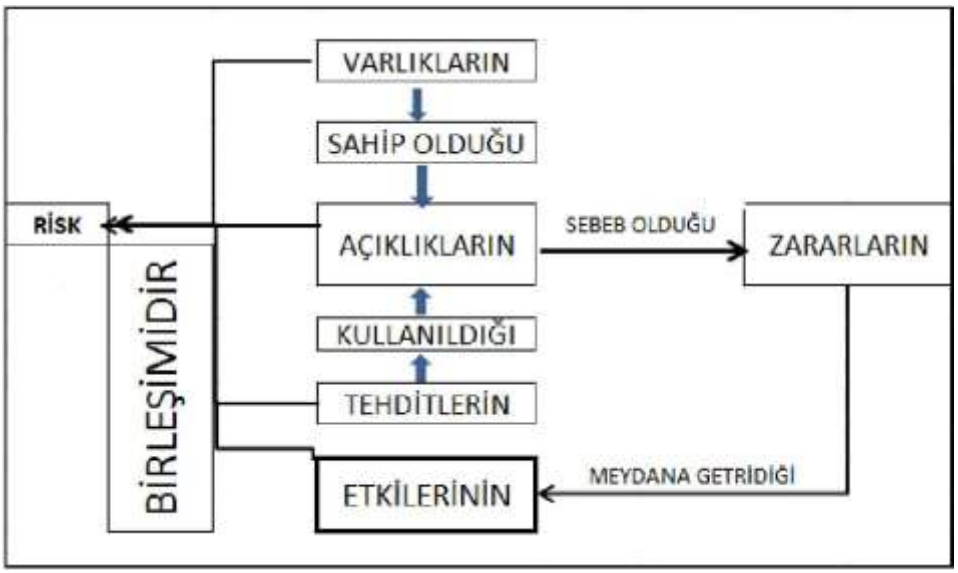
Çizelge 2.1. Riske geleneksel yaklaşım modern yaklaşım (Güneş, 2009)

GELENEKSEL YAKLAŞIM	MODERN YAKLAŞIM
Risk kaçınılması gereken bir afettir.	Risk kaçırılmaması gereken bir fırsattır
Risk bir ekip işidir.	Riskin kurum çapında bir bütün olarak değerlendirilmesi gerekir.
Risk yukardan aşağı hiyerarşi içerisinde yönetilir	Risk farkındalığı tüm kurum çapında geliştirilmelidir.
Risk ölçümü görecelidir.	Risk rakamlarla ölçülebilen nesnel bir değerdir.
Risk yönetimi için prosedürler hazırlanır.	Kurumsal risk yönetim sistemleri geliştirilmiştir.
İç kontrolü sağlayan bir denetleme komitesi mevcuttur.	Risk yönetim sisteminin canlılığını sağlayan bir Risk Komitesi kurulmalıdır.
Mali kaygı ön plandadır.	Riskler stratejik olarak ele alınır.
Risk azaltmaya gayret gösterilir.	Risk optimizasyonu hedeflenir.
Kurum değerini korumaya yönelik aksiyon alınır.	Kurumun sürdürülebilir büyümesi hedeflenir.

Riskin 2 temel bileşeni bulunmaktadır

- Belirli bir sonuca ulaşamama ihtimali veya istenmeyen bir durumun ortaya çıkması ihtimali
- Riskin gerçekleşmesi veya sonuca ulaşamama durumlarda uğranılan zarar

Bu temel bileşenler göz önünde bulundurulduğunda risk istenmeyen durumun meydana gelmesi ile bu durum meydana geldiğinde uğranılan zararın fonksiyonu şeklinde ifade edilebilir. Şekil 2.1' de risk fonksiyonu şematik şekilde ifade edilmiştir.



Şekil 2.1. Risk tanımı şeması (Bingöl, 2010)

Sonuç

Sonuç bir sürecin neticesi olarak isimlendirilir. Bir olayın birden çok sonucu olabileceği gibi birden çok olayın kümülatif bir sonucu da ortaya çıkabilir. Sonuçlar istatiski, ispatlanabilir olanları da vardır ispatlanamayan, kişiden kişiye değişen yapıda olanları da vardır. Olumludan olumsuza sıralanma imkânı olsa da sonuçlar güvenlik yönünden genellikle olumsuzdur.

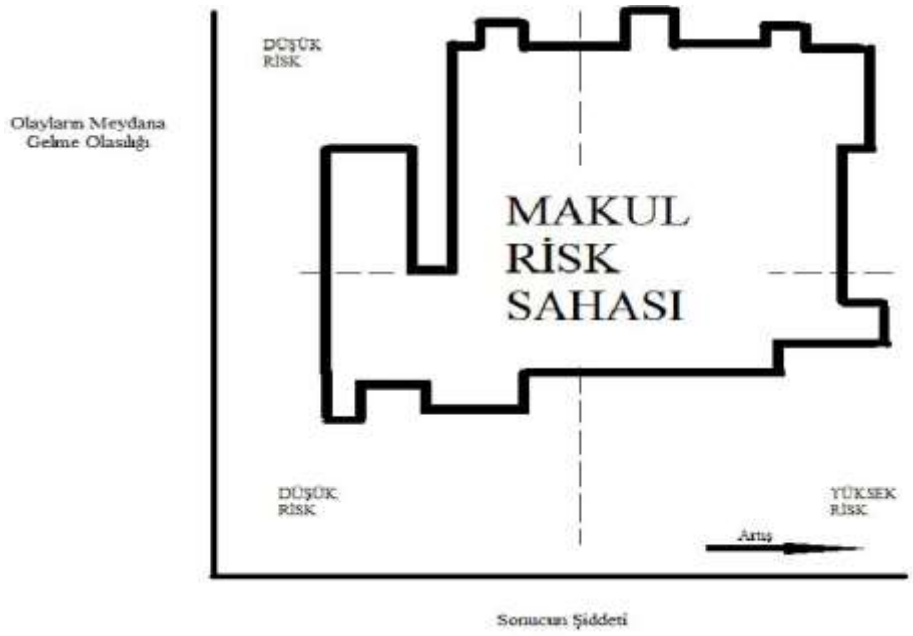
Olasılık

Olasılık bir olayın meydana gelme ihtimali olarak tanımlanabilir. Matematiksel olarak 0- 1 aralığında rastgele bir durumun gerçekleşmesiyle ilişkilendirilen pozitif bir sayıdır. Olasılık gerçekleşecek bir olaya inanma derecesi yahut sürekli tekrarlanan

olaylarda, olayın göreceli meydana gelme sıklığı olarak tarif edilebilir. İnanma derecesi arttıkça olasılık değeri 1' e yaklaşır.

Olasılık gelecekte yaşanacak olaylara dair kısıtlı bilgiye sahip olunması olarak da adlandırılabilir. Özet olarak olasılık gelecekte meydana gelecek olayları kestirememe olarak tarif edilebilir. Ortaya çıkabilecek herhangi durum hakkında bir olasılığın saptanamaması, olasılığı riskten ayıran en temel faktörlerden biridir.

Umumiyetle risk ve olasılık kavramları birbirinin yerine kullanılsa da risk ve olasılık birbirinden farklı şeylerdir. Riskli kısmın doğru idrak edilmesi ve olayın meydana gelmesinin veya olayın hiç meydana gelmemesinin potansiyel sonuçları analiz edilmelidir. Şekil 2. 2' te bu kavram gösterilmiştir.



Şekil 2.2. Olayların meydana gelme olasılığı (Kahraman, 2006).

Şiddet

Riskin ortaya çıkarabileceği zarar derecesidir.

Tehlike

Tehlike, olası riskin gerçekleşmesi halinde potansiyel yaralanma, hastalanma, zarar görme veya bunların bileşimi durumlardır. Bu durumlar kurumlar için insanlar için geçerli olabilir.

Risk kriterleri

Riskin öneminin olası zarar göz önünde bulundurularak değerlendirildiği referans noktalarıdır. Risk kriterleri, kuruluşun amaçlarına, dış ve iç kapsamına dayanır. Risk kriterleri, prosedürler, standartlar, kanunlar, politikalar ve diğer şartlardan faydalanarak hazırlanabilir (TS ISO/IEC Guide 73, 2012)

Çıkar grupları

Riske maruz kalan, riske maruz bırakan veya kendini riske maruz kalmış gibi algılayan kişi ve kuruluşlardır.

İlgili taraf

Bir kurumun kazanımlarından yahut performansından, fayda sağlayan kişi ya da kurum ‘’ilgili taraf’’ olarak tarif edilir. Misal olarak tüketiciler, hissedarlar, kurum çalışanları, bankalar, sendikalar, tedarikçiler veya toplum verilebilir.

Risk algılama

Herhangi bir çıkar grubunun değer ve kaygı durumuna göre şekillenen riske bakış açısı olarak tanımlanmaktadır. Risk algılama, çıkar gruplarının bütçesine, işlem hacmine, tecrübesine, tabi oldukları yasalara ve genel olarak riske yaklaşım tarzlarına göre değişebilmektedir (Kahraman, 2006).

Risk iletişimi

Riske dair verilerin karar verici unsurlarla diğer çıkar grupları arasında paylaşımı veya değişimi olarak adlandırılır. Bu bilgiler, riskin yapısı, oluşturacağı etkinin büyüklüğü, riskin yapısı, şiddeti, kabul edilebilirliği, riskin tarafları ve diğer boyutlarıyla ilgili olabilir.

Arta kalan risk

Doğru kanallardan elde edilen bilgilerin tecrübe sahibi kimselerce değerlendirilip güvenlik önlemleri uygulandıktan sonra kalan riskler olarak tarif edilmektedir.

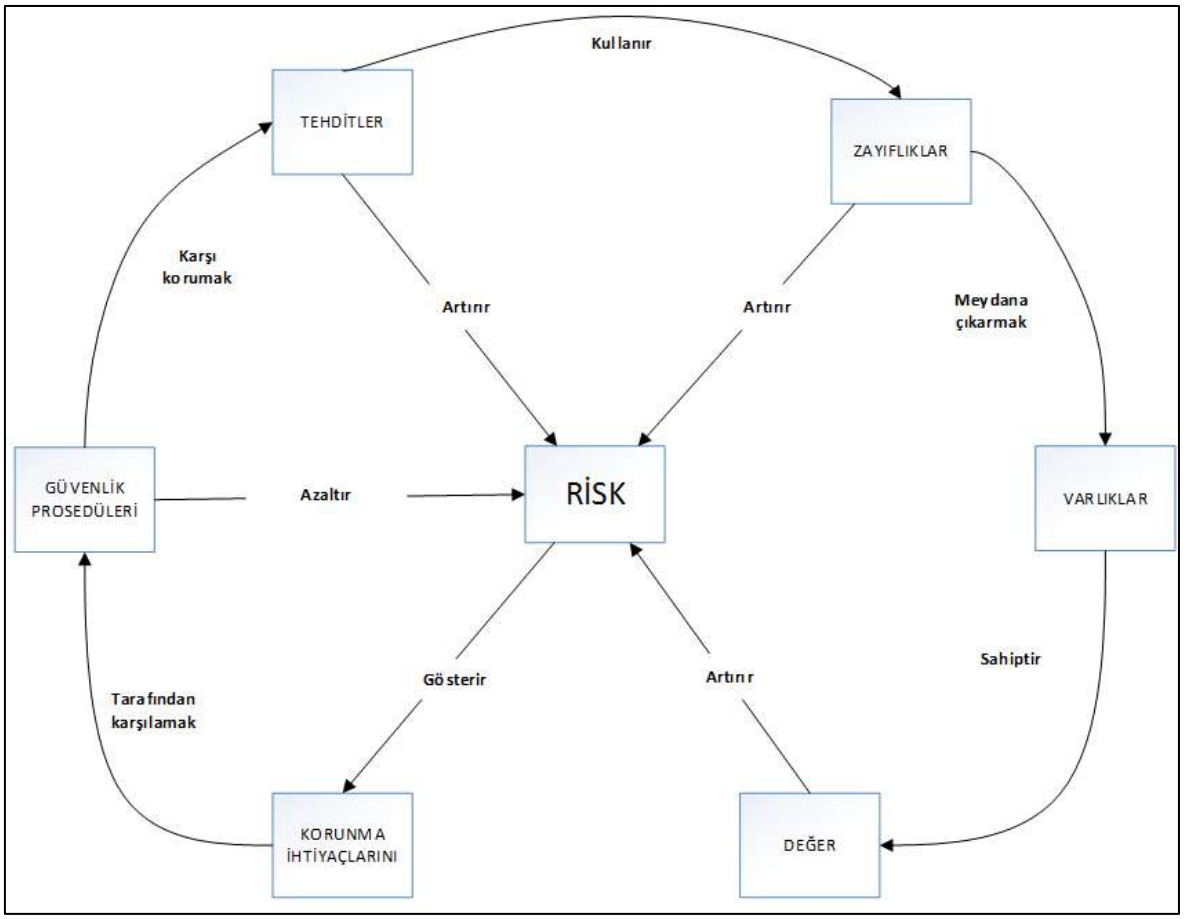
2.3. Risk Yönetiminin Bilgi Güvenlik Sisteminde Uygulanma Gereksinimi

Serbest piyasa ekonomisinin bir gereği olarak firmalar gerek birleşerek gerek iflas ederek sermayenin belirli mecralarda toplanmasına katkı sağlamışlardır. Finans, enerji ve benzeri diğer büyük sektörlerde yer alan kurumlar, holdingler içerisinde bulundukları ülkenin hasılasından aslan payını aldıkça sahip olduğu değerleri korumak, olası krizlerden en az hasarla ayrılmak ve hatta krizlerden büyüyerek ayrılmak için risk birimleri oluşturmuşlar, kurumlarına Risk Yönetim sistemi kurmuşlardır. Günümüzün en akışkan metalarından olan bilgi ve bilgiyi güvenliğini bir bütün olarak ele alan BGYS de Risk Yönetiminde payına düşeni almakta gecikmemiştir. Bilgi güvenliğinin geliştirilmesi adına yapılan çalışmalara başlandığı ilk dönemlerde çözümün hiçbir açık bırakmamak olduğuna inanılıyordu. Ancak gelişmeler gösterdi ki bilgi güvenliğinde bütün açıkları kapatmak her zaman mümkün olmuyordu. Bunun yerine kurumlar bilgi güvenliğinde potansiyel zarar alanlarının önceliklendirilmesini, eldeki kaynakların doğru tespit edilmesini ve zararın büyüklüğüne göre bütçe ayrılıp maliyetlerin dengelenmesini hedefleyen bir Risk Yönetimi anlayışı kazanmışlardır.

Gelişen teknoloji, arz ve talebin hızla şiddetle farklılaşması ve iş süreçlerinin bu doğrultuda karmaşıklaşması sistemler üzerindeki kontrolü oldukça zor hale getirmiştir. Hata ve dolandırıcılığı gerektiği anda fark edememek kurumlara çok pahalıya mal olacağından kurumlar altyapıya gerekli yatırımın yapılması gerektiğini fark etmişlerdir.

Günümüzde Bilişim Teknolojilerine entegre süreçler, artık kurum ve kuruluşlar için hayati önem arz eden unsurlardan biri haline gelmiştir. Bu teknolojilerdeki herhangi bir zafiyet kurumun diğer departmanlarına da sirayet etmekte ve kurumun asli fonksiyonlarını yerine getirememesine sebep olmaktadır (Kahraman, 2006).

Şekil 2.3’ de risk yönetimi ile bilgi güvenlik arasındaki bağlantı resmedilmiştir.



Şekil 2.3. Bilgi güvenliği ile risk yönetimi arasındaki ilişkiler (Kahraman, 2006)

3. ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN TANITIMI

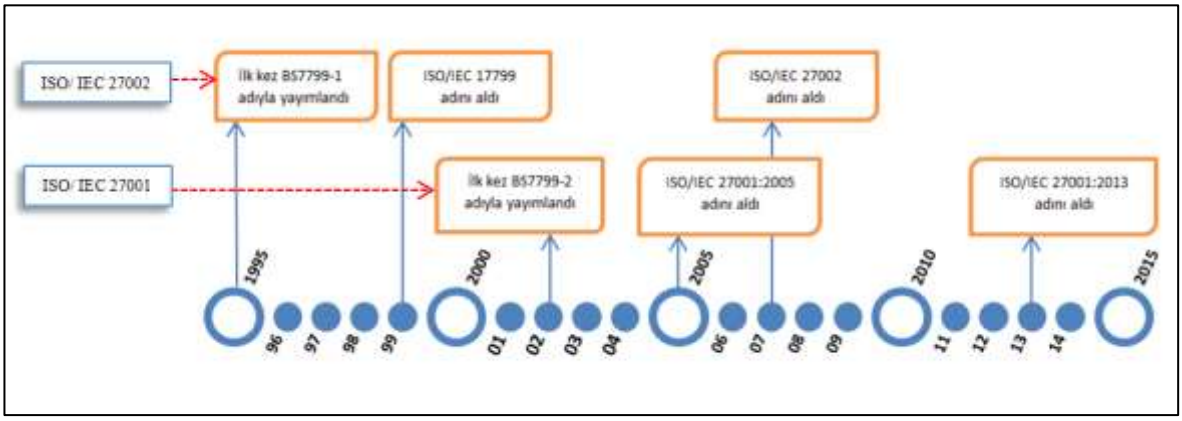
Önceleri şahısları, kurumların belli departmanlarını belki kurumları ilgilendirdiği düşünülen bilgi güvenliğinin ulusal hatta uluslararası ölçüde ele alınıp değerlendirilmesi gereken bir olgu olduğu neredeyse genel olarak kabul edilen bir gerçektir. Bağışlık kazanan insan bedenini etkisi altına almak için kendini yenileyen, yeni bir forma bürünen mikroplar gibi bilgi güvenliği tehditleri de alınan önlemlere karşı sürekli hacim olarak artarak ve yeni bir forma bürünerek hedefine ulaşmaya çalışır. Yazılım veya donanıma dair güncellemeleri ve bunlarda meydana gelen açıkları takip etmenin yanı sıra personelin sürekli eğitimi ve farkındalık bilinci kazandırılması gibi süreçlerin takibi için bilgi güvenliğini parça parça ele almak yerine bir bütün olarak değerlendiren bir bilgi güvenliği standardına ihtiyaç duyulmuştur. Bu konuda irili ufaklı firmaların çalışmaları ile yetinilmemiş ulusal ve uluslararası çalışmalar yapılmıştır. Öncelikle ulusal çalışmalardan ardından Uluslararası Elektroteknik Komisyonunu gerçekleştirdiği çalışmalara yer verilecek sonunda Türkiye' de Bilgi Güvenliği Standartlarına dair yapılan çalışmalardan bahsedilip üçüncü bölümün konusu olan TS ISO/IEC 27001 tanıtılacaktır.

3.1. Genel Olarak Bilgi Güvenliği Standartları

İngiliz Standartlar Enstitüsü (British Standart Institute-BSI) tarafınca yapılan çalışmalar sonucunda 1995 yılında BS-7799 standardının ilk kısmı olan BS7799-1 yayımlanmıştır. Ardından 1999 yılında standardın ikinci kısmı olan BS7799-2 İngiliz standardı yayımlanmıştır

BS7799-1 2000 yılında küçük güncelleme ve adaptasyon süreci nihayetinde ISO tarafınca ISO/IEC–17799 olarak kabul edilmiş ve uluslararası düzeyde kabul gören bir standart halini almıştır. BS-7799 standardının ikinci kısmı olan BS-7799-2 standardı üzerine ilaveler ve düzeltmeler yapılarak ikinci defa İngiliz standardı olarak 2002 yılında yayımlanmıştır. 2005 yılına gelindiğinde Uluslararası Standartlar Organizasyonu (International Organization for Standardization- ISO) tarafından ISO/IEC- 17799 standardı üzerinde değişikler yapılarak ISO/IEC–17799:2005 halini almışken 2007 yılında yapılan düzeltmelerle yayımlanan standardın son hali ISO/IEC- 27002 olmuştur. BS7799-2 ise 2005 yılında yapılan düzenlemeyle beraber ISO İngiliz standardından ISO/IEC:27001 uluslararası standarda dönüşmüştür. Şekil 3.1' de tarihsel akışa göre standartların

yayımlanma süreleri ve geçirdiği değişimler genel hatlarıyla verilmiştir. (Vural ve Sağıroğlu, 2008)



Şekil 3.1. Bilgi güvenliği standartlarının tarihsel gelişimi

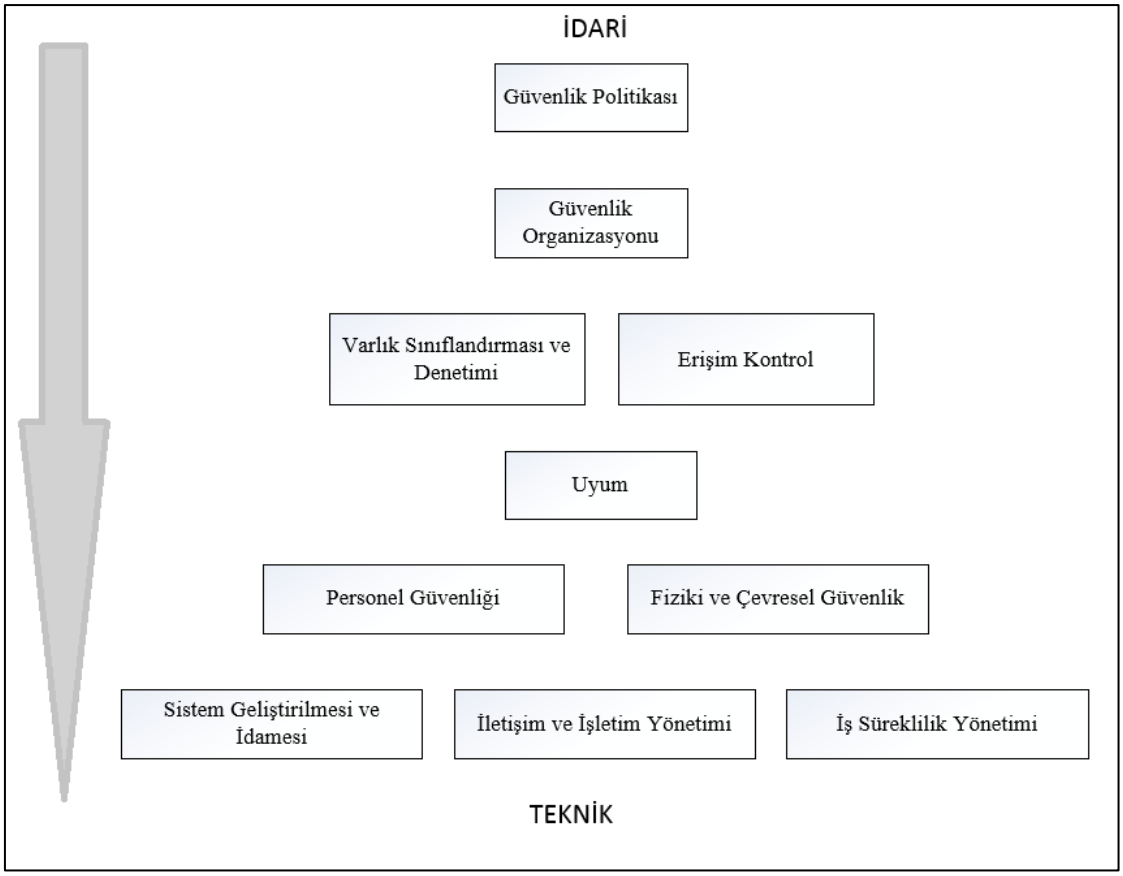
3.1.1. İngiliz standartları

BS-7799 bilginin gizlilik, erişilebilirlik ve doğruluğunu temin edebilmek için belirli güvenlik gereksinimleri oluşturan ve belgeleyen iki aşamalı İngiliz standardıdır. 1995 yılında yayımlanan ilk sürümün birinci bölümünde bilişim güvenliğinin sağlanması için çalışma kuralları yer almakta olup (Information Technology– Code of Practice for Information Security Management) 10 bölüm içerisinde 36 ana kontrol 127 alt kontrol maddesini içermektedir. İkinci bölümde (Information Security Management Systems– Specification with Guidance for Use) bilgi güvenliği yönetimi ele alınmış olup yönetim sisteminin planlanması, kurulması ve sürekliliğinin sağlanması için gerekli olan süreçler adım adım tanımlanmakta ve BGYS' ye ait belgelendirme bu kısım da gerçekleşmektedir.

BS-7799 kurumların bilgi güvenlik yönünden analiz edilmesine katkı sağlarken yalnızca ilgili kurumun prosedürlerini ele almakla kalmaz birlikte çalışılan kurumların ilgili sözleşmelerinin bilgi güvenliği konusunda gereken şartları sağlayıp sağlamadığını da göz önünde bulundurur. BS-7799 standardı endüstri ve ticari kuruluşlardan hatta devlet kuruluşlarından bilgi güvenliğinin sağlanması adına gelen talepler doğrultusunda BSI kuruluşu, BOC, BT, Marks& Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever ve diğer bazı kurumların katılımıyla hazırlanmış bir standarttır. Standardın tarihsel oluşumu incelendiğinde 1993 yılında endüstri çalışma grubunun kurulmuş, 1995

yılında İngiliz standardı olarak kabul görmüş, 1999 yılında büyük bir düzeltmeden geçerek birinci kısmı, 2002 yılında ise ikinci kısmı yayımlanmıştır.

BS-7799 standardı teknik ve idari olmak üzere 2 bölümden oluşmaktadır. Standardın birinci kısmının ilk sürümünde yer alan etki alanlarının idari ve teknik olarak iki ana kısımda incelenmesi Şekil 3.2' de gösterilmiştir (Vural ve Sağıroğlu, 2008).



Şekil 3.2. Standardın etki alanlarının sınıflandırılması (Vural ve Sağıroğlu, 2008)

Etki alanları aşağıda başlıklar halinde özetlenmiştir:

Güvenlik Politikası

Güvenlik politikaları kurumlarda kabul edilebilir güvenlik seviyesinin sağlanması ve sürdürülmesi için tüm çalışanların ve ortak çalışan diğer kurumların uyması gereken kurallar bütünüdür. Üst düzey yönetimince desteklenmeyen güvenlik politikaları ne kadar başarılı hazırlanırlarsa hazırlansınlar, başarısız olmaya mahkûmdurlar. Güvenlik politikaları çalışanlar tarafından anlaşılabilir, sade, uygulanabilir ve güvenlik

yöneticilerince yönetilebilir olmalıdır. Güvenlik politikaları çalışanların sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedefleri kapsayan uygulamaların açıklandığı genel ifadelerdir.

Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikalardan sorumlu olanların belirlendiği, uygulaması gereken kuralların, uygulanmadığında verilecek cezaların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı 7 bölümden oluşmalıdır. Bilgi Güvenliği Politikası içerisinde bulunması gereken bölümler Çizelge 3.1' de gösterilmiştir (Vural ve Sağıroğlu, Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, 2007).

Çizelge 3.1. Güvenlik politikası bölümleri (Vural & Sağıroğlu, Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, 2008).

Bölüm adı	İçeriği
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlandığı bölümdür.
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğunu açıklar.
Kapsam	Politikaya uyması gereken çalışan grupları ve bilgi varlıklarını belirler.
Politika	Uygulanması ve uyulması gereken kuralların yani politikanın yer aldığı bölümdür.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımların açıklandığı bölümdür.
Tanımlar	Teknik terimler ile muğlak ifadeler listelenerek açıklanır.
Düzeltme Tarihçesi	Politika içerisinde yapılan değişiklikler, tarihler ve sebepleri yer alır.

Güvenlik organizasyonu

Kurum personeli tarafından ve beraber çalışılan diğer kurumlarca erişilebilen bilgi güvenliğini ilgilendiren tüm varlıklarının güvenliğinin sağlanmasını içeren çalışmalar bütünüdür.

Varlık sınıflandırması ve denetimi

Kurum bilgi varlıklarının korunmasının sağlanması ve bilgi kaynaklarının uygun koruma seviyesine olduklarının temin edilmesidir.

Erişim kontrol

Bilgiye erişimin gözlem altında tutulması, bilgi sistemlerine yetkisiz erişime izin verilmemesi, yetkisiz kullanıcı erişiminin engellenmesi, hizmetlerin korunması ve uzaktan erişimin uygun standartlar çerçevesinde gerçekleşmesidir.

Uyum

İlgili mevzuatın takibi ve mevzuata aykırı bir işlem gerçekleştirilmemesi, organizasyonun güvenlik politika ve prosedürlerinin sisteme uyumunun sağlanması, sistem takip seviyesinin yükseltilmesidir

Personel güvenliği

Bilgi güvenliği zafiyetlerinin sebepleri araştırıldığında ilk sıralarda yer alan personel unsuru göz ardı edilemeyecek bir etki alanıdır. Personel kasten ve kasıtsız bir şekilde kurumun bilgi güvenliğini tehlikeye atabilmektedir. Bu açıdan faaliyet alanlarına tehditlerden ve bu tehditlerle ilgili sorumluluklardan personelin haberdar edilmesi gerekir.

Fiziki ve çevresel güvenlik

Yetkisiz erişimlerin önüne geçilebilmesi ve çevreden kaynaklanabilecek tehditlere karşı alınan önlemlerdir.

Sistem bakım ve idamesi

Bilgi güvenliğini sağlamak için temin edilen sistemlerin kapsamlı bir şekilde tetkikinin sağlanması, bilginin bütünlüğünün, gizliliğinin ve erişiminin korunması, sistemde kayıtlı kullanıcı bilgilerin değiştirilmesinin ya da yitirilmesinin önüne geçilmesidir.

İletişim ve işletim yönetimi

Bilgi işlem tesislerinin doğru ve güvenle işletildiğinin temin edilmesi, sistem arızalarının en aza indirgenmesi, bilgi işlem ve iletişim hizmetlerinin kullanılabilirliği ve bütünlüğünün sürdürülmesi, ağlarda yer alan bilgilerin emniyetinin ve destekleyen altyapı sisteminin korunması, iş faaliyetlerinin kesintiye uğratılmasının ve varlıklara zarar verilmesinin önüne geçilmesi ve organizasyonlar arası akışkanlığa sahip bilginin yanlış kişilere ulaşması, değiştirilmesi ve kaybedilmesinin önlenmesidir.

İş süreklilik yönetimi

Kurum süreçlerinde karşılaşılan olumsuzlukların giderilmesi ve kritik ticari işlemlerin sürekliliğinin sağlanması.

Kurumlar bilgi varlıklarını tespit edip sınıflandırdıktan sonra, bilgi varlıklarıyla ilgili tehdit ve zafiyetleri analiz ederek bahsi geçen kontrollerden hangilerinin uygulanıp, hangilerinin uygulanmayacağına karar vererek standardın kapsamını kendi kurumlarına özgü şekilde belirleyebilirler.

BS-7799 ikinci kısmında kurumun güvenlik ihtiyaç ve zafiyetlerinin belirlenmesi için gereken bilgi güvenliği yönetiminin çerçevesi tanımlanarak BS-7799 birinci kısmında tanımlanan kontroller uygulanmaktadır.

BGYS ile ilgili bir başka İngiliz standardı Aralık 2005’ te BS-7799-3: 2005 Bilgi Güvenliği Yönetim Sistemleri Risk Yönetiminin Kuralları adıyla yayımlanmıştır. Standart 2006 yılında tekrar gözden geçirilip BS-7799: 2006 adıyla yayımlanmıştır. BS-7799-3 standardı BS-7799-2 standardının uygulanması için destek sağlamak kaydıyla ölçeklenebilir (küçük, orta veya büyük kurumlar) yapıda standardın yaygınlaşmasına

yardımcı olması için tasarlanmıştır. Standart riskin tanımlanması, tanımlanan riskin kontrol edilmesi ve izlenmesi, kontrol yönetim sistemlerinin bakımı gibi risk yönetimiyle ilgili konular üzerine odaklanmıştır (Vural ve Sağıroğlu, 2008).

3.1.2. ISO/ IEC standartları

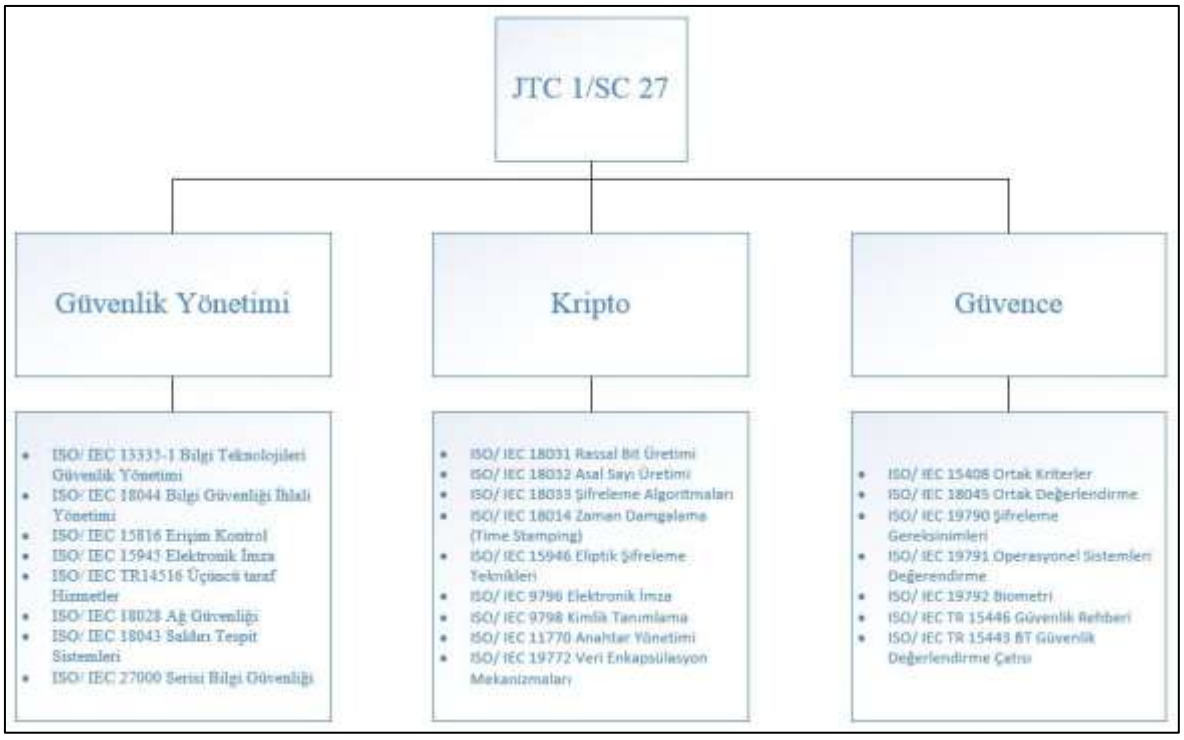
Uluslararası Elektroteknik Komisyonunu (IEC) 1906 senesinde ISO 1947 yılında uluslararası ölçekte ticari ISO ve elektroteknik IEC standardizasyonun sağlanması adına, İsviçre' nin Cenova şehrinde kurulmuştur. ISO ve IEC birlikte çalışma komisyonları oluşturarak Joint Technical Committee (JTC) uluslararası alanda geçerli olacak standartlar ortaya koymaktadırlar. Bununla beraber ISO tarafından bilgi teknolojileri (BT) Güvenlik Standartları ile ilgili çalışmalar JTC- 1 Bilişim Teknolojileri Komitesine bağlı bulunan SC27: BT Güvenlik Teknikleri Alt Komisyonunda gerçekleştirilmektedir. Bu komisyonun sorumluluklarına özet şekilde aşağıda değinilmiştir (Vural ve Sağıroğlu, 2008). Bu sorumluluklar;

- Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması,
- Güvenlik teknikleri ve mekanizmalarının geliştirilmesi,
- Güvenlik kılavuzlarının geliştirilmesi
- Yönetim destek dokümanları ile standartların geliştirilmesidir.

Yukarıda açıklanan görevleri yerine getirmek amacıyla bu komisyon içinde 5 farklı çalışma grubu Working Group (WG) varlığını sürdürmektedir. Bu gruplar aşağıda ifade edilmiştir (Vural ve Sağıroğlu, 2008).

- Çalışma Grubu–1 (JTC 1/SC 27/WG 1): BGYS
- Çalışma Grubu–2 (JTC 1/SC 27/WG 2): Şifreleme ve güvenlik mekanizmaları
- Çalışma Grubu–3 (JTC 1/SC 27/WG 3): Güvenlik değerlendirme kriterleri
- Çalışma Grubu–4 (JTC 1/SC 27/WG 4): Güvenlik denetimleri ve hizmetleri
- Çalışma Grubu–5 (JTC 1/SC 27/WG 5): Kimlik yönetimi ve mahremiyet

1, 2 ve 3 nolu çalışma grupları ve sorumlu oldukları konular Şekil 3. 3' de gösterilmiştir.



Şekil 3.3. ISO/IEC güvenlik çalışma grupları (Vural ve Sağıroğlu, 2008)

SC27 ye bağlı bulunan çalışma gruplarından Çalışma Grubu-1 (WG-1), şekil 3' de yer alan BGYS standartları (ISO/IEC 17799, ISO/ IEC 27000 Serisi) ile ilgili çalışmaları yürütmektedir. Bu standartlar aşağıda kısaca açıklanmıştır.

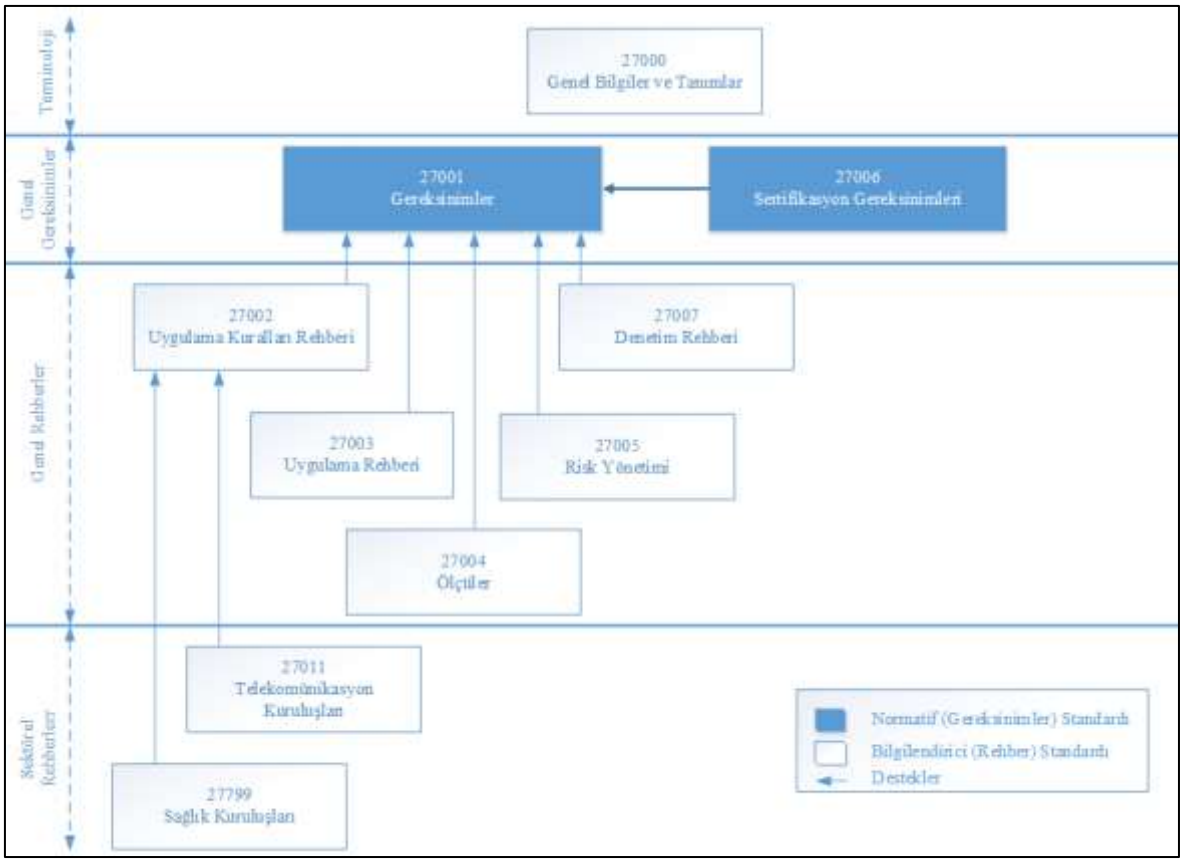
ISO/ IEC 27002 standardı: BS–7799 standardının ikinci sürümü Mayıs 1999'da çıktığında ISO, BSI' nın yayımladığı çalışmayla ilgilenmeye başlamıştır. Aralık 2000'de, ISO BS–7799 standardının ilk bölümünü alarak ISO/IEC 17779 olarak yeniden isimlendirilmiş ve yeni bir standart olarak yayımlamıştır. ISO/IEC 17779 standardı daha önceki bölümde açıklanan BS–7799 standardının ilk bölümüne eşdeğerdir.

ISO/ IEC 27002 standardının uygulamaya alınması kurumsal bilgilerin tam anlamıyla riskten arındırıldığını düşünmek hatalı olur. Bu standart bilgi güvenliği sistemini başlatan ve sürekliliğini sağlamaya çalışan kurumların kullanımı için bilgi güvenliği ile ilgili yol haritası çizer. ISO/ IEC 27002 güvenlik standartlarını bir kurumun uyguluyor olması kuruma aşağıda yer alan avantajları kazandırmaktadır (Vural ve Sağıroğlu, 2008).

- Organizasyonel açıdan sorumlulukların tespitini sağlayarak, BGYS' nin her aşamada uygulanmasını sağlar.

- Kurumun tabi olduğu tüm yasal mevzuatın takibatını sağlayarak kurumun itibarını korur.
- Bilgi yönetim sisteminin içerisinde bulunduğu ve olası tehdit unsurlarından korunması konusunda rehberlik eder.
- İş ortakları, hissedarlar ve müşteriler; kurumun bilgi koruması konusuna atfettiği önem sayesinde kuruma olan güvenleri artırır ve ticari rakipleri arasında piyasada farklı bir yere gelmesini sağlar.
- Güvenlik açıklarının belirlenerek önlem alınması sonucunda mali kayıplar en aza indirgenecektir.
- Kurum personelinin bilgi güvenliği konusunda farkındalık geliştirmesine katkıda bulunur.

ISO/IEC 17799 standardı 2005 yılında gözden geçirilerek ISO/IEC 17799:2005 ismini almasının ardından 2007 yılında ISO/IEC 27002 olarak nihai haline ulaşmıştır. ISO/IEC 27002 Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların BGYS kurmaları, uygulamaları, sürdürülebilir hale getirebilmeleri için hazırlanmış bir kılavuz olup önceki sürümünden farklı olarak, yaşanan problemlerden, arızalardan, kazalardan ders çıkarılıp tekrar yaşanmasına engel olmayı amaçlamaktadır. Bu sebepten, alınmasına ihtiyaç duyulan önlemler için gerekli olan yönetim mekanizmasının kurulmasını sağlar. Ayrıca bilgi güvenliği ihlallerinin yönetimi ile ilgili bilgi güvenliği denetimlerini ve ilgili uygulamaları da içermektedir. ISO, 2005 yılında bir düzenlemeye giderek Şekil 3.4.' de verilen 27000 serisini bilgi güvenliği için kullanma kararı almıştır. ISO/IEC 27000-27059 standartları arasında yer alanlar ISO tarafından SC27 grubuna dâhil çalışma grupları için bilgi güvenliğiyle ilgili planlanan standartlara ayrılmıştır (Vural ve Sağıroğlu, 2008).



Şekil 3.4. ISO 27000 standart ailesi (Özbilgin ve Özlü)

Bilgi güvenliği ile ilgili olarak ISO 27000 serisi güvenlik standartları, (Şekil 3. 4) kullanıcı farkındalığının kazanılması, güvenlik risklerinin en aza indirgenmesi ve de güvenlik açıklarıyla karşılaşıldığı zaman alınacak önlemlerin belirlenmesinde temel bir başvuru kaynağıdır. Bu standartlar temel ISO 9000 Kalite Yönetim ve ISO 14000 Çevresel Yönetim standartlarına uyumlu tasarlandığından yönetim standartlarının gereklerini de yerine getirmektedir.

ISO 27000 standardı, ISO 27000 standartlar ailesi ile ilgili kavramların açıklanmasını sağlayan ve bilgi güvenliği yönetimine yönelik temel bilgileri, teknik terimleri bünyesinde barındıran bir sözlük formatında geliştirilmiştir. ISO 27000 standartlarının büyük bir çoğunluğu bilenen, diğerleri ise basım aşamasında olan standartlar olarak verilebilir (Özbilgin & Özlü)

Çizelge 3.2’ de yayımlanan ve taslak halinde olan ISO 27000 standartları, güncellemeler göz önüne alınmadan son yayımlanma tarihleri baz alınarak kısaca gösterilmeye çalışılmıştır.

Çizelge 3.2. ISO 27000 standart ailesi (Hinson, 2017)

Standart	Yayımlanma Tarihi	Başlık	Notlar
ISO/ IEC 27000	2016	BGYS- Genel Bakış ve Teknik Terimler	ISO 27000 standartlarının genel olarak tanıtımı ve gerekli terimler
ISO/ IEC 27001	2013	BGYS- Gereklilikler	BGYS için kulaktan dolma bilgiler yerine resmi gereklilikler
ISO/ IEC 27002	2013	Bilgi güvenliği kontrolleri için uygulama esasları	BYGS ile ilgili gereksinimlerin karşılanması konusunda rehberlik eden, en iyi uygulamaları içeren standarttır.
ISO/ IEC 27003	2017	BGYS- Uygulama rehberi	BGYS sisteminin uygulanmasıyla ilgili rehberlik yapmayı amaçlayan standarttır.
ISO/ IEC 27004	2016	BGYS metrikleri ve ölçüm	BGYS' nin ölçümü ile ilgili kriterler açısından rehber standarttır.
ISO/ IEC 27005	2011	BGYS risk yönetimi	BGYS' nin önemli bir süreci olan risk yönetimi ile ilgili rehber standarttır.
ISO/ IEC 27006	2015	BGYS belge kaydı ve belgelendirme süreçleri kılavuzu	Belgelendirme kuruluşları için rehber standarttır.
ISO/ IEC 27007	2011	BGYS denetimlerine yönelik rehber standarttır.	Belgelendirme kuruluşlarına, iç ve dış denetim organlarına rehberlik sağlar
ISO/ IEC TR 27008	2011	Bilgi güvenliği denetçileri için hazırlanmış rehber standarttır.	27007 için tamamlayıcı bir standarttır. Bilgi güvenliği kontrollerinin denetiminin üzerine eğilir
ISO/ IEC 27009	2016	ISO/ IEC 27001' in Sektöre has uygulamaları için hazırlanmıştır.	ISO/IEC 27001' in herhangi bir sektör özelinde gerekliliklerini tanımlar.

ISO/ IEC 27010	2015	Sektör içi ve kurum içi haberleşme konusun BGYS içerisinde ele alınışı	Bilgi güvenliği konusunda kurum içi, sektör içi veya ülkeler arası haberleşmeyi belirli standartlar üzerine temellendirmeyi hedeflemektedir.
ISO/ IEC 27011	2016	Telekomünikasyon kuruluşları açısından BGYS' nin uygulanışına yönelik rehber standarttır.	Telekom endüstrisinde bilgi güvenliği kontrollerini ele almaktadır.
ISO/ IEC 27013	2015	ISO/ IEC 27001 ve ISO/ IEC 20000 standartlarının entegrasyonuna dair bir rehber.	ISO/ IEC 27000 ile BT Servis Yönetiminin/ ITIL uyumlulaştırılmasını hedefler.
ISO/ IEC 27014	2013	Bilgi Güvenliğinin Yönetimi	ISO/IEC JTC1/SC 27 Telekomünikasyon Standardizasyon Sektörüyle iş birliği içerisinde spesifik olarak organizasyonların bilgi güvenliği aranjmanlarını yönetmesi adına geliştirilmiştir.
ISO/ IEC TR 27015	2012	Finansal servislerin bilgi güvenliği yönetimi için hazırlanan bir rehberdir.	Bu rehber bankalar, sigorta kuruluşları, kredi kartı firmaları vb. firmaların ISO27000 uygularken karşılaşacakları problemleri en aza indirgemek amacıyla hazırlanmıştır.
ISO/ IEC TR 27016	2014	BGYS- Organizasyonel Ekonomi	Bilgi güvenliğine dair yatırımların geri dönüşünü, mali tablolarını düzenlemeyi hedef alan bir standarttır.
ISO/ IEC 27017	2015	Bulut bilişim hizmetiyle ilgili bilgi güvenliğiyle ilgilenir.	ISO/ IEC 27002 temel alınarak bulut bilişim hizmetinin bilgi güvenliği kontrolü altında uygulanması amacıyla geliştirilmiş bir standarttır.
ISO/ IEC 27018	2014	Bulut bilişimde kimlik tanımlama konusunu bilgi güvenliği	Bulut bilişimde mahremiyet konusunu ele alır.

		ekseninde değerlendiren bir standarttır.	
ISO/ IEC TR 27019	2013	ISO/ IEC 27002 temel alınarak hazırlanan enerji endüstrisi için bir bilgi güvenliği rehberi.	Bu standart ISO/IEC 27002:2005' in enerji endüstrisinin organizasyonuna yardımcı olmak amacıyla hazırlanmıştır.
ISO/ IEC 27021	Taslak Aşamasında	Bilgi güvenliği yönetimi profesyonelleri için mesleki gereklilikleri içeren rehber.	Bu alanda görev yapanlar için beceri ve bilgi rehberi.
ISO/ IEC 27023	2015	ISO/ IEC 27001 ve ISO/ IEC 27002 standartlarının gözden geçirilmiş versiyonlarını uyumlulaştırmak ve analiz etmek için bir rehber	Bu standart ISO/ IEC 27001 ve ISO/ IEC 27002 standartlarının son versiyonlarını eski versiyonlarıyla kıyaslamak veya analiz etmek için tasarlanmıştır.
ISO/IEC 27031	2011	Bilgi ve komünikasyon teknolojilerinin iş sürekliliği için hazırlık durumunu gözden geçirir.	Bilişim ve iletişim teknolojilerinin sürekliliğinin yanı sıra genel iş sürekliliğini desteklemeyi hedefler.
ISO/IEC 27032	2012	Siber güvenlik için rehber.	Siber boşluktaki bilginin güvenlik, erişilebilir ve bütünlüğünü korumayı temin eder.
ISO/ IEC 27033	2015	Ağ güvenliğinin tasarımı ve güvenliğini sağlamayı hedefler.	Ağ bağlantısının yanı sıra kablosuz IP ağ hesaplarının güvenliğini temin eder. Ayrıca VPN (Virtual Private Network) kullanıcıları arasındaki komünikasyonun güvenliğini sağlamaya çalışır.
ISO/ IEC 27034	2016	Uygulama güvenliği-Gözden geçirme	Tekrar kullanabilir bilgi güvenliği kontrol fonksiyonları kütüphanesi oluşturmayı hedefler.

ISO/IEC 27035	2016	Bilgi Güvenliği Olay Yönetimi- Olay yönetiminin prensipleri	Olay ve problem yönetimi için yapılması gereken hazırlıkları kapsar.
ISO/IEC 27036	2016	Tedarikçi ilişkileri için Bilgi Güvenliği	Bilişim ve iletişimin dış kaynak yönetiminin bilgi güvenliği organlarıyla ilgilenir.
ISO/IEC 27037	2012	Dijital kanıtların toplanması, tanımlanması, edinilmesi ve korunmasını amaçlayan bir rehber.	Kanıt değeri taşıyabilecek dijital verilerin saklanması, tanımlanması ve korunmasını amaçlar.
ISO/IEC 27038	2014	Dijital redaksiyonu hedefler	Dijital dokumanın redaksiyonu yapılırken dikkat edilmesi gereken bilgi güvenliği unsurları
ISO/IEC 27039	2015	Saldırı sezme ve önleme sistemi(IDPS) nin seçimine, kullanımına ve konumlandırılmasına rehberlik eder.	Bu standart IDPS sisteminin efektif kurulumunu sağlama konusunda kuruma rehberlik eder.
ISO/IEC 27040	2015	Depo/ Bellek güvenliği	Kaydedilen veriler için bilgi güvenliği
ISO/IEC 27041	2015	Olay soruşturma yeterliliği ve uygunluğu konusunda rehberlik sağlar.	Hayati önem arz eden adli delillerin bütünlüğünü temin eder.
ISO/IEC 27042	2015	Dijital kanıtların yorumlanması ve analiz edilmesi konusunda kuruma rehberlik eder.	Bilgi güvenliğinin adli delillerinin analitik metotları.
ISO/IEC 27043	2015	Olay soruşturma prensipleri ve süreçleri	Adli veri soruşturmasının temel prensipleri
ISO/IEC 27050	2016	Elektronik keşif- Genel bakış ve farkındalık.	4 parçadan oluşan bu standart elektronik ortamda yedeklenen verinin fazlarını keşfetmeyi amaçlar.
ISO/IEC	Taslak	Siber güvenlik, ISO ve IEC standartlarını bir	Bu standart ISO 27000' e ek olarak ISO ve IEC

PDTR 27103	Aşamasında	arada ele alır.	standartlarının kullanışlı olarak nasıl uygulanacağını gösterir
ISO/IEC 27799	2016	Sağlık sektöründe bilgi güvenliği	ISO/ IEC 27002 kullanılarak sağlık endüstrisinde bilgi güvenliğinin temini

3.1.3. Türk standartları

Türkiye' de bilgi güvenliği standartları ve geriye kalan tüm standartlarla ilgili çalışmalar, belgelemeler TSE tarafından yapılmaktadır. TSE teknik kurulunun ISO/ IEC 17799: 2000 standardının tercümesini gerçekleştirerek 11 Kasım 2002 tarihinde aldığı karar ile TS ISO/ IEC 17799 Bilgi Teknolojisi- Bilgi Güvenliği Yönetimi için Uygulama Prensipleri Türk Standardı olarak kabul edilmiştir. TS ISO/IEC 17799 standardı; kuruluşlar bünyesinde bilgi güvenliğinin temelini atan, onu gerçekleştiren ve sürekliliğini sağlayan, bilgi güvenliği yönetimi ile ilgili tavsiyeleri içermektedir.

TSE tarafından yapılan BGYS belgelendirme sürecine yönelik çalışmalar nihayetinde BS 7799–2: 2002 standardı Türkçeye kazandırılmış ve "Bilgi Güvenliği Yönetim Sistemleri–Özellikler ve Kullanım Kılavuzu" adı altında TS 17799–2 standardı olarak 17 Şubat 2005 tarihinde yürürlüğe geçmiştir. Ancak TS ISO/IEC 27001:2006 "Bilgi Teknolojisi–Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri–Gereksinimler", 02.03.2006 tarihinde TSE tarafınca Türk standardı olarak kabul edildi. Bu sebepten TSE TS 17799–2 standardını iptal etmiştir (Vural ve Sağıroğlu, 2008).

3.2. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

ISO/IEC 27001 dünya geneli geçerliliğe sahip olan ve gün geçtikçe daha fazla alanda zorunlu hale getirilen bir standarttır. Kurumlarda bilgi güvenliğinin tesisi ve sürdürülmesini amaçlamaktadır. Kurumun ISO/IEC 27001 standardını uygulaması ve sertifikasını alması, dünyanın bilgi güvenliği alanında en başarılı firması olması gerektirmez, zaten standardın bu tür bir amacı bulunmamaktadır. ISO/IEC 27001 standardının amacı Bilgi Güvenliği konusunda kurumun seviyesinin kurum yöneticileri tarafından bilinir hale getirilmesi ve onlar tarafından alınan kararlar doğrultusunda sürekli artan bir güvenlik seviyesinin sağlanmasıdır (Çetinkaya, 2008).

3.2.1. ISO/IEC 27001 sertifikasyon süreci

ISO/IEC 27001 belirli prosedür ve yönetim gereksinimleri sağladıktan sonra yetkili kuruluşlarca sağlanan ve 3 yıl geçerliliği olan bir sertifikadır. Şekil 3.5' de örnek bir ISO/IEC 27001 Sertifikası gösterilmiştir.


A, B, C faaliyetlerini yerine getirmekte olan

X, Y, Z LİMİTED ŞİRKETİ

ISO/IEC 27001 Uluslararası sistem standardına uygun bir Bilgi Güvenliği Yönetim Sistemi dokümantasyonu kurmuş ve yönetmektedir.

Belge No: XXX. XXX. XXX

Yayın Tarihi: XX/XX/2017

Geçerlilik Tarihi: XX/ XX/ 2020

Şekil 3.5. ISO/IEC 27001 sertifikası

Bir kuruluşun ISO/IEC 27001 sertifikasına sahip olması, kurumun güvenlik risklerini bildiği, yönettiği, belli riskleri de ortadan kaldırmak için kaynak ayırdığı ve harekete geçtiği anlamına gelmektedir (Şen, ISO 27001 Kurumsal Bilgi Güvenliği Standardı).

Kurum ve kuruluş gibi tüzel kişilikler ISO/IEC 27001 sertifikasını Türkiye' de Türk Standartları Enstitüsü veya diğer bazı danışmanlık firmalarından edinebilmektedirler. Temin edilen bu sertifika belirli aralıklarla yetkili firmalarca denetimden geçerler.

Bir kurumun ISO/IEC 27001 sertifikasını verebilmesi ve denetimini sağlayabilmesi için bir akreditasyon kurumunca akredite edilmesi diğer bir deyişle denklik onayı alması gerekmektedir. İngiltere' de bu standardın akreditasyon görevini United Kingdom Accreditation Service (UKAS) adlı kurum yerine getirmektedir. Türkiye' de ise bu görevi

27.10.1999 tarih ve 4457 sayılı yasa ile hayata geçen Türk Akreditasyon Kurumu (TURKAK) yerine getirmektedir. Türk Standartları Enstitüsü, ISO/IEC 27001 konusunda TURKAK' ın belirlediği şartları yerine getirmek zorundadır. Bu şartlar sağlanmadan akreditasyon sağlanamamaktadır. TURKAK uluslararası bir akreditasyon kurumu olan European co-operation for Accreditation (EA)' nın bir üyesidir (Ersoy, 2012).

3.2.2. ISO/IEC 27001 özellikleri

ISO/IEC 27001 ölçülebilirlik, tekrarlanabilirlik ve ölçeklenebilirlik gibi 3 temel özelliğe sahiptir. Bu 3 özellik sayesinde risklerin daha gerçekçi şekilde ele alınıp değerlendirilmesi ve daha doğru adımlar atılabilmesi sağlanmıştır.

Ölçülebilirlik

Sadece kurum tarafından değil üçüncü taraflarca da objektif bir şekilde değerlendirilmesi ISO/IEC 27001' in tercihe şayan özelliklerindendir. Varlıkları değerlendirerek tehdit değerlerini, zayıflıkları, etkilenme derecelerini, risklere karşı toleransları ortaya koyan standart tehditlerin gerçekleşebilme ihtimallerini somut verilerle ortaya koyar.

Tekrarlanabilirlik

Çeşitli tedbir uygulamalarını bünyesinde barındıran yönetim sistemi belirli bölümler için tekrar tekrar uygulanabilir. Bu sayede risklerin gerçekleşme oranı aşağı çekilir.

Ölçeklenebilme

BGYS kurum içinde belirli bir bölüm için tasarlandıktan sonra diğer departmanlar için uygulanabilir. Zamanla işlevini yitiren bölümler kapsam dışında bırakma olanağı her zaman mevcuttur. Uygulamaya bir kapsam belirlemek kurumun hacmine, yapısına ve işleyiş yapısına göre farklılık gösterir. Hangi bölümlerin kapsanacağına hangilerinin kapsam dışı bırakılacağı kurum inisiyatifine kalmış bir durumdur (Ersoy, 2012).

3.2.3. ISO/IEC 27001 içeriği

ISO/IEC 27001 Standart Maddeler ve Ek-A kontrol noktalarından oluşur. Kurum kendi tercihlerine, tedarikçilerine, iş hacmine, faaliyet alanına, bilgi varlıklarına göre Ek-A maddeleri üzerinden seçimlik hakka sahiptir. Belirlediği kıstaslar üzerinden denetimler geçirir. Ancak kurumun faaliyet alanı veya iş hacmi ne olursa olsun standart maddeler üzerinde seçme hakkı yoktur. Standart maddelerin bütün hepsi sağlanmak zorundadır.

Standart maddeler

Kurumun bilgi güvenliğini temel olarak sağlaması gerekenlerin bahsedildiği bölümdür. Bu maddeler standardın sürekliliği sağlanması için başlangıç olarak sağlanması gereken unsurlardır. Nasıl ki şehir tasarlanırken önce altyapı çalışmaları tamamlanmadan atılacak herhangi bir adımda büyük maliyet ve zaman kayıpları yaşanırsa; ISO/IEC 27001 için altyapı mahiyetinde olan Standart Maddeler tamamlanmadan yol kat edilmesi beklenemez. Şekil 3.6' da ana başlıklar halinde sıralanan Standart Maddeler organizasyonel unsurları barındırır.

0 Giriş	**7 Destek**
1 Kapsam	7.1 Kaynaklar
2 Atıf yapılan standartlar ve/veya dokümanlar	7.2 Yetkinlik
3 Tanımlar ve terimler	7.3 Farkındalık
4 Kuruluşun Yapısı	7.4 İletişim
4.1 Kuruluşu ve yapısını anlama	7.5 Dokümante Bilgi
4.2 İlgili tarafların ihtiyaç ve beklentilerini anlamak	**8 Operasyon**
4.3 Bilgi Güvenliği Yönetim Sistemi kapsamının belirlenmesi	8.1 Operasyonel planlama ve kontrol
	8.2 Bilgi güvenliği risk değerlendirmesi
4.4 Bilgi Güvenliği Yönetim Sistemi	8.3 Bilgi güvenliği risk işleme
5 Liderlik	**9 Performans değerlendirme**
5.1 Liderlik ve taahhüt	9.1 İzleme, ölçme, analiz ve değerlendirme
5.2 Politika	9.2 İç denetim
5.3 Görev, sorumluluk ve yetki	9.3 Yönetimin gözden geçirmesi
6 Planlama	**10 İyileştirme**
6.1 Risklere ve Fırsatlara Yönelik Eylemler	10.1 Uygunsuzluk ve düzeltici faaliyet
6.2 Bilgi Güvenliği Hedefleri ve Planlama	10.2 Sürekli iyileştirme

Şekil 3.6 ISO 27001 standart maddeler

Ek- A maddeler

Ek- A maddeleri, Standart Maddelere nazaran daha spesifik daha kendine özgü maddeler barındırır. Ek- A maddeleri içerisinden ihtiyaca bağlı seçimler yapılır. Kurum kendi donanımına ve faaliyet alanına uygun olan maddelerle ilgilenir. Aşağıda şekil 3. 7 de başlıklar halinde sıralanmıştır.

A.5 Bilgi güvenliği politikaları
A.6 Bilgi güvenliği organizasyonu
A.7 İnsan kaynakları güvenliği
A.8 Varlık yönetimi
A.9 Erişim kontrolü
A.10 Kriptografi
A.11 Fiziksel ve çevresel güvenlik
A.12 İşletim güvenliği
A.13 Haberleşme güvenliği
A.14 Sistem temini, geliştirme ve bakımı
A.15 Tedarikçi ilişkileri
A.16 Bilgi güvenliği ihlal olayı yönetimi
A.17 İş sürekliliği yönetiminin bilgi güvenliği hususları
A.18 Uyum

Şekil 3.7. ISO/IEC 27001 Ek- A kontrol maddeleri

3.2.4. ISO/IEC 27001 standardı' nın kuruma katkıları

- Kurum güvenlik politikalarını ve bağlı olarak bilgi güvenliğini yönetir
- Bilgi varlıklarının farkına varılıp korunmasını sağlar.
- Kurumsal bilgi varlıklarının uygun bir şekilde korunmasını temin eder ve bu sayede, şirketin iş, zaman, para ve itibar kayıplarının önüne geçer.
- Bilgi kaynakları denetimi vasıtasıyla bilginin, gizlilik, erişilebilirlik ve bütünlüğünün korunması sayesinde bilgi güvenliğini sağlar.
- Tehdit ve riskleri en aza indirerek iş sürekliliğini sağlar.
- Kanun ve yönetmeliklere uyum sayesinde kurumu olası hukuki yaptırımlara karşı korur.

- Kurumun, çalışanlarının ve birlikte iş yapılan üçüncü tarafların güvenlik risklerini minimuma indirir.
- Eğitim ve sözleşmeler ile personel, yönetici ve üçüncü tarafların bilgi güvenliği farkındalıklarını arttırır.
- Kurumum itibarını yükseltip piyasada rekabet avantajı sağlar.
- Geliştirilen güvenlik politikaları sayesinde, sistemlerin kötü amaçlar için kullanımını ve suiistimalleri engeller.
- İş sürekliliğini sağlamak için oluşturulan kontroller ile kurumun iş ve finans zararını minimize eder.
- Kurumun iç-dış tehditlerden zarar görme risklerini, bilgi güvenliği ihlal olaylarını doğru yöneterek minimize eder (Yılmaz, 2014).

3.3. Bilgi Güvenliği Yönetim Sistemi

BGYS, kurumların kritik önemi haiz bilgilerini muhafaza edebilmek için hazırlanan sistematik bir yaklaşımdır. Kritik bilginin muhafazası BGYS nin en temel amaçlarındandır. Bu sistem çalışanları, iş süreçlerini ve BT sistemlerini kapsar (Önel ve Dinçkan, 2007).

3.3.1. Bilgi güvenliği yönetim sistemi kavramı

BGYS, kurumlarda bilgi güvenliği yapısını kurmak, gerçekleştirmek, işletmek, takibini sağlamak, gözden geçirmek, sürdürmek ve geliştirmek adına, iş riski yaklaşımına dayalı yönetim sistemi bütününün bir parçasıdır. BGYS' nin kurulmasıyla; uygun yöntemlerin ortaya konması, olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, örgütsel yapılar kurulması ve donanım/yazılım fonksiyonlarının sağlanması gibi bir dizi denetimin birbiriyle işbirliği içerisinde gerçekleştirilmesi anlamına gelmektedir.

BGYS için gereklilikleri belirten standart olan ISO/IEC 27001'in ana teması, kurumun hassas bilgilerinin yönetilmesini sağlamak ve etkili bir bilgi güvenliği elde etmek için yönetim sistem süreçlerinin oluşturulması, gerçekleştirilmesi ve sürdürülebilirliğinin sağlanmasıdır. Ayrıca farklı büyüklüklerdeki kurumlara uygulanabilecek biçimde tasarlanmıştır. Söz konusu standart, kurumun sahip olduğu teknolojik olanaklar ve bunların güvenliğine bağlı olarak hareket etmez. Bu yönüyle de ISO/IEC 27001 teknik ve teknoloji

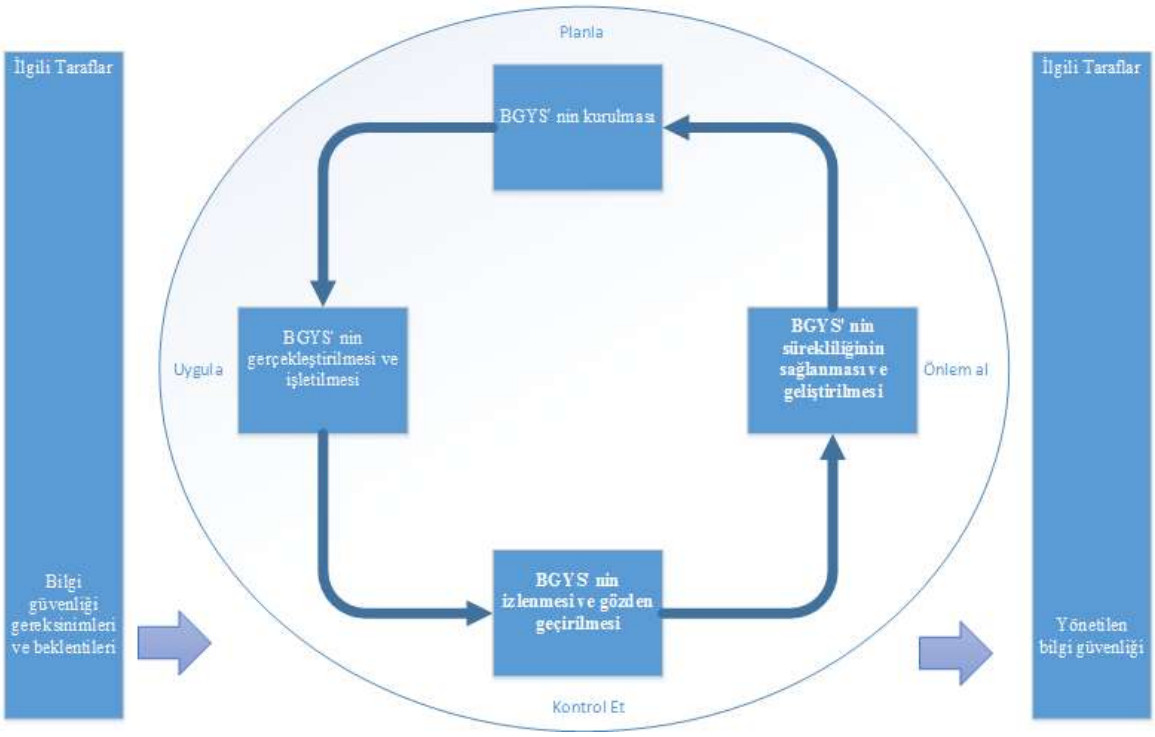
bağımlı bir standart değil, asıl ilgi alanı bilginin güvenliği olan bir standarttır (Bingöl, 2010).

3.3.2. Bilgi güvenliği yönetim sisteminde süreç yaklaşımı

BGYS sürekli devinim halinde olması gereken aktif bir süreçtir. Ayrıca diğer Kalite Yönetim sistemi standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirilmesinden ötürü ISO/IEC 27001 standardı planla-uygula-kontrol et-önlem al (PUKÖ) döngüsünü benimsemiştir. Bu standart ile beraber hayata geçirilecek bütün faaliyetler bir süreç olarak ele alınmaktadır. Bu süreçlere yapılan girdilerle elde edilen veriler ile süreç sonucunda çıktılar peyda olmaktadır. Ayrıca bir sürecin çıktısı diğer sürecin girdisi vazifesini görmektedir. Bir kurum dâhilinde, tanımları ve yönetişimleriyle beraber süreçlerin meydana getirdiği bir sistem uygulaması "süreç yaklaşımı" olarak ifade edilebilir. Süreç Yaklaşımı, kullanıcılarına aşağıda yer verilen konuların önemini işaret eder:

a) Bilgi güvenliği ihtiyaçlarını ve bilgi güvenliği için prosedürlerin ve stratejilerin belirlenmesi gereksinimini anlamak,
b) Kurum bünyesinde ki tüm riskleri yönetmek amacıyla, kurumun bilgi güvenliği risklerini yönetmek için gereken denetimleri yapmak ve sürekliliğini sağlamak,
c) BGYS' nin performansı ve verimliliğini takip etmek ve sürekliliğini sağlamak,
d) Objektif ölçümler ekseninde sürekli gelişimi sağlamak (Bingöl, 2010).

PUKÖ modelini görsel olarak anlatan Şekil 3. 8. de bir BGYS' nin bilgi güvenliği gereksinimlerini ve üçüncü tarafların beklentilerini girdi olarak nasıl ele aldığı ve gerekli aksiyon ve süreçler vesilesiyle, bu gereksinimleri ve beklentileri tatmin edecek bilgi güvenliği neticelerini nasıl ürettiği gösterilmektedir (Önel ve Dinçkan, 2007).



Şekil 3.8 PUKÖ döngüsü (Önel ve Dinçkan, 2007)

Planla (BGYS' nin kurulması): BGYS politikasının ve süreçlerin hazırlanması

Uygula (BGYS' nin gerçekleştirilmesi ve işletilmesi): Hazırlanan politikaların uygulanması, süreçlerin gerçekleştirilmesi

Kontrol et (BGYS' nin izlenmesi ve gözden geçirilmesi): BGYS politikası ve süreç performansının değerlendirilmesi, uygulanabilen alanlarda ölçülmesi ve neticelerinin raporlanması

Önlem al (BGYS' nin sürekliliğinin sağlanması ve iyileştirilmesi): Yönetimin değerlendirme sonuçlarına göre, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi

Bilgi güvenliği yönetiminin belirli bir aralıkta yerine getirilmesi gereken kurallar bütünü olarak ele almak hatalı olur. Sürekli kendini yenileyen bir gelişim süreci olarak ele alınmalıdır. PUKÖ modelinde gösterildiği gibi planla, uygula, kontrol et ve önlem al faaliyetleri bir döngü olarak devam etmelidir. PUKÖ modeli esas olarak ne yapılacağının net bir şekilde ortaya konması, alınan kararların hayata geçirilmesi ve çalıştığının temin edilmesi hedefine uygun olmayan kontroller için tedbirlerin alınmasıdır.

3.3.3. Bilgi güvenliği yönetim sistemine dair yanlış algılamalar

Göreceli olarak yeni addedilen BGYS hakkında gerek kamu gerekse özel sektörde işlevselliği engelleyen bir takım yanlış algılar mevcuttur. Çizelge 3.3' de gösterilen yanlış algıların tespit edilip olması gereken bakış açısı kurum personeline kazandırıldığında yalnızca bilgi işlem farkındalığının kuruma nüfuz etmesine katkı sağlanmakla kalmayıp BGYS' nin verimliliğini teminat altına alacaktır.

Çizelge 3.3. BGYS ile ilgili yanlış algılar (Marttin ve Pehlivan, 2010).

BGYS' ye dair yanlış algılar	İdeal bakış açısı
1) BGYS' nin kapsamı Bilgi İşlem birimleridir.	1) BGYS, kurumu bir bütün olarak ele alır.
2) BGYS' yi kurma ve yürütme sorumluluğu Bilgi İşlem birimi başkanına aittir.	2) BGYS' ni kurma ve yürütme görevi kurumun en üst düzey yöneticisine aittir.
3) BGYS bir bilgi teknoloji sürecidir.	3) BGYS bilgi güvenliği sürecidir.
4) BGYS yalnızca bilgi işlem birimleri ile bağlantısı vardır.	4) BGYS kurum bütün birimleri ile bağlantılıdır.
5) BGYS yazılım/ servis/ donanım tedarik sürecidir.	5) BGYS kapsamında yazılım/ servis/ donanım tedarik işlemi gerçekleştirilebilir.
6) BGYS dış hizmet olarak satın alınabilir.	6) BGYS danışmanlık hizmeti olarak edinilebilir. Ancak kurulumunu ve sürekliliğini sağlamak kurumun kendisine ait bir sorumluluktur.

4. ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNE KURUMSAL GEÇİŞ

Bilgi güvenliği kurumsal olarak ele alınıp değerlendirilmezse engellerden kaçınma konusunda zafiyet yaşanması kaçınılmaz olur. Zira bilgi güvenliği yönetimi sadece anti virüs yazılımları, güvenlik duvarları gibi teknik önlemlere endekslenemeyecek kadar karmaşık ve sebep olabileceği maddi manevi kayıplar itibarıyla azımsanamayacak kadar ehemmiyetli bir kavramdır. Risklerin en aza indirgenmesi, kritik bilgilerin muhafazası ve iş sürekliliğinin sağlanması BGYS' nin kurumlarda sürdürülebilir bir şekilde işletilmesiyle sağlanabilir. BGYS' nin hayata geçirilmesi için güvenlik komisyonlarının kurulması, güvenlik politikasının oluşturulması, uygun risk analiz yaklaşım yönetiminin seçilmesi ve kullanımı, dokümanların oluşturulması gerekmektedir.

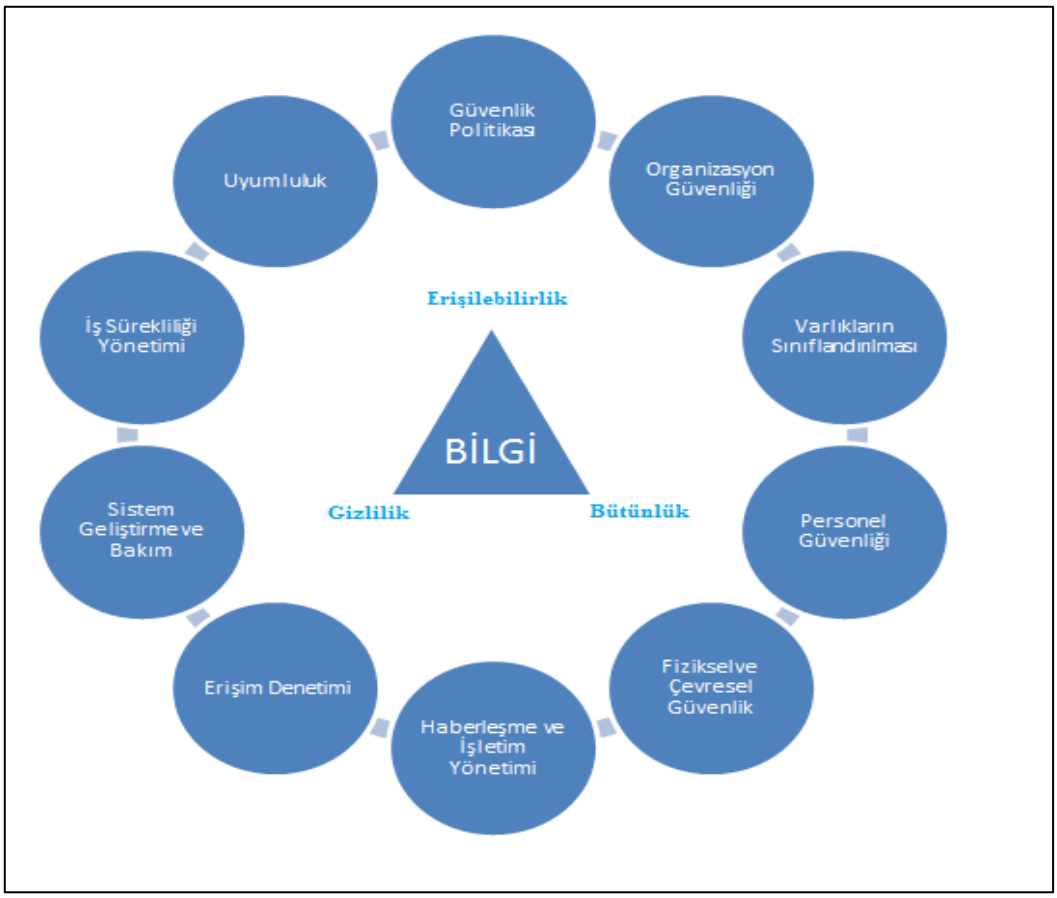
İnsan, bilişim, teknoloji farkındalık gibi pek çok değişkenin etkilediği kurumsal bilgi güvenliği girift süreçlerden oluşmaktadır. Kurumlarda gerçekleşen bilgi güvenliği problemleri incelendiğinde üst yönetimden alt kademeye kadar kurum bünyesinde görevli herhangi bir personelin bu tür zafiyetlere sebep olabildiği gözlemlenmektedir. Tüm kurum teşkilatına nüfuz eden, olmuş ve olası muhtemel bütün riskleri göz önünde bulundurarak adeta bir yaşam tarzı şeklinde benimsenmesi gereken BGYS için uluslararası geçerliliği olan ISO/IEC 27001 en temel başvuru kaynağıdır. ISO/IEC 27002 ise ISO/IEC 27001 ile ilgili olası ihtiyaçların karşılanması konusunda rehberlik sağlayan bir standarttır (Sagıroğlu ve diğerleri, 2007).

4.1. TS ISO/IEC 27002 Bilgi Güvenlik Yönetim Sistemi Gereksinimleri

Güvenlik altyapısının vaz geçilmez unsurlarından olan yönetsel tedbirler, teknoloji uygulamaları ve farkındalık süreçleri bir bütün değerlendirilmelidir. Teknolojik açıdan üst seviyede olan bir kurum farkındalık geliştirme konusunda sınıfta kaldıysa bilgi güvenliğinde başarıyı yakalayamaz. Nitekim günümüzde yaşanan bilgi güvenliği aksaklıklarının büyük çoğunluğu personel kaynaklıdır. Yani bu üç alandan yalnızca birinde üst seviyeleri yakalamak hiçbir şey ifade etmeyebilir. Birlikte işletilmelerinden ortaya çıkacak olan sinerji ortaya çıkması muhtemel tüm tehditlere karşı ön savunma mekanizması geliştirecektir.

Yönetsel önlemler, hazırlanan plan ve prosedür doğrultusunda güvenlik yönetiminin icra edilmesi olarak ifade edilebilir. Hazırlanan plan ve prosedürlerin yazılı hale getirilmesi hayati önem arz etmektedir. Çünkü yazılı olmayan kuralların uygulanması ve tekrarlanması çok mümkün gözükmemektedir. Bilgi güvenliği sağlanmasında her işte olduğu gibi en temel unsur uygulanabilir planlar, gerçekleştirilebilir hedefler ve üst yönetimin sergileyeceği iradedir.

Bilgi güvenliğinde başat olarak nitelendirilen ISO/IEC 27001 standardı ve bu standardın gereksinimlerine yer veren ISO/IEC 27002 standardı birbirinden farklı ama birbiriyle oldukça ilişkili iki standarttır. İki standart arasındaki ilişki şekil 4.1' de görüldüğü gibi ISO/IEC 27002 bilgi güvenliğinin sağlanması hususunda ihtiyaç duyulan temel gereksinimlere yer verirken, ISO/IEC 27001 ise bilgi güvenliğinin temel esaslarından olan bilginin gizliliği, erişilebilirliği ve bütünlüğünü kapsayan bir BGYS' nin kurulumunu hedefler (Kahraman, 2006).



Şekil 4.1. ISO/IEC 27002 ile ISO/IEC 27001 arasındaki ilişki (Kahraman, 2006)

4.1.1. Güvenlik politikası

Tüm prensiplerde ve uygulamalarda olduğu gibi bir sistem işletilmeye çalışıldığında önce üst kadronun ikna edilmesi ve sürece dâhil edilmesi gerekmektedir. Güvenlik politikasının varoluş amacı da yönetimin bilgi güvenliği farkındalığı oluşturmasına katkı sağlamak yönetimi bilgi güvenliği konusunda ne kadar ciddi olduğunu tüm kuruma ifade etmektir. Çünkü yazılı bir politika hazırlandığında bunun görüşülüp karara varılmış bir politika olduğu başta üst yönetim olmakla birlikte tüm personelce kabul edilir.

Güvenlik politikası tabiri caizse kurumun bilgi güvenliği manifestosu olarak ifade edilebilir. Kurumun bilgi güvenliğine olan ihtiyacını ve bilgi güvenliğine dair kavramları bilgi varlıklarını kullanan bütün personele duyurma amacını güden güvenlik politikası, kurumun iş gereksinimleriyle ortaya çıkabilir veya yasal zorunluluklar dolayısıyla hazırlanmış olabilir. Tasarlanan güvenlik politikasında hazırlanış nedenlerine, kanun maddeleriyle yahut iş gereksinimleri itibarıyla detaylı bir şekilde yer verilmelidir (Öztürk, 2008).

Güvenlik politikasında yer alması gereken unsurlara genel olarak yer vermek gerekirse (Öztürk, 2008):

Bilgi güvenliği tanımı

Bilgi güvenliği politikası kurumun tamamını ilgilendiren bir husus olduğundan kurumun geneline hitap etmesi gerekir. Bilgi güvenliğiyle ilgili uluslararası düzeyde yıllardır çalışma yapılsa da Türkiye' de çok da bilinen bir kavram değildir. Bu sebepten ötürü bilgi güvenliğinin sağlanması amacıyla hazırlanan bir güvenlik politikasında bütün çalışanların anlayacağı basitlikte bilgi güvenliği tanımına yer verilmesi gerekmektedir.

Bilgi güvenliği ihtiyacı ve kapsamı

İnsanlar uygulaması gereken kuralların hiçbir amaca hizmet etmediğini düşündüğü zaman o kurala riayet etme kapasiteleri düşer. Herhangi bir zorlukla karşılaştıkları zaman uygulamaktan hemen vazgeçerler. Dolayısıyla çalışanlardan bir güvenlik politikasını benimsemelerini talep etmeden önce bu güvenlik politikasına kurumun neden ihtiyaç

duyduğunu açık bir şekilde tanımlamak önem arz etmektedir. Çalışanların uygulayacakları prensiplerin sebebini öğrenmeleri kadar prensiplerin kapsamını, ilgilendirdiği alanları ve kapsam dışı bırakılan alanları da öğrenmeleri ehemmiyetlidir. Örneğin: '' *İş bu güvenlik politikası Bilgi İşlem altyapısını kullanan tüm personeli, bilgi işlem verilerine erişen üçüncü taraf kullanıcıları ve dış hizmet sağlanan kurumlar arasından bilgi işlem verilerine erişen kullanıcıları kapsamaktadır* '' .

Bilgi güvenliği hedefleri

Kurumun uzun vadeli stratejileriyle ilişkilendirilmiş bir BGYS kurulumunun varmak istediği amacı ve hedefi hakkında personeli bilgilendirmek için bilgi güvenliği hedeflerine yer verilmesi gerekmektedir. Örneğin: ''*Kurumun imajını ve temsil ettiği makamın itibarını korumak, üçüncü tarafla gerçekleştirilen sözleşmelerin gerekliliklerini sağlamak ve temel faaliyet alanlarının kesintisiz şeklide işletilmesini temin etmek amacıyla kurumun sahip olduğu bütün bilgi varlıklarının güvenliğini sağlamayı hedefliyoruz* ''

Risk yönetim çerçevesi

Sahip olunan bilgi güvenliği risklerinin yönetimi önemli bir husustur. Risklerin en aza indirgenmesi şirketin uzun vadeli hedeflerine güvenle ulaşabilmesi için gereklidir. Bu bağlamda güvenlik politikasında nasıl bir risk yönetiminin benimsendiğine yer verilmesi gerekmektedir. Örneğin: '' *Kurum yönetimi kurumumuzun sahip olduğu risklerini yönetmek için bilgi güvenliği risklerinin ortaya konması, analizi ve en alt seviyeye indirgenmesi gerekmektedir*. ''

Yönetimin bilgi güvenliğini sağlama sözü ve politika dokümanının onayı

Kurum üst yönetiminin bilgi güvenliği sağlanmasında ve sürdürülmesindeki önemli rolüne tezin önceki kısımlarında değinilmişti. Üst yönetimin bilgi güvenliğini sağlama konusundaki azim ve kararlılığı başarıya ulaşmada hayati önem arz etmektedir. Bu bağlamda güvenlik politikasında sembolik de olsa bilgi güvenliğinin sağlanmasında her türlü desteğin verileceğine dair ifadeye yer vermelidir. Örneğin: '' *Yönetim birimi olarak bilgi güvenliğinin sağlanması adına hazırlanan bu güvenlik politikasına riayet öneminin*

altını çizerken, kontrolünün yapılmasının ve ihlal durumlarında gerekli yaptırımların icra edilmesinin yönetim tarafından desteklendiğini beyan ederim ''.

Bilgi güvenliği ilkeleri

Kurum içerisinde bilgi güvenliğinin takibi için gerekli olan prensipler olarak adlandırılabilir. Kurum çalışanlarından beklenen davranışlar bütünüdür. Örneğin: '' *Kurum personeli iletişim kaynaklarını kullanırken kuruma ait verilerin gizliliğini sağlamakla, işlediği bilgileri yedeklemekle, bilgi güvenliği ihlal olaylarını raporlamakla ve bu ihlalleri önleyecek tedbirleri almakla mükelleftir. Ayrıca kurum içi bilgi kaynakları 3. kişilerle paylaşılamaz ve bilişim kaynakları TC yasalarına aykırı faaliyetler icra etmek için kullanılamaz.* ''

Roller ve sorumluluklar

Bir amacı olan kurum veya kuruluşta görevli her bireyin üstüne düşen vazifeye rol denir. Bilgi güvenliği konusunda da tüm personelin üzerine düşen roller vardır. Üzerine düşen rol ve görevleri yerine getirirken gerçekleştirilmesi gereken faaliyetler ve ortaya çıkan sonuçları kabul etmek ise tüm kurum personelinin sorumluluğudur. Örnek verilmek istenirse '' *Her bir kurum personeli ve üçüncü taraf bu politikaya ve bu politikanın kapsadığı prosedür ve talimatlara uymakla yükümlüdür. Birim sorumlularından müteşekkil Güvenlik Komisyon Kurulu bilgi güvenliği alt yapısını desteklemek ve sürdürülebilirliğini temin etmekle yükümlüdür.* ''

Politikanın ihlali ve yaptırımlar

Üst yönetim tarafından kurum stratejileri doğrultusunda hazırlanan güvenlik politikası ihlal edildiğinde, ihlal eden kullanıcıya yönelik yaptırımlar uygulanmalıdır. Bu yaptırımlar kurum personelinin anlayabileceği şekilde güvenlik politikasında yer almalıdır. Örneğin: '' *Güvenlik politikasında yer verilen görev ve sorumlulukların ihlali durumunda Personel Yönetmeliği icabınca uyarma, kınama, para cezası veya sözleşme feshi yaptırımlarından bir veya birkaçı kurum yönetimince uygulanabilir*.''

Atıflar (Diğer prosedür, standart ve süreçlere atıflar)

Kurumların, bilhassa uluslararası ticari ilişkileri bulunanların kendi içlerinde uyması gerekli olan kurallardan olduğu kadar alışveriş içerisinde bulunduğu çevrelerin uyması gereken kanun, yönetmelik ve standartlardan da haberdar olmalı ve kendi dokümanlarını hazırlarken gerekli alanlara atıfta bulunmalıdır. Örneğin: '' *Kalite güvence prosedürü, iş sürekliliği ve olağanüstü durum planı, bt risk yönetimi politikası ve taktik plan yönetimi prosedürü bu politikayı destekler.*''

Bilgi güvenliği politikası gözden geçirme kuralları

İnsanlar tarafından hazırlanan hiçbir kural, kanun, prosedür kusursuz değildir. Gerek ilk aşamada gerek ilerleyen dönemlerde tekrar gözden geçirmeye üzerinde değişiklikler yapılmaya ihtiyaç duyabilir. Uygulanabilirlik ve sürdürülebilirlik açısından değerlendirilip gereken güncellemeler yapılmalıdır. Güvenlik politikası da bu gözden geçirilme ve güncellenme ihtiyacından müstağni değildir. Güvenlik politikasının kimler tarafından ne sıklıkla gözden geçirilip, güncelleneceği belirlenmeli ve bu dokümanda yer verilmelidir. Düzenli sıklıkla gerçekleştirilen gözden geçirmeler ve güncellemeler dışında yasal gereklilikler, teknolojik yenilikler dolayısıyla da güncelleme gerekliliği ortaya çıkabilir. Örnek vermek gerekirse: '' *Güvenlik politikası, güvenlik komisyon kurulunca düzenli olarak 6 ayda bir gözden geçirilir. Yönetmeliklerde yaşanan bir değişim veya bilgi güvenliği uygulama süreçlerindeki değişiklikler gereğince güvenlik politikasında güncelleme yapılabilir. Gözden geçirilen ve güncellenen politikanın Kurum Başkanınca onaylama işlemi yapılır.* ''

Güvelik politikasında yer alması gereken hususlar yukarıda zikredilmeye çalışılmıştır. Güvenlik politikasını hazırlarken içerik kadar önemli bir başka konu ise içeriğin okuyucuya nasıl sunulduğudur. Halk arasında meşhur bir söz vardır '' *ne kadar bilirsen bil, anlattıkların karşındakinin anlayabildiği kadardır.*'' Bu bağlamda güvenlik politikasının personelde kalıcı bir etki oluşturabilmesi için dikkat edilmesi gereken bazı özellikleri vardır (Öztürk, 2008).

- Politikanın mümkün oldukça kısa olması gerekmektedir. Zira uzun bildiriler, beyanatlar sıkıcı bulunup okunmayabilirler. Kelimeler tasarruflu kullanılmalı okuyucuya kısa ve net ifadelerle anlatılmak istenenler aktarılmalıdır.
- Karmaşık teknik terimlerden uzak durmaya çaba sarf edilmelidir. Kurumun her biriminden çalışanların okuyacağı hatırda tutularak anlaşılır bir dil kullanılmalıdır.
- Güvenlik politikası gerçekçi ve ayakları yere basan bir politika olmalıdır. Personelin altından kalkamayacağı, uygulanması imkânsız ifadeler barındıran bir politikanın uzun ömürlü olmayacağı aşikârdır.

4.1.2. Organizasyon güvenliği

Kurum içerisinde bilgi güvenliğinin temin edilmesi için piyasanın eğilimlerinin takip edilmesi, hedeflerin gerçekleştirilmesi için diğer standartları ve kanunları izlemek güvenlik konularıyla ilgili bağlantının kurulması için kurum dışı uzmanlarla irtibat sağlanmalıdır. Organizasyon güvenliğinin sağlanması için bina edilmesi gereken 3 sistem vardır (Kahraman, 2006).

Bilgi güvenliği altyapısı

Süreç yönetiminin sağlıklı sürdürülebilmesi adına görev ve sorumluluklar açıkça belirlenmelidir. Bilgi güvenliği altyapısı oluşturulurken dikkat edilmesi gereken hususların ilki bilgi güvenlik ekibi yahut bilgi güvenlik takımı kurulmasıdır. Bu sorumluluğu üstüne alacak ve atılması gereken adımların takibatını yapacak bir ekip kurulması mühim bir konudur. Yönetim, kurum içinde bu tür bir ekibi lüzumsuz bulursa dışardan danışmanlık hizmeti de satın alabilir. Bu ekibin erişim yetkisi yüksek olmalı olay anında müdahale kapasitesi daraltılamamalıdır. Bu ekibin görevlerini sıralayacak olursak;

- Proje hazırlama,
- Hazırlanan projelerin dokümante edilmesi ve raporlanması,
- Güvenlik politikasının kurum ilkeleri çerçevesinde hazırlanması,
- Politikaların ve bunlara bağlı alt politikaların tasarlanması,
- Personel taleplerinin değerlendirilmesi ve bu bağlamda güncellemeler yapılması,
- Kurum bölümlerinin bilgi işlem zafiyetlerinin takibi,
- Eğitim ve farkındalık çalışmalarını hazırlanması,

- Varlıkların tespit edilmesi, tasnifi, iş süreklilik planlarının hazırlanması

Üçüncü taraf erişiminin güvenliği

Üçüncü tarafla irtibat halinde olan kurumlarda her zaman bilgi güvenliği riski mevcuttur. Veri paylaşımı konusunda tedbirli olunmalı, bu duruş sözleşmelerle desteklenmelidir. Sözleşmeler vasıtasıyla bir denetim mekanizması oluşturulmalıdır. Erişimin biçimini, paylaşılan bilginin önemini, üçüncü tarafça tercih edilen güvenlik sistemlerini haiz bir güvenlik sözleşmesinin varlığı zaruridir.

Dışarıdan kaynak sağlama

Bilgi güvenliğini idame ettirmek için bazı durumlarda dışarıdan kaynak sağlama yöntemine başvurulabilir. BGYS için dış kaynağa başvuran kurumların ilke ve standartları ilgili taraflarca hazırlanmış ve kabul edilmiş bir sözleşmede detaylı bir şekilde yer almalıdır.

4.1.3. Varlıkların sınıflandırılması (Envanter oluşturulması)

Bilgi güvenliğinin sağlanması hususunda kilometre taşlarından birisi varlıkların sınıflandırılması yahut varlık envanterinin oluşturulmasıdır. BGYS her kurum için değişken olan kendini yenileyen içinde bulunduğu duruma göre şekil alan pragmatik bir sistemdir. Her ne kadar değişmeyen temel güvenlik unsurlarını haiz ise de BGYS üzerine en çok zaman ve emek harcanan kısmı kurumdan kuruma değişkenlik arz eder. Yani her kurumun kendine has bir BGYS' si vardır. Kurumda BGYS' yi kurmakla görevli olan birim veya danışmanlık firmasının üzerine BGYS' yi bina edeceği temel değer varlık envanteridir.

Varlık envanteri tabiri caizse kurumun tam kapsamlı check- up sonucudur. Kurumun sahip olduğu yahut olmadığı unsurlar, yedeklenmesi gereken donanımlar, riskli bilgiler ihtiva eden yazılımların tespit edilmesini sağlar. Ayrıca hangi dokümanın yanlış ellere geçtiğinde telafi edilemez sonuçlara yol açabileceği, hangi birimlere hangi personelin girebileceği yine sağlıklı hazırlanmış bir varlık envanteri ile tespit edilir. BGYS danışmanı doktora benzetilirse, reçete yazmak için gerek verileri yani MR sonucunu, varlık envanteri olarak adlandırmak hatalı olmaz (Koç, 2008).

Varlık envanteri faaliyetlerine değinmeden önce ifade edilmesi gereken temel kavramlar (Koç, 2008):

Varlık: Kurumun kuruluş amacını gerçekleştirmek için ihtiyaç duyduğu ve bu sebepten ötürü değerli olan bütün şeylerdir. Firmanın değerli addettiği bütün unsurları haizdir. Örnek olarak yazılım, donanım, bilgi ve insan verilebilir. Bu örnekler arasında en soyut olan kavram bilgidir. Firmada neredeyse her yerde bulunabilen bilgiyi, donanım ve yazılımlar işlerken depolama üniteleri depolar. Çalışanların zihinlerinde ve konuşmalarında dahi kendine yer bulur. Varlık kategorisinde yer alan tanımlar:

- Bilgi varlıkları: Kurumun kütüphanelerinde, donanımlarında, bilgi sistemlerinde muhafaza edilen ve kurumun iş süreçlerinde farklı şekillerde yer alan veridir
- Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları
- Fiziksel varlıklar: Bilgisayar ekipmanları (kasa, ekranlar, diz üstü bilgisayarlar), iletişim ekipmanları(yönlendirici, faks, telsiz), manyetik kayıt ortamları(kartuş, cd, flash disk), diğer teknik ekipmanlar(güç kaynakları, adaptör, havalandırma üniteleri), mobilya, yerleşim düzeni
- Servisler: Bilgi işleme ve haberleşme servisleri (web servisi, e- ticaret servisi, ftp servisi), ışıklandırma, havalandırma, ısınma
- İnsan: Personel de kurumun bir varlığı olarak adlandırılabilir. Genellikle 5 tanımın varlığı kabul edilir ancak bazı otoriteler ek bir kategori daha tanımlar
- Soyut varlıklar (Şen ve Yerlikaya, 2013): Kurumun piyasadaki itibarı ve imajı

Varlık sahibi: Bir varlığın gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanmasında sorumluluk sahibi olan kişidir. Örneğin: kurum pazarlama bilgilerinin sahibi olan pazarlama bölümü müdürü. Varlık sahibinin diğer görevleri ise varlık değerinin belirlenmesi ve varlık risk değerlemesinin yapılmasıdır

Varlık Emanetçisi: Varlığın sürekliliğinin sağlanmasına katkıda bulunan kişidir. Varlık sahibinden farklı kişilerdir. Örneğin: Kurum pazarlama bilgilerinin sahibi pazarlama bölüm müdürü iken emanetçisi ilgili veri tabanı yöneticisidir.

Varlık envanteri oluşturma

Risk analizi sürecinin vazgeçilmez unsurlarından birisi varlıkların muayyen hale getirilmesi ve varlıklara değer atfedilmesi kısaca varlık envanterinin hazırlanmasıdır. Zimmet listesi başlangıç için tercihe şayan olabilir ancak envanter listesi zimmet listesiyle kıyaslanmayacak ölçüde kapsamlı bir dokümandır. Varlık envanteri hazırlamadan evvel varlık yönetim prosedürü hazırlanması gerekebilir. Zira envantere eklenecek veya çıkarılacak bir varlık söz konusu olduğunda kümülatif listeye ihtiyaç duyulur.

Liste oluşturulurken dikkat edilmesi gereken ilk husus varlıkları gruplandırmaktır. Çünkü tüm varlık maddeleri alt alta yazıldığında istenilen varlık maddesinde ulaşmak zorlaşırken hangi varlık değerli hangi varlık riskli tespiti güç hale gelecektir. Bilgi varlıkları, yazılımsal varlıklar, fiziksel varlıklar hizmetler en yaygın gruplandırma tekniğidir.

Bilgi varlıkları varlık envanteri için tespit edilmesi gereken ilk varlık grubudur. Bu kayıt yapıldıktan sonra bu varlığın saklandığı ortamların hemen envantere kaydedilmesi gerekmektedir. Envanterin sağlıklı oluşturulması ve kullanım verimliliği açısından önemli bir işlemdir.

İkinci olarak süreç varlıklarının belirlenmesi gerekmektedir. Her organizasyon farklı bir birey gibi düşünüldüğünde her organizasyonun kendine has birçok süreci bulunabilmektedir. Tüm süreçler BGYS kapsamında değerlendirilemeyeceğinden ele geçirilmesi ve değiştirilmemesi gereken bilgileri haiz süreçler yahut iş sürekliliğini ve firma itibarını etkileyebilecek süreçler envanter listesinde alınabilir (örneğin sistem ağı, sarf malzemeleri).

Varlık envanteri bir tabloda toplanabileceği gibi birden çok tabloya da ihtiyaç duyulabilir. Varlık sayısı çok yüksekse varlıklar yazılım, fiziksel, bilgi gibi ayrı ayrı envanterlerde tutulmasında fayda vardır.

Varlık envanteri, muhtemel bir felaket senaryosunda kurtarılması veya geri kazanılması gereken varlıkların detaylarını kapsamalıdır(örneğin varlık tipi, bulunduğu yer, yedek bilgileri, lisans bilgileri, formatı ve ticari bilgileri).

Varlık envanterinde yer alması gereken bilgilere aşağıda yer verilmiştir:

Varlık: Varlığın adının yazdığı bölümdür. Varlıkları birbirinden ayırt etmek için gereklidir.

Varlık grubu: Varlık envanterinin daha verimli kullanılabilmesini sağlamak için varlıklar gruplandırılabilir. Benzer görevi icra eden varlıkları benzer gruplara alınabileceği gibi iş süreçleri kapsamında bir gruplandırma yapılabilir.

Varlık sahibi: Varlık sahibi tanımlanan görev ve sorumluluklar ekseninde belirlenir. (Pazarlama Bölümü Müdürü)

Emanetçi: Varlığın emanetçisi tanımlanır. (Örneğin: Sistem Yöneticisi)

Bulunduğu yer: Varlığın bulunduğu fiziksel yeri belirtir.

Gizlilik Değeri: Varlığın yetkisiz kişilere geçmesi halinde ortaya çıkacak zarar ifade edilir.

Bütünlük Değeri: Varlığın bütünlüğüne halel gelmesi halinde ortaya çıkacak zarar belirtilir.

Erişilebilirlik Değeri: Varlığın erişilebilirlik değerinin ifade edilmesi gerekir.

Değer: Gizlilik, bütünlük ve erişilebilirlik değerleri harmanlanarak belirlenebilecek bir değerdir.

Varlığın Eklenme Tarihi: Varlığın edinilme ve kurum bünyesine alınma tarihidir. Risk analizi seçiminde kullanılabilir.

Açıklama: Varlıkla ilgili belirtilmesi gereken ek hususlar bu kısımda belirtilir (Koç, 2008).

Çizelge 4.1’ de örnek bir varlık envanteri verilmiştir.

Çizelge 4.1. Varlık envanteri (Koç, 2008)

Sıra No	Varlık Grubu	Varlık	Kategori	Varlık Emanetçisi	Gizlilik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	Değer	Varlığın Eklenme Tarihi	Açıklama
1										
2										
3										

Sınıflandırma

Varlıkların envanterinin çıkarılmasına mukabil değerlendirilmesi risk analizi yapabilmek için gereken verilerin elde edilmesi açısından zaruridir. Varlıkların değerlendirilmesi konusunda hangi değerlendirme kıstasının tercih edileceği, kurumdan kuruma farklılık gösterir. Organizasyonlardaki varlıkların çeşitliliği değerlendirme metotlarını belirler. Değerlendirme metotları nitel ve nicel olarak ikiye ayrılır.

Nitel metotlardan örnek olarak ‘’Düşük, çok düşük, yüksek, çok yüksek’’ verilebilir. Derecelendirme seviyelerinin çeşitliliği organizasyonun ihtiyacına göre farklılık gösterir. Derecelendirmeye fazla ihtiyaç duymayan işletmeler düşük, orta, yüksek gibi temel derecelendirme seviyeleriyle yetinirken daha hassas bir ölçüye ihtiyaç duyan işletmeler çok yüksek, kritik veya ihmal edilebilir gibi kavramları tercih edebilirler. Derecelendirme metotlarında dikkat edilmesi gereken husus muğlak ifadelerden kaçınılmasıdır. Yani herhangi bir varlığın değeri ‘’ yüksek’’ olarak addedildiği zaman karşılığının net bir şekilde anlaşılması gerekmektedir.

Derecelendirme konusunda yaşanabilecek bir başka sorun hangi varlığın nitel hangi varlığın nicel metotlarla değerlendirileceği konusudur. Bir varlığa değer atfedilirken edinme maliyeti yahut üretim maliyetini temel unsur almak yanıltıcı olabilir zira üretim maliyeti 100 tl olan bir ürün veya donanım kötü niyetli kişilerce erişilebildiği takdirde firma adına ciddi maliyetlere sebep olabilmektedir. Bu tür varlıklar değerlendirilirken nitel metotlar tercihe şayan olmaktadır.

Varlık değerini hesaplarken kullanılan 3 değer vardır: Gizlilik, bütünlük, erişilebilirlik. Bazı varlıkların gizliliğinin temin edilmesi asıl gereklilik iken bazılarında bütünlük unsuru ağırlık verilmesi gereken özellik olabilir. Örneğin: Veri koruma kasası için erişilebilirliğin sağlanması bütünlüğün gizliliğin korunmasından daha elzemdir. Her organizasyon personel, çalışma ortamı, iş hacmi itibarıyla diğer firmalardan farklı olması hasebiyle varlık değerlendirme stratejileri de kendine özgü olmalıdır (Koç, 2008).

Varlık değerleme: Her birisi bir diğerinden farklı olan kurumların sahip olduğu varlıklar çok çeşitlidir. Kurumda çalışma alanına göre inşaat malzemeleri de bulunabilir, sağlık cihazları da bulunabilir. Muhasebe departmanından bir kişinin inşaat malzemeleriyle ilgili bir varlık değerlemesi yapması gerçekçi kabul edilemez. Her çalışan kendi işiyle ilgili varlıkların gizlilik değerini, taşıdığı riskleri, bütünlüğünün kaybedildiği kurumun uğrayacağı zararları daha iyi değerlendirir. Bu bağlamda varlık değerleme görevi o varlığın sahibi olarak adlandırılan çalışana aittir. Ancak varlık sahibinin kendisinin değerlemede güçlük çekeceği kadar varlığı varsa BGYS kurulundan destek alabilir.

Varlık değerlemesi yaparken hataya mahal vermemek ve öznel hareket etmemek için doğru bir metodolojinin tercih edilmesi gerekmektedir. Tercih edilen bu metodolojinin ilerleyen zamanlarda karışıklığa neden olamamak adına varlık sınıflandırma kılavuzunda muhafaza edilmesi gerekmektedir. Varlığın gizlilik, bütünlük ve erişilebilirliğinin doğru değerlendirilmesi için Şekil 4.2' den faydalanılabilir (Koç, 2008).

	Varlık Değerleri			
Güvenlik Hedefi	DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
GİZLİLİK	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkilemez /çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
BÜTÜNLÜK	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
ERİŞİLEBİLİRLİK	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Şekil 4.2. Varlığın değerleme tablosu (Koç, 2008)

Varlık Sınıflandırma: Bilginin paylaşımı ve güvenliği kurumların hayatını devam ettirebilmesi için ehemmiyetli bir husustur. Bilginin sadece kurumlar arası değil kurum için güvenliği de üzerinde durulması gereken bir husustur. BGYS' de hangi bilgiye hangi çalışanın ulaşacağı, bilginin sınıflandırması vasıtasıyla belirlenir. Bir varlığın korumasının nasıl sağlanacağı, hangi kullanıcının ne kadar erişebileceği, varlığın konumu gibi soruların cevabı varlık sınıflandırma değeri ile ortaya çıkar.

Sınıflandırma prosedürünün faydaları sıralanmak istenirse;

- Bilgi kaybından kaynaklanabilecek karlılık ve itibar kaybı riskini azaltacaktır.
- Kurumun ilişki içerisinde bulunduğu diğer kurumlara ait bilgilerin kaybı uzun vadede iş kaybına neden olabilecektir.
- Riskler makul şekilde yönetilirse kurumlar arası bilgi değişimi kolaylaşacaktır.

Bilgi etiketleme

Üst yönetimce görevlendirilen bir birimce elektronik ve yazılı ortamlardaki bilgilerin etiketlenmesi gerekmektedir. Bu konuyla ilgili prosedürlerin hazırlanmalı ve uygulamaya geçilmelidir.

Hazırlanacak prosedürde üzerinde durulması gereken aktiviteler şunlardır;

- Bilgiye erişim
- Kopyalama
- Depolama
- İletim (e- posta, telefon, faks vs.)
- Özellikle bilgisayar kullanılarak işlenen suçlarda kanıt olması için bütünlüğün ele alınması ve güvenlik vakalarının kayıt altına alınması
- İmha etme

Kurum genelinde tüm çalışanlar prosedür hakkında uygulama eğitimi almalıdırlar. Gerek elektronik gerekse fiziki mecrada mevcut bulunan varlıkların etiketlenmesine azami gayret edilmelidir. Uygulanması planlanan prosedür için bilgi sınıflandırma seviyeleri tanımlanmalı ve her aşama için alınan önlemler kayıt altına alınmalıdır. Bu bağlamda bilhassa elektronik mecralarda bulunan bilgi varlıkları için çalışanlar ihtiyaç duyulan tedbirleri almalı, sonrasında kurum çalışanının varlığı kullanmasına izin verilmelidir (Koç, 2008).

Bu tür dokümanlar, kılavuzlarda yahut diğer kaynaklarda yer alan varlık envanteri belirleme örnekleri bir tavsiye hükmündedir. Bu kılavuzların hazırlanış amacı BGYS kurulumunda kuruma ve ilgili departmana bakış açısı kazandırabilmek ve gerçekçi örnekler vererek kendine has olan varlık envanteri belirleme sistemini kazandırmaktır. Bir kurumda başarıya ulaşan sistemin benzer özelliklere sahip başka bir kurumda aynı sonuçlara ulaştırmasını beklemek hataya mahal verebilir. Çünkü kurumlarda insanlar gibidir sahip olduğu varlıklar, tehlikeler, eksiklikler bir diğerine tamamıyla benzemez. Bu yüzden her kurum varlığını nasıl belirleyeceğini bir uzmandan destek görmek vasıtasıyla kendisi belirlemelidir (Ersoy, 2012).

Varlık envanteri hazırlanırken yaşanabilecek sorunlar:

- Sahip olduğu varlıkların tespiti ve analizi yapılacak çalışanın iş yoğunluğu sebebiyle kendisiyle görüşememek,
- Personelin yaptığı işe ve kullandığı teçhizata karşı olan bilgisizliği,

- Bilgisizliğe bağlı olarak aynı işi yapan çalışanlarla yapılan görüşmede alınan farklı cevaplar
- Envanter hazırlama çalışmaları personel tarafından angarya olarak görülebilmesi ve çalışanların gerekli çabayı sarf etmemesi,
- Varlıklarda gerçekleşen yenilenmeler, eksilmeler, yıpranmalar, eklenmeler gibi sürekli dikkat ve gayret gerektiren değişiklikleri takip etmenin zorluğu bunlardan birkaçıdır (Ersoy, 2012).

4.1.4. Personel güvenliği

Bilgisayarlardan ve yazılımlardan farklı olarak hata yapmak üzere yaratılan insanoğlu bilgi güvenliğine dair yaşanan zafiyetlerin baş müsebbibidir. Kurumda personel hataları, hırsızlık, sahtekârlık ve araçların yanlış kullanımı gibi sebeplerle kurum bilgi güvenliği çalışanlarca riske atılabilir. Adı geçen risklerin önüne geçebilmek adına işe alımlarda personelin, sorumluluklarıyla ilgili yeterince bilgilendirilmesi gerekmektedir. Ayrıca personel sorumlulukları sözleşmelerde yer almalı ve muhtemel hatalara karşın çalışanlar gözlemlenmelidir. Bilgi işleme araçlarının kullanıcıları, üçüncü taraf kullanıcılar gizlilik sözleşmesi imzalamalıdırlar (Kahraman, 2006).

<u>İş tanımlarında güvenlik</u>

Kurum personel alımlarında personelin sorumlulukları arasında daha evvelden hazırlanan güvenlik politikası gereği güvenliğe dair konuların yer verilmesi hatta alım kıstasları arasında güvenlik maddeleri yer almalıdır.

Personelde gerek bilgi güvenliği farkındalığının oluşması gerekse bilgi güvenliği yaşam döngüsünün sağlanması adına personele güvenlik rolleri ve sorumlulukları atanmalı ve yazılı hale getirilmelidir. Bu sorumluluklar güvenlik politikasının hedef ve amaçlarını, belirli varlıkların güvenliklerini tesis etmek ve belirli güvenlik faaliyetlerinin icra edilmesi detaylarını içermelidir.

Sorumlulukların yazılı hale getirilmesine ek olarak işe alma koşul ve şartları da bu amaca hizmetkâr olmalıdırlar. Personel alım koşulları personelin bilgi güvenliğine dair sorumluluklarını ve bu sorumlulukları yerine getirmemesi halinde cezai müeyyidelerini

içermelidir. Ayrıca işe alırken güvenilir referanslar temel alınmalı ve özgeçmişin gerçeklemesi yapılmalıdır.

Kullanıcı eğitimi

Kurum personeli ve kurum bilgi varlıklarına erişimi olan üçüncü taraf kullanıcıları, hazırlanan politikalar ve prosedürlerle ilgili eğitim almalıdır. Söz konusu eğitimin kapsayacağı konular ise; yasal yükümlülükler, bilgi güvenliği farkındalığı, alanıyla ilgili risk başlıkları, şifre belirleme teknikleri, yazılım paketlerinin kullanılması, güvenlik gereksinimleridir.

Güvenlik saldırılarının saptanması

Kurumların sağanak bir şekilde siber saldırıya maruz kaldıkları günümüz koşullarında siber saldırıları bir tehditten öte iş hayatının doğal bir süreci gibi algılayıp bu saldırıdan ne dersler çıkarılabileceği konuşulmalı ve bu minvalde çalışmalara hız verilip bir sonraki saldırıdan en hasarla ayrılmaya gayret gösterilmelidir.

Çalışanlar bu süreçte kendilerine düşen görevler konusunda bilinçlendirilmeli herhangi bir tehdit unsuruyla karşı karşıya kalındığında rapor verme şeklini öğrenmelidir. Çalışanlar gözlemledikleri ve tehlikeli buldukları her vakayı belirlenen haberleşme noktalarına ne kısa süre zarfında iletmelidirler (Kahraman, 2006).

4.1.5. Fiziksel ve çevresel güvenlik

Bilgi güvenliğinin sağlanmasında çalışan farkındalığı, eğitimler, yazılımlar kadar önemli olan bir unsur da fiziksel ve çevresel güvenliktir. Ağ üzerinden yapılan siber saldırılara karşı gereken yatırım yapılırken çevresel unsurlar göz ardı edildiğinde kurum maddi ve manevi kayıplara uğrayabilir.

Fiziksel ve çevresel güvenlikten kast olunan bina çevresine çekilen azami yükseklikte duvarlar, bina girişinde yer alan özel güvenlik ekipleri, kritik verileri barındıran odalara şifreli veya kartlı giriş sisteminin tesis edilmesi gibi önlemlerdir.

Fiziksel ve çevresel güvenliği ana başlıklar itibarıyla incelemek gerekirse; güvenli bölgeler, teçhizat güvenliği, genel denetimler olarak sıralanabilir (Kahraman, 2006).

Güvenli bölgeler

Fiziksel koruma kurumların bilgi güvenliğini tesis edilmesi ve sürdürülmesi hususunda en çok başvurduğu yöntemlerden birisidir. Kurum çevresinde fiziksel engellerin oluşturulması, örneğin bir kart kontrolüne sahip giriş kapısı, yüksek bir duvar veyahut danışma masası gibi akla gelen her şeydir.

Güvenli alan oluşturulmasının bir numaralı gereksinimi fiziksel giriş denetimleridir. Güvenli alanlara dahil olmak isteyen kişilerin denetimi sağlanmalıdır. Güvenli alanlara giren ziyaretçilerin giriş ve çıkış tarihleri detaylı şekilde not edilmeli veyahut bu bilgileri not eden bir kart okuma sistemi temin edilmeli. Ziyaretçilere izin verilen saatlerde giriş hakkı verilmeli ve işlemini gerçekleştirene değin kurum görevlisi tarafından eşlik edilmelidir.

Personelin kimlik taşıması kurum bilgi güvenliğinin sağlanmasında önemli bir unsurdur. Kritik bilgilere erişim yetkisi verilenler belirli olmalı ve erişim sürekli denetlenmelidir. Tüm erişimleri denetlemek adına parola, giriş kartı gibi kimlik doğrulama işlemleri kullanılmalıdır. Kimlik kartı taşımadığı tespit edilen bir kişi görüldüğünde ani bir şekilde yetkililere bildirilmesi konusunda tüm personel teşvik edilmelidir. Bu kapsamda güvenlik konusunda gelişmiş kurumlar göz veya parmak izi teknolojisinden faydalanarak fiziksel giriş denetiminde başarıya ulaşmışlardır.

Oda, araç ve büroların güvenliğinin sağlanması güvenli alan oluşturulması için ehemmiyet verilmesi gereken ikinci konudur. Bu konuda akla gelen ilk güvenlik hamlesi kilitli hale getirilebilecek her şeyin kilitlenmesidir. Binaların inşasında veya seçiminde dikkat çekmeyen göze batmayan çizgiler tercih edilmelidir. Güvenli alan seçerken yangın, su baskını, patlama, heyelan, yıldırım gibi doğal afetler göz önünde bulundurulurken askeri saldırı kundaklama gibi insan temelli tehlikeler dikkatlerden kaçmamalıdır. İşletme tarafınca idare edilen bilgi işleme araçları fiziksel olarak üçüncü taraf çalışanlarınca erişilemeyecek bir konumda olması gerekmektedir. Yedek donanımlar ve yedekleme

araçları için kurum merkezinde gerçekleşebilecek felaketlerden en az hasarla ayrılabilmek adına merkeze uzak yerler tahsis edilmelidir.

Güvenli alanların tesis edilmesi ve sürdürülebilir hale getirilmesi için gerekli olan bir diğer unsur yükleme ve dağıtım alanlarının ayrılmasıdır. Bina dışından bulundurma bölgesine olan erişim sadece belirli yetkili personele özel olmalıdır. Dışardan gelen malzemeler bulundurma bölgesinden kullanılacağa alana alınırken muhtemel risklere karşı kontrolden geçirilmelidir. Bulundurma bölgesi dağıtım personelince binanın risk içeren bölgelerine ulaşması engellenecek ve sadece mevcut malzemeyi verip kurumdan ayrılacak şekilde bina edilmelidir.

Teçhizat güvenliği

Varlıkların kaybolmasını ve hasar görmesini engellemeye yönelik tedbirler bütünüdür. Verimli bir yerleştirme politikası ile teçhizatlar için risk oluşturan çevresel tehditlerin önüne geçilmeye gayret gösterilmelidir. Çünkü doğru bir yerleştirme planı ile kritik verilerin yaşayabileceği tehlikeler en aza indirilebilir. Çevrede yaşanabilecek olası felaketlere karşın özel koruma tedbirleri hayata geçirilmelidir. Veri iletimini sağlayan güç ve haberleşme kablolarının içinde bulunduğu riskler tespit edilmeli ve bu bağlamda önlemler alınmalıdır. Benzer risk taşıyan ve benzer amaca hizmet eden teçhizatlar için alan seçimi ortak olmalı ve düzenli bakımları yapılması için denetim sıklaştırılmalıdır.

Genel denetimler

Kurum çalışanları mesai saatleri içerisinde ve dışarısında alabilecekleri tedbirlerle bir takım bilgi güvenliği zafiyetlerinin önüne geçebilirler. Bu anlamda masa üzerinde yazıcının içerisinde veya etrafında, fotokopi makinde kişisel hiçbir doküman bırakılmamalıdır. Yazıcıların ve fotokopi makinalarının kullanılmadığı zaman kilitli olmasına özen gösterilmelidir. Kritik bilginin yazıcıdan çıktısı alındıktan sonra yazıcı hafızasından kritik bilginin silindiğinden emin olunmalıdır. Mesai saatleri dışında kritik bilgileri haiz dolap ve odalar kilitli tutulmalıdır. Teçhizatın yetkisiz kullanımının önüne geçebilmek için düzenli denetimler yapılmalıdır (Kahraman, 2006).

4.1.6. Haberleşme ve işletim yönetimi

Bilgi işleme araçlarının güvenliğinin tesis edilmesinde önemli unsurlardan birisi de haberleşme ve işletim yönetimidir. Bilgi işleme araçlarının verimli işletimi adına işletim prosedürleri, yönetimin önderliğinde, hazırlanmalıdır. Kişisel bilgisayarların açılmasından, teçhizat bakımına sistemin işletilmesine yönelik bütün faaliyetler bu prosedürlerde yer almalıdır. Prosedür hazırlanması gereken bir başka husus ise olay yönetimidir. Ani durumlarda, potansiyel tehditlerde nasıl davranılacağı olay yönetimi prosedürlerinde bahis konusu olmalıdır.

Kurum dâhilinde bilgi işleme araçlarının değişim yönetimine dair bir yaklaşım bulunmalıdır. Sorumluluklarda, prosedürlerde, donanım ve yazılımlarda yaşanacak tüm değişikliklere karşı kurum hangi adımı atacağını bilmelidir. Yaşanan değişikliklerin ve yerine getirilen yeni teçhizatın kaydı tutulmalıdır.

Haberleşme yönetiminde dikkat edilmesi gereken bir diğer unsur ise kapasite planlaması ve sistem kabulüdür. Kurum kapasitenin hassas bir şekilde tespit edilmesi ve bu hesap üzerine uzun vadeli plan yapılması işletim yönetiminin mühim bir unsurudur. Kapasitenin doğru planlanması hem işlem gücü ayarlamasına katkıda bulunur hem de depolama konusunda kurumun kaynak israfının önüne geçer. Kurum yeni bir bilgi sistemi edineceği zaman yahut sürüm yükselteceği zaman bu işlemleri bir kurallar silsilesi dâhilinde yapmalıdır. Yeni bir sistem kabul edileceği takdirde belirlenen kıstasların yazıldığından ve denetimden geçtiğinden emin olmalıdır.

Kurum bilgi işlem sisteminin ve iletişim hizmetlerinin sürdürülebilirliğini sağlamak için uzun vadeli bir yedekleme sistemine sahip olmalıdır. Kritik bilgiler ve yazılımların yedekleme kopyaları belirli aralıklar alınmalıdır. Ayrıca yapılan faaliyetlerin bağımsız denetim firmalarınca kontrolü için işletme kayıtlarının da yedeklemesi yapılmalıdır.

Haberleşme ve işletim yönetiminde ortam yönetimi önemli bir etkendir. Çünkü etiketlenmeyen ve yetkisiz erişimleri sınırlandırmak için veri kullanım kaydı tutulmayan bir sistem yanlış maksatlarla kullanıma açıktır. Ortam üretici firmanın sözleşmede yer alan şartlarına uygun şekilde tasarlanmalı yahut istenilen koşulları bir şekilde sağlamaya yönelik düzenlemeler yapılmalıdır.

Organizasyonlar arası yazılım ve bilgi değişimi sürekli denetim altında tutulmalıdır. Ayrıca ilgili mevzuat ile uyumlu olması gerekmektedir. Bilgi ve yazılım nakledilirken istenmeyen sonuçlar ortaya çıkmaması ve kurum itibarının yara almaması adına nakil prosedürleri belirlenmelidir. Nakil esnasında problem yaşamamak için kurum, bilgi değişim anlaşması imzalamalıdır. Nakil için tercih edilecek ulaştırma vasıtalarının nitelikleri, kuryeler için hazırlanan bir prosedür kapsamında tanımlanmalıdır. Hareket halinde iken ürünün zarar görmesini engellemek adına paketleme uygun bir şekilde yapılmalıdır.

Ticaretin büyük kısmının elektronik mecrada yapılması zaman ve mekân bakımından kolaylıklar sağlarken beraberinde bir takım risk unsurlarını da getirmiştir. Bilginin değiştirilmesi, haksız kazanç ya da anlaşma ihtilafları gibi tehditler elektronik ticaretin risklerindendir. Bu risklerin önüne geçebilmek adına güvenlik politikaları oluşturulmalı ve takibatı sağlanmalıdır. Halka açık olan sistemlerde sitelerde yer alan bilgilerin, ticaretin dâhil olduğu mevzuat ile uyumlu olması gerekmektedir (Kahraman, 2006).

4.1.7. Erişim denetimi

Bilgi güvenliği sisteminin kurulması ve sürdürülmesinde erişim denetimimin sağlanması temel yapı taşlarından biridir. Erişim denetimi ise iki soru üzerine bina edilmiştir. ‘’Kaynaklara kim erişiyor? Nasıl erişiyor?’’. Bu sorular doğru cevaplandığında yetkisiz değiştirme ve açığa çıkarma vakalarının önüne geçilebilir.

Erişim denetiminde kullanıcı sorumluluğu önem arz eden bir bileşendir. Kullanıcılar donanım ve yazılımlarıyla ilgili sorumlulukları hakkında bilgilendirilmelidirler. Dahili ve harici ağların denetlenmesi bilinçli kullanıcı kolaylaştırıcı etmen görevi görmektedir. Kullanıcılar yaptığı işlerin izlenebilmesi için, kişisel ve tek kullanım için tasarlanan tanımlayıcı (kullanıcı kimliği) sahibi olmalıdırlar. Zaman denetiminin sağlanması adına tanımlanan çalışmazlık süresinden sonra erişim hizmetinin kapatılması adına terminal zaman aşımı ve tehlike potansiyeli yüksek uygulamalarda bağlantı süre kısıtlaması getirilmelidir.

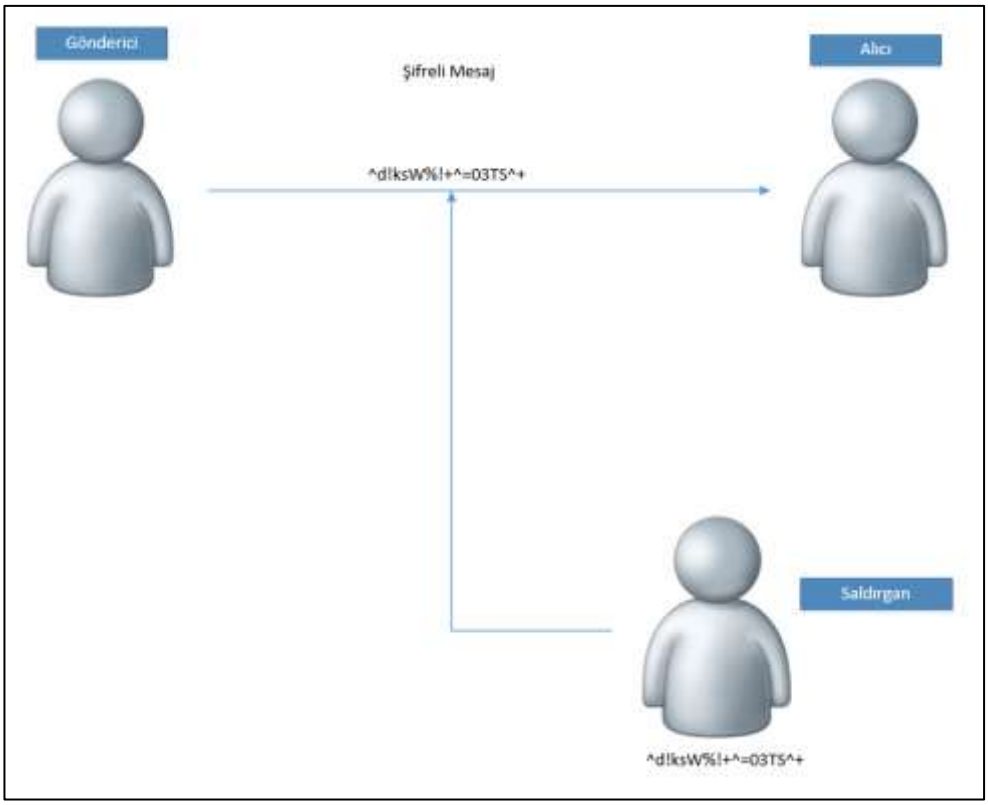
Uygulama ve sistemlerin erişimlerdeki sapmaları analiz edebilmek ve bir daha yaşanmaması adına tedbirler almak için sistemler sürekli kayıt altına alınmalıdır. Güvenlik

zafiyeti yaşamamaktan daha kötüsü o zafiyetten ders çıkaramamaktır. Bu bağlamda personel tarafından veya kayıt cihazlarıyla gözlemlenebilen her olay kaydedilmelidir (Kahraman, 2006).

4.1.8. Sistem geliştirme ve bakım

Herhangi bir kuruma herhangi bir sistem yerleştirilmeye çalışırken vakit ayrılması gereken asıl unsur o sistemin verimli işleyebilmesi adına alınması gereken güvenlik gereksinimleridir. Güvenlik gereksinimi tam olarak tespit edilip gereken önlemler alındıktan sonra harekete geçildiği takdirde risk seviyesi istenen ölçülere yaklaşılmış olur. Uygulamaya geçilmeden önce uygulamalarda yaşanabilecek, kullanıcı verilerinin ele geçirilmesi, kaybedilmesi veya değiştirilmesi gibi aksaklıkların önüne geçebilmek adına uygun kontrol sistemleri ve etkinlik kayıtları hazırlanmalıdır.

Bilginin gizliliği, bütünlüğünün ve erişilebilirliğinin temin edilmesi için gerekli sistemlerden biri de şifreleme sistemidir. Şifreleme yapılırken hangi şifreleme seviyesinin hangi etkinlikler için kullanılacağına karar verme aşamasına dikkat edilmelidir. Günlük, basit ve kritik önemi haiz olmayan bilgiler için ağır şifreleme tekniklerinin kullanılması hem kaynak hem zaman israfına neden olacaktır. Aynı şekilde kritik bilgiler içinde yüksek seviyede şifreleme tekniklerinin kullanılması gerekmektedir. Şekil 4. 3’ de görüldüğü üzere kötü niyetli kullanıcı veriyi ele geçirse dahi mesaj şifreli olduğundan herhangi bir şekilde kötü amaçları için kullanamaz.



Şekil 4.3. Şifreli bir iletişim ağına maruz kalan saldırgan (Kahraman, 2006)

Bilgi işleme sistemlerinin barındırdığı dosyaların güvenliğini sağlamak için alınması gereken önlemlerin başında işletim programları kütüphanesinin güncellenmesi düzenli aralıklarla yetkilendirilmiş kişiler tarafından yapılmalıdır. Gerçekleştirilen tüm güncellemelerin kaydı tutulmalıdır. Olası risklere karşı yazılımların önceki sürümleri listesi muhafaza edilmelidir (Kahraman, 2006).

4.1.9. İş sürekliliği yönetimi

Kurumların faaliyetlerinin kesintiye uğratan yangın, deprem, su baskını, kaza gibi etmenlere karşı önceden tedbir alıp bozulmaya ve icra edilen faaliyetin kesintiye uğramasına engel olmaya yönelik atılan adımlar bütününe İş Sürekliliği Yönetimi adı verilmektedir. İş sürekliliği yönetimi sadece bozulmaya yönelik tedbir almakla kalmaz aynı zamanda önüne geçilemeyen bazı durumlarda bozulmanın telafisini yönelik uygulamaları da hayata geçirir.

Siber saldırıların kurumlara maddi olarak ciddi kayıplar verdirdiği son dönemde iş sürekliliği yönetimine verilmesi gereken değerin farkındalığı artmaktadır. Üretim maliyeti

caydırıcı olmayan zararlı bir yazılımın, hedef aldığı kurumun faaliyetlerini aksatmaktan da öte tamamen iş yapamaz hale getirecek şiddetle zarar verebildiği göz önünde bulundurulursa iş sürekliliği yönetimi sisteminin kurumlar açısından önemi daha iyi takdir edilecektir.

Başarılı bir iş sürekliliği yönetimi riskleri tanımlamalı, en aza indirgemeli ve meydana gelen zararların sonuçlarına yönelik tedbirler almalıdır. Bu bağlamda denetimler ve operasyonlar gerçekleştirmelidir. İş sürekliliği yönetimi kapsamında, istenmeyen bir vaka gerçekleştiğinde hangi çalışanın hangi görevi üstleneceği belirlenmelidir. Belirlenen görev sorumluluklarla ilgili belgelerin hazırlanması gerekmektedir.

Olası doğal felaket veya insanlar tarafından planlı şekilde ortaya çıkarılan vakalara yönelik kurum personeline eğitim verilmelidir. Felaket anında yapılacaklar planlanmalı hesapta olmayan koşullar için B planı hazırlanmalıdır. Görev ve sorumluluk dağılımının, hazırlanan planların, verilen eğitimlerin verimlilik düzeyini tespit edebilmek ve farkındalığın artması adına iş sürekliliği tatbikatları düzenlenmelidir.

Olası felaket senaryosu kapsamında her türlü donanım, yazılım, kağıt vb. ekipman kurum yerleşkesinde yedek olarak saklanmalıdır. Faaliyetlerin aksamaması adına hizmet verebilecek kapasiteye sahip olan bir yedek merkez de tesis edilmelidir. Bilgisayar firmalarıyla imzalanan sözleşmede yedek merkezin işletilmesine dair servis, bakım ve destek hizmetlerine dair maddeler yer almalı ve alınacak hizmetlerin kapsamı en ince ayrıntısını hesaba katılarak anlatılmalıdır (Kahraman, 2006).

4.1.10. Uyumluluk

Bireylerin gerek sosyal gerek çalışma hayatlarını idame ettirebilmeleri için uyum sağlamaları gereken kurallar vardır. Kişi doğduktan sonra hatta bir kısmı için, doğmadan evvel yaşadığı ülkenin yürürlüğe koyduğu ceza kanuna, medeni kanuna tabidir. Kanun maddelerini bildiği ön kabulü vardır ve kanun maddeleriyle çatışacak bir fiil işlediği zaman kendini kanundan haberdar olmamakla savunamaz. Her birey vatandaş olarak neleri yapıp neleri yapamayacağını, sorumluluklarını ve yasalarla suç olarak addedilen bir faaliyet içerisinde olduğunda cezai müeyyidesinin olduğunu bilmekle mükelleftir. Kurumlar da aynı şekilde kuruldukları andan itibaren Ticaret Kanunu, Borçlar Kanunu vb. kurumları

ilgilendiren kanunlara tabidir. Her kurumun faaliyet gösterdiği alana göre tabi olduğu kanun, yönetmelikler tebliğler vardır. Bankacılık sektöründe faaliyet sergileyen bir kurum bankacılığın tabi olduğu yönetmelik ve tebliğlere tabidir, sağlık sektöründe hizmet veren bir kuruluş yine kendi alanını ilgilendiren hükümlere tabidir.

Bütün bu ifadeler göz önünde bulundurulduğunda kurum içerisinde alınan kararlar ve hazırlanan plan ve prosedürler, gerek kurumun faaliyetlerinin sürdürülebilirliği gerekse prestij açısından kurumun tabi oldu yasal yükümlülükler göz önünde bulundurulmalıdır.

4.2. TS ISO/IEC 27001 Bilgi Güvenlik Yönetim Sistemi

Bu uluslararası standart, sağlıklı bir BGYS bina etmek, uygulamak, sürdürmek ve sürekli geliştirmek için gerekenleri sağlamak amacıyla tasarlanmıştır. Bir kurum için BGYS' ye adapte olmak ve gerekliliklerine uyum sağlamaya gayret sarf etmek stratejik bir karardır. BGYS kurulumu, kurum ihtiyaç ve varlıklarına göre değişkenlik gösterir. BGYS risk yönetim süreci sayesinde bilginin güvenliğini, erişilebilirliğini ve bütünlüğünü garanti altına alır.

BGYS' yi süreç tasarlayan, bilginin yönetimini ve kontrolünü sağlayan genel bir yönetim unsuru olarak değerlendirmemek BGYS' nin kurumun tamamına nüfuz etmesine engel olabilir. Bu bağlamda BGYS uygulamaları kurumun ihtiyaçları çerçevesinde hazırlanmalıdır (ISO/ IEC 27001, 2013).

4.2.1. Kapsam

Bu standart BGYS kurulumu, uygulaması, sürdürülebilirliği ve sürekli iyileştirilmesini hedefler. Bu standart ayrıca bilgi güvenliği risk değerlendirme ve risk işleme gerekliliklerini göz önünde bulundurularak BGYS kurulumunu hedefler. Bu uluslararası standart pazar hacmine veya faaliyet alanına bakılmaksızın bütün kurumlara uygulanabilir.

4.2.2. Atıf yapılan standartlar ve/veya dokümanlar

ISO/ IEC 27001' de atıfta bulunulan dokümanlara resmi olarak atıfta bulunulmuştur ve uygulamanın başarıya ulaşması için zaruri olan dokümanlar tercih edilmiştir.

4.2.3. Tanımlar ve terimler

Bu dokümanda yer verilen tanım ve terimler ISO/ IEC 27000 de detaylı bir şekilde açıklanmıştır.

4.2.4. Kuruluşun Yapısı

BGYS' den önce kurum kendisini anlamalı, ihtiyaçlarını güçlü ve zayıf yanlarını tespit edebilmeli akabinde BGYS' nin kurumun hangi alanlarına nüfuz edeceğine karar vermelidir.

Kuruluşu ve yapısını anlama

Organizasyon hedeflerini gerçekleştirebilmek adına, iç ve dış değişkenleri doğru belirlemeli, kurumun genel yapısını analiz etmelidir. Kurumun yapısını doğru analiz etmek BGYS kurulumu açısından yüksek önem taşımaktadır. Çünkü kıyafet dikeceği vücudun ölçülerini iyi alamayan terzinin hata yapma ihtimalinin yüksek olduğu gibi kurumun yapısı iyi analiz edilmeden bina edilmeye çalışılan bir BGYS de hatalara açık olacaktır. Bu ihtiyaçları tam tespit edebilmek için ISO 31000 den faydalanılabilir.

İlgili tarafların ihtiyaç ve beklentilerini anlamak

BGYS ile ilgili taraflar ve bu tarafların bilgi güvenliğinin sağlanmasına yönelik ihtiyaçları kurum yönetimi tarafından ortaya konmalıdır. İlgili tarafların gereksinimi yasal gereksinimler ve sözleşmede yer alan hükümleri de kapsar.

BGYS kapsamının belirlenmesi

Kurum BGYS sınırlarını ve uygulanabilirliğini, kapsamını belirlemek için tespit etmelidir. Bu tespiti yaparken kurum; iç ve dış değişkenleri göz önünde bulundurmalı ve tarafların ihtiyaçlarını anlamalıdır. Diğer kurumlarla olan bağımlılıklar ve ara yüzler değerlendirilmelidir.

BGYS

Organizasyon bu uluslararası standart ile uyumlu bir şekilde BGYS' yi inşa etmeli, sürdürmeli ve sürekli gelişimini teminat altına almalıdır.

4.2.5. Liderlik

BGYS kurulumunda temel yapı taşlarından birini oluşturur. Üst yönetimin desteği, BGYS politikası, görev ve sorumlulukların dağılımı gibi kilit konular ortaya konur.

Liderlik ve taahhüt

Üst yönetim liderlik göstermeli ve BGYS konusunda üzerine düşenleri yerine getirmelidir. Yönetim güvenlik politikasını ve bilgi güvenliği hedeflerini hazırlamalıdır. Yeterli kaynağı ayırmalı ve BGYS' nin entegrasyonu için gereken hazırlıkları tamamlamalıdır. BGYS kapsamında belirlenen uzun ve kısa vadeli hedeflere varıldığını ve sürekli gelişim sağlandığını temin etmelidir.

Politika

Üst yönetim organizasyon amaçlarıyla uyumlu, sürekli gelişimle ve uygulanabilir gereklerle ilgili komutların yer aldığı bir güvenlik politikası hazırlamalıdır. Politika organizasyonla iletişim halinde ve dokümante edilmiş olmalıdır. Ayrıca kurum içi ve dışı tüm taraflarca ulaşılabilir olmalıdır.

Görev, sorumluluk ve yetki

Üst yönetim rol ve sorumlulukların dağıtımından ve ilgililerin haberdar edildiklerinden emin olmalıdır. BGYS gereksinimlerinin ISO/ IEC 27001 göz önünde bulundurularak tatmin edildiğinden ve BGYS performans seyrinden üst yönetimin haberdar edildiğinden emin olunmasını sağlamak için görev ve sorumluluklar titizlikle dağıtılmalıdır.

4.2.6. Planlama

BGYS sisteminin temellerinin atıldığı noktalardan birisini teşkil eder. Risklerin tehditlerin, açıklıklarının belirlenmesi ve söz konusu tehditlerin gerçekleşmesi halinde ortaya çıkacak zararın tespiti bu bölümde yapılır. Yapılan tespitler doğrultusunda alınacak aksiyonlar yine bu bölümde belirlenir.

Risklere ve fırsatlara yönelik eylemler

A. Genel

BGYS için planlama yapılırken kurum yapısını doğru analiz edilmeli ve ilgili tarafların beklentileri hesaba katılmalıdır. Risk ve fırsatlara dair çalışma yapılırken BGYS' nin istenilen sonuçlara ulaşma imkânı temin edilmeli, istenmeyen etkilerden korunmak için tedbirler alınmalı, sürekli gelişim gözetilmelidir. Kurum ayrıca risk ve fırsatlara dair faaliyetlere planında yer vermeli ve bu faaliyetleri BGYS süreciyle entegre etmelidir.

B. Bilgi güvenliği risk değerlendirme

Risk değerlendirme çalışmasında öncelik verilmesi gereken ilk husus kapsam ve varlıkların belirlenmesidir. Bir diğeri olmadan pek anlam ifade etmeyen bu iki kavram kurumun hedeflerine ilerlerken enerji israfının önüne geçer. Risk değerlendirmesinde kapsam belirlemek ilgilenilecek ve risklerden arındırılacak bölgeleri belirlemek adına önemlidir. Hangi alanların risk değerlendirme kapsamına alınıp alınmayacağına karar verebilmek için alanları tanımlamak zaruridir. Önceki bölümde varlıkların envanteri oluşturma işlemi tafsilatlı şekilde anlatıldığı için varlık tanımlama aşamalarında detaya girilmeyecektir (Eskiyörük, 2007).

- Tehditlerin belirlenmesi

Herhangi bir tehdit unsurunun var olan açıklıktan faydalanarak kasten veya kazara varlıklara zarar verme potansiyelidir. Tehdit unsuruysa varlıklara zarar verme ihtimali bulunan vakalar olarak ifade edilebilir. Tehdit unsurları sıralanmak istenirse (Eskiyörük, 2007):

Doğal tehditler: Su baskını, yangın, deprem, heyelan gibi tehditler.

Çevresel tehditler: Zararlı atıklar, çevreden gelebilecek gürültüler vb.

İnsan kaynaklı tehditler: Personelin varlıkları hatalı kullanımı sebebiyle ortaya çıkan durumlar. Güvenlik tedbirlerine riayet etmeme, dikkatsizlik, izinsiz erişim vb.

Tehditler ele alınırken herhangi bir tehdidin küçümsenmesi veya göz ardı edilmesi hatalı bir tutum olur. Zira küçümsenen unsurlar diğer tehdit kalemlerini tetikleyerek beklenmeyen zararlara sebebiyet verebilir. Tehditler değerlendirilirken yapılması gereken tehdidin kaynağını belirlemektir. Tehdit kaynaklarının tespiti için başvurulacak mecra ise varlık sahipleridir. Tehditlerin tümünü bir arada görmek risk değerlendirme çalışmasını kolaylaştırabilir. Aşağıdaki şekil 4.4' de bilgi güvenliğine tehdit oluşturan unsurlar ve kaynakları genel olarak sıralanmıştır(B: Bilerek, K: Kazara, D: Doğal, Ç: Çevresel).

Tehdit	Tehdidin Kaynağı
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriyel bilgi sızması	B, K
Bombalama veya silahlı saldırı	B
Yangın	B, K
Güç kesintisi	B, K, Ç
Su kesintisi	B, K, Ç
Havalandırma sisteminin arızalanması	B, K, Ç
Donanım arızaları	K
Güç dalgalanmaları	K, Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B, K
Saklama ortamlarının eskiyip kullanılmaz duruma gelmesi	K
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılım hataları	B, K
Lisansız yazılım kullanımı	B, K
Yazılımların yetkisiz kullanılması	B, K
Kullanıcı kimlik bilgilerinin çalınması	B, K
Zararlı yazılımlar	B, K

Şekil 4.4. Bilgi güvenliğinde karşılaşılan tehditler ve kaynakları

- Açıklıklıların belirlenmesi

Sistem güvenliğinde, çevresel etmenler üzerinde, denetimler, yerleşim düzeninde bulunan ve bilgi güvenliğini sekteye uğratabilecek herhangi bir vakadır. Açıklıkların tehlike arz edebilmeleri için tehdit unsurunun bulunması gerekmektedir. Tehditlerle bir araya geldiğinde ortaya sorun çıkartan açıkların değerlendirilmesi hangi tehdit unsurunun hangi açıkla ilgili olduğunu ve söz konusu açıklıkların gerçekleşebilme olasılıklarını ele alır. Açıklık listeleri oluşturulurken geçmişte yapılan risk değerlendirmelerinden, sistem denetim raporlarından, üretici uyarılarından, sistem güvenlik taramalarından, yazılım güvenlik analizlerinden ve sızma test sonuçlarından faydalanılabilir. Şekil 4.5'de bazı örnek açıklıklar ve bu açıklıkları gerçekleştirebilecek tehditler sıralanmaya çalışılmıştır.

Altyapı ve çevre	Binada yeterli fiziksel güvenliğin bulunmaması	Hırsızlık
	Binalara ve odalara girişlerde yetersiz fiziksel kontrol	Kasten zarar verme
	Eski güç kaynakları	Güç dalgalanması
	Deprem bölgesinde bulunan yapılar	Deprem
	Herkesin erişebildiği kablosuz ağlar	Yetkisiz erişim
	Dış kaynak kullanımında işletilen prosedür ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği	Yetkisiz erişim
Donanım	Periyodik yenilemenin yapılmaması	Donanımların bozulması nedeniyle erişimin durması
	Voltaj değişikliklerine, ısıya, neme, toza duyarlılık	Güç dalgalanmaları
	Periyodik bakım eksikliği	Bakım hataları
	Değişim yönetimi eksikliği	Kullanıcı hataları
Yazılım	Yama yönetimi eksikliği/yetersizliği	Hassas bilginin açığa çıkması
	Kayıt yönetimi eksikliği/ yetersizliği	Yetkisiz erişim
	Kimlik tanımlama ve doğrulama eksiklikleri	Yetkisiz erişim
	Şifre yönetimi yetersizliği	Başkalarının kimliğine bürünme
	Şifre veri tabanlarının korunmaması	Yetkisiz erişim
	Erişim izinlerinin yanlış verilmesi	Yetkisiz erişim
	İzinsiz yazılım yüklenmesi ve kullanılması	Yasal gerekliliklere uyum
	Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi	Yazılım hataları
	Yazılımların yeterli test edilmemesi	Yetkisiz erişim
Haberleşme	Korunmayan haberleşme hatları	Haberleşmenin dinlenmesi
	Hat üzerinden şifrelerin açık olarak iletilmesi	Yetkisiz erişim
	Telefon hatlarıyla kurum ağına erişim	Yetkisiz erişim
	Ağ yönetimi yetersizliği/eksikliği	Trafiğin aşırı yüklenmesi
Personel	Eğitimi eksikliği	Personel hataları
	Güvenlik farkındalığı eksikliği	Kullanıcı hataları
	Donanımların veya yazılımların yanlış kullanılması	Personel hataları
	İletişim ve mesajlaşma ortamların kullanımını düzenleyen politikanın eksikliği/yetersizliği	Yetkisiz erişim
	İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması	Kasten zarar verme

Şekil 4.5. Açıklıklılar ve ilgili tehditler (Eskiyörük, 2007)

- Mevcut ve Planlanan Kontrollerin Belirlenmesi

Ortaya konulan tehditler, açıklıklar ve bu açıklıkları gerçekleyebilecek tehditlerden sonra yapılacak faaliyet bu tehditleri ortadan kaldıracak veya en aza indirgeyecek kontrollerin planlanmasıdır. Uygulanacak kontroller, açıklıkların tehditlerden etkilenerek zarara sebebiyet verme ihtimalini azaltacağı için olasılık değerlendirmesinde ve buna bağlı olarak risk derecelendirmesinde ehemmiyet arz edecektir. Kontroller ilerleyen başlıklarda detaylı bir şekilde ele alınacaktır (Eskiyörük, 2007).

- Olasılık Değerlendirmesi

Risk değerlendirilmesinde önemli sacayaklarından biri de tespit edilen açıklıkların gerçekleşme olasılığının belirlenmesidir. Tüm açıklıklar için ayrı ayrı olasılık değerlendirmesi yapılmalıdır. Tehdidin kaynağının motivasyonu, açıklığın türü, mevcut kontrollerin etkinliği bir arada ele alınmalıdır. Her kurum kendi yapısına ve amaçlarına göre nasıl bir olasılık değerlendirmesi yapacağına kendi karar verecektir. Örnek olasılık değerlendirme tablosu şekil 4.6' da gösterilmiştir.

Olasılık seviyesi	Olasılık Tanımı
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesine engel olacak kontroller mevcuttur.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçeklemesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.

Şekil 4.6. Olasılık değerleme tablosu (Eskiyörük, 2007)

- Etki Analizi

Olasılık analizinde mevcut açıklıkların tehditler vasıtasıyla gerçekleşme olasılığı belirlenmeye çalışılmıştı. Etki analizinde ise gerçekleşen açıklığın kurum üzerindeki olası etkileri belirlenmeye çalışılır. Etki analizinde gerçekçi sonuçlar elde edebilmek için söz konusu varlığın görevi, varlığın etkilediği verinin kritikliği, varlığın maddi değeri vb. değerler göz önünde bulundurulmalıdır. Bu değerler kimi varlıkları değerlendirmek için eksik kalabilir o zaman söz konusu varlık için kurum gerçekçi bir kıstas bulmalıdır. Daha önceden hazırlanmış iş etki analizleri kontrol edilebilir. Sistemin çalışmadığı dönemdeki gelir kaybı ve sistemin yenilenme maliyeti gibi niteliksel unsurlar da göz önünde bulundurulabilir. Şekil 4.7' de örnek bir Etki Değerlemesi tablosu gösterilmiştir.

Etki Derecesi	Etki Tanımı
Yüksek	Açıklığın gerçekleşmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. İnsan hayatı kaybı veya ciddi yaralanmalar gerçekleşebilir
Orta	Açıklığın gerçekleşmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir. Yaralanmalar gerçekleşebilir.
Düşük	Açıklığın gerçekleşmesi durumunda: Kurumun bazı varlıkları etkilenir Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

Şekil 4.7. Üç seviyeli etki değerlendirmesi (Eskiyörük, 2007)

- Risk Derecelendirmesi

Bilgi güvenliğini tehdit eden risklerin hangisine karşı ne kadar tedbir alınması gerektiğini tespit etmek için risklerin derecelendirilmesi gerekmektedir. Uygulanacak kontrollerin seçimi bu derecelere göre yapılır. Risk, bir tehdit vasıtasıyla hayat bulan açıklığın gerçekleşme olasılığına karşı alınan kontrollerin ne ölçüde başarıya ulaştığının fonksiyonudur. Risklerin derecelendirilmesi için bir matris oluşturulması kurum açısından faydalı olabilir. Şekilde 4.8’ de örnek bir risk derecelendirme matrisi gösterilmiştir.

		Etki Seviyesi		
		Düşük	Orta	Yüksek
Olma Olasılığı	Düşük	Düşük	Düşük	Düşük
	Orta	Düşük	Orta	Orta
	Yüksek	Düşük	Orta	Yüksek

Şekil 4.8. Örnek risk derecelendirme matrisi (Eskiyörük, 2007)

Bu matriste yer alan değerler kurum yetkililerince belirlenmelidir. Hangi olma olasılığının ne ölçüde etki edebileceğine ancak kurum içinde görev alan o tehlikeyi birinci elden gözlemleyen kişi vakıf olabilir. Yukardaki matriste olma olasılığı ‘’Orta’’ olan bir açıklığın etki seviyesi ‘’Yüksek’’ ise etki derecesi orta olarak adlandırılmıştır. Tercihe göre olma olasılıkları rakamlarda da ifade edilebilir. Olma olasılıklarına 0 ile 1 arasında değerler verilirken, etki seviyesinde 0 dan 100 e kadar sayılar verilerek bu ikisinin çarpımından ortaya sayısal bir veri çıkartılabilir.

Kurum yönetimi risk derecelendirmesini yaptıktan sonra riskin neyi ifade ettiğini tanımlamalı ve bu risk karşısında kurumun nasıl bir önlem alması gerektiğine karar vermelidir. Gerçekleri somut bir şekilde ortaya koymak ve ileri yönetimlere kaynak teşkil etmesi açısından bu tür bir kaydın tutulmasında fayda vardır (Eskiyörük, 2007). Şekli 4.9’ da örnek bir tablo halinde gösterilmiştir.

Risk Derecesi	Risk açıklaması ve yapılması gerekenler
Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edilebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içeresinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Şekil 4.9. Risk dereceleri ve tanımları (Eskiyörük, 2007)

- Uygun Kontrollerin Belirlenmesi

Risk derecelendirme çalışmalarının neticesinde risklerin en aza indirgenmesi yahut ortadan kaldırılması için bu minvalde kontrollerin gerçekleştirilmesi gerekmektedir. Önerilen kontrollerin hedefi riski kurum tarafından kabul edilebilir seviyeye çekmek olmalıdır. Kontroller belirlenirken kurum kapasitesi, yasal düzenlemeler, kurum personelinin kontrollere vereceği tepkiler göz önünde bulundurulmalıdır. Uygulanacak kontroller 3 ana başlık altında toplanabilir (Eskiyörük, 2007).

- Teknik güvenlik kontrolleri

Diğer kontrol unsurlarını yazılım, donanım ve sistem kontrolleri sayesinde daha aktif çalışmasını sağlayan bir kontrol çeşididir. Kurumun veri tabanına kimin ulaşıp ulaşamayacağının belirlenmesi ve sürekli kontrolünün yapılması gerekmektedir. Bu anlamda kriptografik anahtar yönetimi ve kimlik tanımlama bir kontrol unsurudur. Kimliği ve yetkileri tanımlanan kullanıcı kendisine verilen şifre yardımıyla kendisine belirlenen çerçeve dışında hareket edemez. Sistem de gerçekleşen herhangi bir olağan üstü durum veya saldırı sürekli denetleme sayesinde hemen tespit edilmeli ve gerekli düzeltmeler anında gerçekleştirilmelidir. Önüne geçilemeyen bir güvenlik ihlali olduğunda ise bütünlüğü bozulan veriler yedeklerden temin edilerek eski haline döndürülür.

- Yönetimsel kontroller

Yönetimsel kontroller hazırlanan prosedür ve politikalar vasıtasıyla kontrollerin belirli bir istikamette ilerlemesini ve canlı kalmasını sağlar. Prosedür ve politikaların daha etkin kullanılabilmesi için dokümante edilmesi ve farkındalık oluşturma adına çalışanlara eğitim verilmesi yine bu kapsamda değerlendirilir. Alınan güvenlik tedbirlerinin ve sistemin düzenli aralıklarla denetlenmesi gerekir. Düzenli denetlemeye rağmen gerçekleşebilecek olaylar için acil durum müdahale ekiplerinin kurulması gerekmektedir.

- Operasyonel kontroller

Kurumun faaliyetlerini gerçekleştirirken, kasten veya sehven ortaya çıkabilecek hataları engellemeye yönelik kontrollere operasyonel kontroller denir. Bu amaçla operasyonel kontrollerin uygulanma şekli tafsilatlı bir şekilde dokümante edilmesi ve bu dokümanların kurum genelinde farkındalığının sağlanması gerekmektedir. Operasyonel kontroller tasarlanırken alınması gereken ilk önlem kurum çalışanlarınca ve ziyaretçiler tarafından erişilebilir alanların kontrol altına alınmasıdır. Veri sınıflandırma ve yaka kartı kullanımı bu bağlamda alınacak aksiyonlardan birkaçıdır. Çevresel unsurların oluşturabileceği tehlikelere yönelik hareket algılayıcılar ve güvenlik kameraları tercih edilebilir.

C. Bilgi güvenliği risk işleme

Etkileri, olasılıkları ve uygulanacak tedbirleri belirlenen riskler toplu şekilde ortaya konduktan sonraki adım ise risk işleme adımıdır. Mevcut olan bütün kontrol mekanizmalarını uygulamak kuruma hem zaman hem de bütçe kaybı yaşatacağından bu kısımda seçilen risk işleme yöntemi kullanılarak riskleri en aza indirgemeye gayret gösterilir (Eskiyörük, 2007).

- Risk işleme yöntemleri

Kurum kapasitesine, tehditlerine ve hedeflerine göre risk işleme yöntemini seçmelidir. Başlıklar halinde sıralanmak istenirse risk işleme yöntemleri aşağıdaki gibidir.

Riskin kabulü: Risk sonucu ortaya çıkması muhtemel zararlar kabul edilerek kurumu aynı şekilde yönetmeye devam etmek

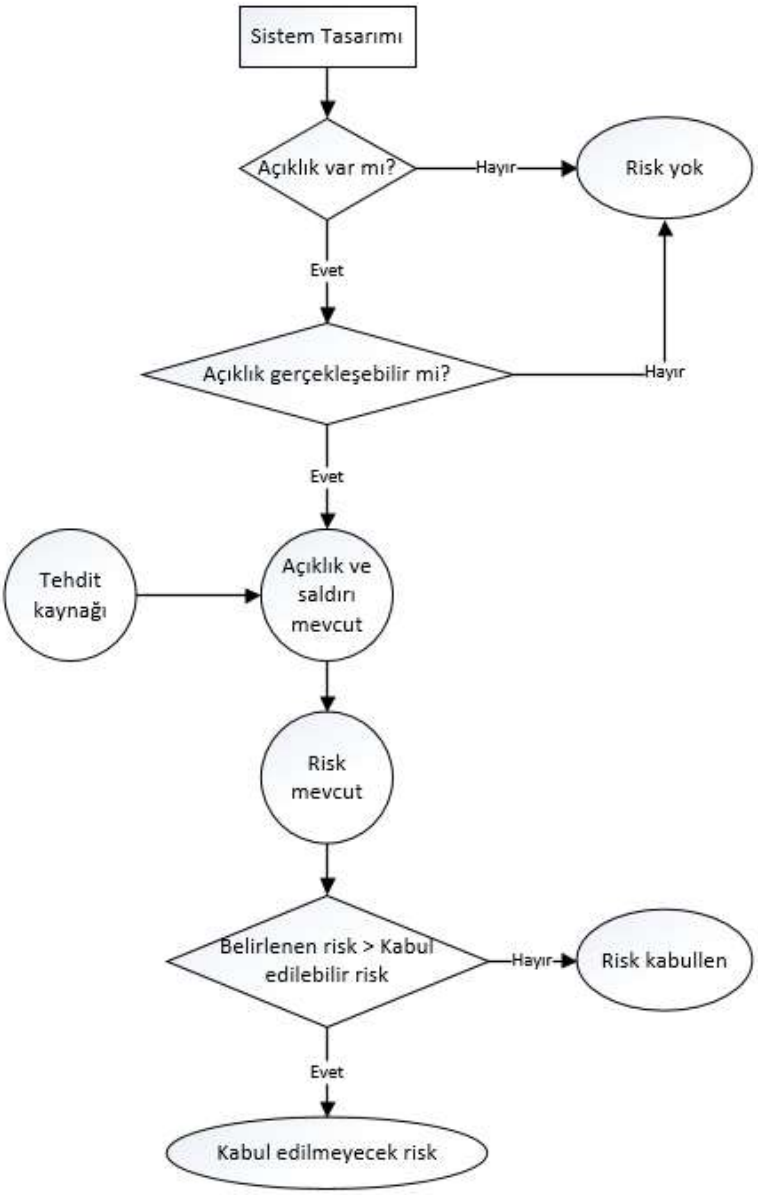
Riskten kaçınma: Riskin kökeninde yatan sebebi tamamen devre dışı bırakmaktır (Risk unsuru olan bir yazılımı hiç yüklememek).

Riskin azaltılması: Uygulanan kontroller vasıtasıyla açıklığın oluşturacağı zararın etkisinin azaltılması.

Riskin transferi: Risk unsuru olan açıkların gerçekleşmesi halinde oluşacak etkiyi bir başkasının üstlenmesini sağlamak (örneğin sigorta yaptırmak).

- Kontrollerin uygulanması

Tespit edilen risklerin azaltılması için kurum tarafından bir takım kontroller belirlenir. Ancak kurum için bazı riskler tespit edilip ortadan kaldırılması gerekenler sınıfına girerken bazıları için alınacak önlemler oluşturacağı etkiden fazla olacağından önlem alınmaya değer olmayanlar sınıfına girer. O yüzden önce riskin kuruma maliyeti, risk için alınacak önlemin kuruma maliyeti, saldırganın saldırıdan elde edeceği kazanç belirlenir ardından hangi kontrolün uygulanacağı ortaya konur. Şekil 4. 10’ da hangi risk için kontrol uygulanacağı hangi riskin kabul edileceği gösterilmiştir. Riskler göz önünde bulundurularak kontrol politikası uygulanırken açıklığım gerçekleşme olasılığını en aza indirgeyecek kontroller uygulanır.



Şekil 4.10. Kabul edilecek risklerin belirlenmesi (Eskiyörük, 2007)

- Kontrollerin uygulanmasında izlenecek yaklaşım

İlk olarak önceki risk derecelendirme aşamasında tespit edilen ve sıralanan riskler önceliklendirilir. Her riske gereken kadar güç sarf edilmelidir. Ardından riskler için belirlenen kontroller gözden geçirilmelidir. Bu bağlamda kontroller için fayda- maliyet analizleri yapılır. Yapılan analizler sonucunda teknik, yönetimsel ve operasyonel kontrollerden oluşan bir kontrol seçilir. Bu kontrollerin sürdürülebilirliğinin sağlanması için gerekli sorumluluklar atanır ve planlar hazırlanır. Planlar risk derecelendirmelerini ve bunlar için seçilen kontrolleri, kontroller için atanan sorumlulukları ve kontrollerin

uygulanmasının tahmini başlangıç ve bitiş tarihleri yer almalıdır. Planlar da hazırlandıktan sonra kontroller uygulanır. Kontrollerin istenilen sonuçları kazandırıp kazandırmadığını ortaya koymak için düzenli aralıklarla toplantı yapılmalıdır.

- Artık risk

Kontrollerin uygulanması her zaman risk kalemlerini sıfıra indirgemez. Bir takım risk unsurları uygulanan kontrollerin ardından mevcudiyetini korumaya devam eder. Bu risklere artık risk denir. Eğer artık riskin seviyesi kabul edilebilir seviyenin altındaysa yönetim tarafından riskin varlığı kabul edilmeli ve onaylanmalıdır, eğer kabul edilebilir seviyenin üzerinde ise risk işleme işlemleri tekrarlanmalıdır.

Bilgi güvenliği hedefleri ve planlama

Kurum belirli bir düzeye ve fonksiyona sahip bir takım bilgi güvenliği hedefleri tasarlamalıdır. Bu hedefler ölçülebilir, bilgi güvenliği politikasıyla uyumlu ve güncel olmalıdır. Ayrıca bilgi güvenliği gerekliliklerini göz önünde bulundurmalı ve risk değerlendirme süreçlerini göz önünde bulundurmalıdır.

Kurum hedeflerine ulaşmak için hazırlaması gereken planda yapılması gerekenler, kullanılacak kaynaklar, sorumluluklar, bitiş tarihi ve sonuçları değerlendirme yöntemi yer almalıdır.

4.2.7. Destek

Gerçekleştirilecek faaliyetlerin verimliliğini artırmak ve takviye etmek için kurum genelinde gerekli tedbirler alınmalıdır.

Kaynaklar

Kurum BGYS nin inşa edilmesi, uygulaması ve sürdürülebilirliği için gerekli olan kaynağı belirlemelidir. Bu kaynaklar yönetimin onayıyla ayrılmalıdır.

Yetkinlik

Bilgi güvenliği performansının istenen düzeyde sağlanması için personel yetkinliği ve hizmet yeterliliği sürekli denetim altında tutulmalıdır. Personel alım sürecinde eğitim ve deneyim unsurları göz önünde bulundurulmalıdır. Alınan aksiyonların etkinliği temin edilmeli ve değerlendirilmelidir.

Farkındalık

Kurum genelinde bilgi güvenliğinin kuruma katkıları ve personelin bilgi güvenliğinin sağlanmasındaki rolü konusunda farkındalık geliştirilmelidir.

İletişim

Kurum bilgi güvenliğinin sağlanmasında iç ve dış iletişimin önemini kavramalı ve bu bağlamda kimin, ne zaman, kimle, hangi konuda iletişim gerçekleştireceğini belirlemelidir.

Dokümante bilgi

Kurum BGYS bu uluslararası standardın gerekli gördüğü dokümante bilgiyi içermelidir. Bu dokümante BGYS' nin işlevselliğinin artırılması adına bilgi üst yönetimin gözetiminde hazırlanmalıdır. Üst yönetim ayrıca dokümante bilginin gözden geçirilmesi ve güncellenmesi sorumluluğunu da üstlenmelidir. Dokümante bilginin ulaşılabilirliğinin sağlanması için güvenlik tedbirleri alınmalıdır.

4.2.8. Operasyon

Önceki bölümlerde hazırlanan plan ve programların hayata geçirilmesi bu bölümde yapılır.

Operasyonel planlama ve kontrol

Kurum BGYS gerekliliklerini karşılamak için oluşturulan süreçlerin kontrolünü ve uygulamasını planlamalıdır. Risklere ve fırsatlara yönelik eylemler bölümünde yer alan

aksiyonlar gerçekleştirilmelidir. Kurum ayrıca bilgi güvenliği hedefleri ve planlama bölümünde yer alan hedefleri gerçekleştirmek için planları uygulamalıdır. Kurum dokümante edilmiş bilginin boyutlarını yapılan planlama dâhilinde kontrol altında tutmalıdır.

Bilgi güvenliği risk değerlendirmesi

Kurum hazırlanan planlar doğrultusunda bilgi güvenliği risk değerlendirmesini gerçekleştirmelidir. Önemli değişiklikler risklere ve fırsatlara yönelik eylemler bölümünde yer alan kaideler göz önünde bulundurularak gerçekleştirilmelidir. Kurum risk değerlendirmesi sonuçlarını saklı tutmalıdır.

Bilgi güvenliği risk işleme

Kurum bilgi güvenliği risk işleme planına sadık kalmalı ve gerçekleştirilen eylemlere dair sonuçları muhafaza etmelidir.

4.2.9. Performans değerlendirme

Prosedürlerin ve faaliyetlerin sonuçları takip edilmelidir. Bu takibatın yapılmasının temini için birimler tesis edilmelidir.

İzleme, ölçme, analiz ve değerlendirme

Kurum bilgi güvenliği performansını ve BGYS etkinliğini değerlendirmelidir. Bu bağlamda hangi değerlerin takibinin ve ölçümünün yapılması gerektiğini belirlemelidir. İzleme, ölçüm, analiz ve değerlendirme için metotlar belirlenmekle kalmayıp izlemeyi kimin yapacağı, hangi sıklıkla yapacağı belirlenmelidir. Analiz ve değerlendirme sorumlulukları da açıkça ortaya konmalıdır.

İç denetim

Kurumun BGYS gerekliliklerinin yerine getirilmesi ve ISO/IEC 27001 standardının talimatlarının takibinin yapılmasının teminatı için bir iç denetim mekanizması oluşturması gerekmektedir. Kurum denetimin metotlarını, sıklığını ve sorumluluklarını açıkça ortaya

koymalıdır. Denetim kriterleri ve kapsamı üst yönetimce belirlenmelidir. Denetim sonuçlarının ilgili birimlere raporlandığı teminat altına alınmalıdır.

Yönetimin gözden geçirmesi

Üst yönetim kurum dâhilinde BGYS' nin planlan şekilde kurulduğunu ve sürdürüldüğünü gözden geçirmelidir. Üst yönetim sistemi gözden geçirirken önceki yönetim raporlarını, BGYS ile ilgili kurum içi ve kurum dışı değişimleri göz ardı etmemelidir. Üst yönetim denetim, ölçüm, analiz ve izleme sonuçlarını sürekli izlemelidir.

4.2.10. İyileştirme

BGYS' nin gerçekleştirilme sürecinde karşılaşılan uyumsuzluklar ve bu uyumsuzlukların nedenleri belirlenmelidir. Uygunsuzluklara karşı alınacak önlemler ortaya konulmalıdır.

Uygunsuzluk ve düzeltici faaliyet

Uygunsuzluk gerçekleştiğinde mümkün olduğunda hızlı bir şekilde kontrol altına almak ve düzeltmek adına olaya müdahale edilmelidir. Uygunsuzluğun kök sebeplerinin bir daha gerçekleşmeyecek şekilde ortadan kaldırılması için uygunsuzluk izlenmeli ve analiz edilmelidir. Benzer uygunsuzluk potansiyeli taşıyan konular tespit edilmeli ve gereken tedbirler alınmalıdır. Uygunsuzluğun kök nedeni ve bu bağlamda alınan aksiyonlar dokümante edilmelidir.

Sürekli iyileştirme

Kurum BGYS' nin uygunluk, yeterlilik ve etkinlik performansının sürekli gelişimini temin etmelidir.

4.3. Vaka Analizleri

ISO 27001 BGYS' yi deneyimleyen kurumların yaşadığı problemleri ve başarıları yeni başlayan kurumlar için ayağı yere basan kaynaklar olabilir.

4.3.1. Wirefast limited liability company

İngiltere, ABD ve Asya'daki teknoloji tesisleri bulunan Wirefast Limited Şirketi bankacılık, finans, petrol, gaz ve sağlık sektörlerinde iletişim hizmetleri sağlamaktadır. İletişim tabanlı iş süreçlerini iyileştiren, otomatikleştiren ve geliştiren Wirefast, müşterilerine hayati önem arz eden bilgilerine istedikleri zamanda ve şekilde ulaşabilme güvencesini vermektedir. Ayrıca bu hizmeti makul bir maliyet karşılığında sağlamayı amaçlamaktadır.

Güvenlik faktörünü faaliyetlerinin temel yapı taşı olarak addeden Wirefast 2011 de en iyi uygulama seviyesine erişmek için ISO 27001 sertifikasını almaya karar vermiş ve bu bağlamda bir BT danışmanlık firmasına başvurmuştur. Firma boşluk analizinden ön sertifikasyon denetimine hatta ilk sertifikasyon denetimine rehberlik etmeyi taahhüt etmiştir.

İlk eğitimin ardından ISO 27001 sertifikası edinmek için gerekli çalışmalar danışman firma eşliğinde gerçekleştirilmeye başlanmıştır. Proje aşamaları şu şekilde işlemiştir:

- Yönetim taslağı; kapsam tanımlama ve politika geliştirme
- Varlığın kayıt defterine ekseninde hazırlanan risk değerlendirmesi ve risk işleme
- BGYS belgelerinin tamamlanması
- Personel bilinçlendirme ve teslimat
- İç BGYS denetimi
- Ön sertifika boşluk analizi
- Sertifikasyon denetimi

BGYS iş süreçlerinin gelişimi için anlaşılan danışmanlık firması tarafından ileri koçluk ve bilgi aktarımı hizmeti alınmıştır. Wirefast yöneticilerinden Paul Green ‘’ ISO 27001 standardının tarafımızca hızlı bir şekilde benimsenmesi adına süregelen uzman desteği firmamıza paha biçilmez bir avantaj sağlamıştır. Güvenlik gerekliliklerinin sıkı bir şekilde güncellenmesi her zaman çalışma prensiplerimizin temel yapıtaşını oluşturmuştur. Firmamız Apache ve Red Hat Linux gibi ileri düzey teknoloji platformlarıyla faaliyetlerini yürütmekte ve yeni sistem güncellemelerinin takibini hızlı bir şekilde gerçekleştirmektedir.

Teknik ekibimizin risk içeren değişim sürecini benimsemiş olması ve teknik donanımızın yüksek seviyede olması ISO 27001 standardıyla bizim teknik güvenlik modelimiz arasında birçok paralellik bulmamıza sebep olmuştur. Büyük tatmin yaşadığımız durum ise ISO 27001 standardının bilgi güvenliğini sağlarken yönetim sistemimizi de güçlendirmesi olmuştur. Başta yönetim kurulu başkanımız (CEO) James Powell- Tuck olmak üzere 35 kişilik ekip üyemizin tam desteği ISO 27001 standardının yürürlüğe girmesinde kritik rol oynamıştır.

Diğer teknoloji firmaları yöneticilerinin siber güvenlik gerekliliklerinin iş yapmaya engel teşkil edebileceğini düşünüyor olabilirler lakin bizim deneyimimiz faydadan başka bir şey sağlamamıştır. Taslaktaki detaylar ve kontrol noktalarının kullanımındaki esneklik bilgi güvenliğinin temel yapı taşları olan gizlilik, bütünlük ve erişilebilirlik arasında denge sağlamayı kolaylaştırmaktadır. ISO 27001 standardına uyum sağlamak, firmalara kendi yönetim sistemi süreçlerini hazırlamaları konusunda yardımcı olmaktadır'' açıklamalarında bulunmuştur.

Mayıs 2012 de başlangıç sertifika denetiminin ardından Wirefast ISO 27001 sertifikasını almaya hak kazanmıştır. Süregelen sertifikasyon dönemi içerisinde finansal işler müdürü Paul White '' Wirefast her zaman müşteri bilgilerinin mahremiyetine özen göstermiştir. Sertifikayı edinmek bize bu taahhüdümüzü ve bilgi güvenliğinin uluslararası standartlarda sağlandığını teminat altına alma imkanı vermiştir'' dedi. James Powell- Tuck ise '' Bizim sistemimiz teknolojik seviye anlamında her zaman en iyiler sınıfında yer almıştır ancak ISO 27001 sertifikası bize rakip firmalar karşısında açık bir üstünlük sağlamıştır'' dedi (It Governance, 2013).

4.3.2. Abu dhabi gas ındustries ltd. (GASCO)

1978' den beri doğal gaz çıkarma ve işleme alanında faaliyet gösteren GASCO müşteri tatminini üst seviyelere çıkarmak için ISO 27001 sertifikası edinmiştir. Bu süreçte bir danışmanlık firmasından rehberlik alınmıştır. Sertifikaya sahip olurken edindiği tecrübeleri paylaşan kurum proje yöneticisi Asmaa Al Kindi danışman firmayla yapılan görüşmelerden ortaya bir yol haritası çıkarttıklarını ifade etmiştir. Bu yol haritası temel olarak 3 bölümden oluşmaktadır: Boşluk analizi/ plan aşaması, uygulama ve denetim. Plan kısmında kapsam ve politika tanımlanır, güvenlik organizasyonu inşa edilir ve risk

değerlendirme çerçevesi hazırlanır. Uygulama aşamasında risk değerlendirme ve iç denetim kısmı gerçekleştirilir. Son olarak denetim kısmında takip edilen kontroller ışığında aksiyonlar alınır.

Asmaa Al Kindi' ye göre çalışan farkındalığı, güvenlik gereklilikleri ve üst yönetim desteği ISO 27001 standardının en temel ögelerini teşkil etmektedir. Çalışan tutumu ve çalışanların uyum yetenekleri sertifikasyon edinme süresince kurumu en çok uğraştıran etmenlerden olmuştur.

Bilgi güvenliği yöneticisi Mona Younaes ISO 27001 sertifikasyon sürecine 2007 Ekiminde başladıklarını ve bu tarihten itibaren 8 ay içerisinde sürecin tamamlandığını ifade etmektedir. Bu başarının elde edilmesindeki motivasyon ise kurumun iş pratiklerini geliştirmek ve kurum bilgi varlıklarının korunması olmuştur. Mona Younes sertifikasyon sürecinde izledikleri adımları kısaca açıklamıştır

Plan aşaması/ Boşluk analizi

Gasco boşluk analizini gerçekleştirmek için bir danışmanlık firmasından destek almıştır. En iyi güvenlik uygulamalarından ilham alınarak kurumun var olan güvenlik kontrollerindeki boşluklar tespit edilmiş ve bunları doldurmak için atılması gereken adımlar tanımlanmıştır.

Plan aşamasında bilgi varlıklarının, sistem risklerinin, politika ve prosedürlerin tanımlanmasını içeren bir takım kontrol noktaları danışmanlık firması tarafından hazırlanmıştır. Birkaç örnekle izah etmek gerekirse:

- Destek
- Çalışan hesap kontrolü
- Bilgi güvenliği olay yönetimi
- Risk yönetimi
- Bilgi sınıflandırması

GASCO tarafından önceki senelerde kurulan güvenlik dairesi iş sorumluluklarının takibini yapıyordu. ISO 27001 kapsamında bu dairenin personel sayısı artırıldı. Sonra alınacak aksiyonları tartışmak için bir güvenlik forumu oluşturuldu.

Risk değerlendirme aşamasında GASCO' nun ortaya koyduğu riskler şunlardır:

- Bilgisayar riski
- Personel riski
- Fiziksel güvenlik
- Erişim kontrolü
- Şifre karmaşıklığı riski

Risk değerlendirme aşamasında danışmanlık firmasınca ön planda tutulan hususlar BGYS' nin uygulanması ve sürdürülmesi olmuştur. Ve bu aşamaya risk değerlendirme yaklaşımı geliştirilerek başlanmıştır. Bilgi varlıkları, tehditler, riskler tanımlanmaya gayret gösterilmiş ayrıca herhangi bir varlığın gizlilik, bütünlük ve ulaşılabilirlik özelliğine zarar verebilecek kırılganlıklar tespit edilmiştir.

Uygulama aşaması

Risk değerlendirmenin ardından bir risk işleme planı GASCO tarafından tasarlamıştır. Bilgi güvenliği risklerini yönetebilmek adına uygun yönetim aksiyonları, kaynaklar, sorumluluklar ve öncelikler tanımlanmıştır. Güvenlik takımı risk işleme planı doğrultusunda belirli başlıklara yönelmiştir.

- İnsan kaynakları güvenliği
- Fiziksel ve çevresel güvenlik
- İletişim ve operasyon yönetimi
- Hesap kontrolü
- Bilgi güvenliği olay yönetimi
- İş sürekliliği yönetimi
- Uyumluluk

Risk işleme süreci boyunca BT güvenlik ekibi ölçüm kriteri belirlemiş ve güvenlik için farkındalık çalışmaları gerçekleştirmişlerdir. Ekip ayrıca hizmet seviyesi anlaşmaları hazırlamışlardır. Bu anlaşmalar BT bölümü ile diğer bölüm ve departmanlar arasında imzalanır.

Mona Younaes' GASCO personelinin güvenlik farkındalığının ve eğitiminin oldukça yüksek seviyede olduğunu ifade etmiştir. ISO 27001 standardı dahilinde personel farkındalığının artırılması için çok farklı metotlar kurum tarafından uygulanmıştır. Duvar posterleri hazırlanmış ve düzenli aralıklarla farkındalık mailleri atılmıştır. Bunun dışında sayısız bilgilendirme oturumu kurum tarafından düzenlenmiştir. Mona Younaes konuşmasında ISO 27001' e geçiş sürecinde personelin yaşadığı zorluklara yer vermiştir. Güvenlik sisteminin baştan sona değişmesi personel için zorluklar ortaya çıkarmıştır. Çünkü bir takım spesifik görevlerin gerçekleştirilmesi değişmiş ve bu durum onların zaman tüketimlerini artırmıştır. Örneğin: BGYS sistemine geçmeden önce personel BT bölümüne gidip belirli bir görev için rahatça soru sorabiliyorlardı ancak BGYS yönetiminden sonra bu işlemi gerçekleştirebilmeleri için birçok adımdan geçmeleri gerekmektedir. BGYS' ye uyum sürecinde en çok zorlanılan kısım ise personelin değişikliğe karşı direnmesi, yeniliklere uyum sağlamayı reddetmesi ve eski alışkanlıklarında diretmesi olmuştur. Başlangıçta değişikliklerin hemen kabul edilmemesine rağmen değişiklerin faydaları personelce gözlenmeye başlandıktan sonra zaman içerisinde uyum sağlanmaya başlanmıştır.

Denetim aşaması

GASCO yönetimi BGYS uygulamalarını takip etmiştir. Ayrıca iç denetim ekibi tarafından BGYS denetimi sağlamıştır. Ancak kurum profesyonel bir denetim firmasından yardım almayı ihmal etmemiştir. Denetim firması 6 ayda bir risk yönetim testini GASCO için gerçekleştirmektedir. Sertifika edinimi gerçekleştikten sonra denetim firması yıllık denetimini gerçekleştirmekte ve 3 yılda bir tekrar değerlendirme yapmaktadır (Abu Talib, El Barachi, Khelifi ve Ormandjieva, 2012).

SONUÇ VE ÖNERİLER

Yaygın bir şekilde iddia edildiği üzere küçülen ve küreselleşen dünyada şeylerin iletişim hızı önceki dönemlerle kıyaslanmayacak seviyelere gelmiştir. Uzak mesafeler arası iletişim ve haberleşme ilk zamanlarda güvercin, duman, ateş, çan vb ekipmanlarla sağlanırken elektriğin keşfiyle hız kazanmıştır. Kablolar vasıtasıyla iletişim sağlayan telgraf sadece belirli uyarıları karşı tarafa iletebilmiştir. Daha sonra ortaya çıkan telefon ise sesin iletimini sağlamıştır. Nihai olarak gelinen noktada ise görüntü ve ses eş zamanlı olarak arzu edilen noktaya iletilebilmektedir. Dokunma, koklama ve tatma hissinin iletilip iletilemeyeceği ise tartışma konuları arasında yerini almış bulunmaktadır.

Bu gelişmelerin baş müsebbibi ve sonucu olan teknoloji, geliştikçe daha çok bilginin üretilmesine, iletilmesine ve saklanmasına vesile olmuştur. Daha çok bilginin üretilmesi ve saklanması ise teknolojinin ilerlemesini tetiklemiştir. Bu şekilde bir döngü içerisinde gelişen teknoloji bilgiyi kuvvetlendirmiş, kuvvetlenen bilgi ise teknolojiyi geliştirmiştir ve sirkülasyon bu minval üzerine devam etmektedir.

Modern hayatın birçok alanını daha konforlu hale getiren teknolojik gelişmeler ilk dönemlerde bireysel çabalarla ve ufak çapta atölyelerden doğduysa da zaman içerisinde çeşitli nedenlerden dolayı belirli başlı kurum ve kuruluşların varlığını gerekli kılmıştır. Her ne kadar her keşif belirli sayıdaki insanın zihninde başlayan bir yolculuk da olsa küreselleşen dünya pazarına ulaşmak isteyen her fikir küresel iletişim ağı olan bir kuruluşa muhtaç olmaktadır. Bu durum bilgi kurum ve kuruluşların tekeline almasına vesile olmuştur. Daha çok bilgiye sahip olan kuruluş daha da zengin hale gelmiştir. Gelişen ve zenginleşen kurumlar küçük ölçekteki firmaları elemine ederek daha da güçlenmiş bir piyasa metaı olan bilgiye verilen ehemmiyet bu ölçüde fazlalaşmıştır. Çünkü yaygın olarak kabul edilen bir başka gerçek ise daha çok kıymetli eşyaya sahip olanın daha güçlü olduğu, bilgi çağında ise en kıymetli eşyanın bilgi olduğudur. Dolasıyla gücü elinde bulundurmak ve topluma yön vermek için olmazsa olmaz unsur bilgi olmuştur.

Bilginin insan ve toplum nezdinde kıymeti artarken bir başka deyişle bilinirken kolay yoldan bilgi elde etmek isteyen kurum ve kuruluşlar açısından bilginin cazibesi bir başka boyut kazanmıştır. Kurumlar daha çok bilgiye sahip oldukça daha da güçlenmiştir ancak o bilgiyi ele geçirmek isteyen art niyetli kurumların sayısı da artmıştır. Bu durum

kurumlar üzerindeki baskı ve tehdidi artırmıştır. Bu tehditlerin basit bir endişeden çok daha ötede olduğunu son dönemde firmalar (Yahoo, Twitter) üzerinde yaşanan siber saldırılar ispat etmiştir. Milyonlarca $ zarara giren dev firmaların kimi iflasın eşiğine gelirken kimi edindiği tecrübelerle hayatına devam etmeyi başarmıştır. Kurumlar siber saldırıdan bu şekilde etkilenirken bilgi çağında dev kurumlar şeklinde yönetilen devletler de siber tehditten üstlerine düşeni fazlasıyla almışlardır. Çünkü devletler siber saldırıya uğradığında sadece maddi kayıp vermekle kalmamakta aynı zamanda ekonominin kalbi sayılabilecek merkez bankası çökebilmekte, ulaşım sekteye uğrayabilmekte ve ekonomi kaosa sürüklenebilmektedir. Eskiden askeri alanda meydana gelen savaşlar artık siber arenada gerçekleşmektedir. Tehditlerin bu boyuta ulaşması devletleri bütçelerinde bu alana daha fazla kaynak ayırmaya itmiştir. Hatta bir takım devletler kendi siber savunma ekiplerini kurarken bazısı da siber saldırı konusunda uzmanlar yetiştirmeye başlamıştır.

Artan tehditlere karşı bilgi güvenliğini temin etmek için alınan tedbirlerde gelişmektedir. Yaşanan saldırılardan sonra alınacak aksiyonların bir fayda sağlamayacağı takdire şayandır. Bu bağlamda saldırı gerçekleşmeden alınacak önlemler daha uzun ömürlü ve etkili çözümler sunmaktadır. Kurumların tedbir almaları gereken tehdit unsurları ise oldukça fazladır ve kurumdan kuruma değişmektedir ayrıca farklı departmanlarda farklı aksiyonlara ihtiyaç duyulabilir. Örneğin: Personelden kaynaklanan tehditler, çevreden kaynaklanan tehditler, ağ kaynaklı tehditler. Her tehdit kaynağı için farklı bir personel tayin edilemeyeceğinden tehditleri ve kurumu bir bütün olarak ele alan, farklı tehdit unsuruna farklı çözümler geliştirmek yerine bütüncül bir güvenlik sistemi getirmek, hem maliyet hem de zaman açısından kurumlara avantaj sağlamaktadır. BGYS bu alandaki ihtiyacı tatmin için kurumlar tarafından ortaya çıkarılmış bir sistemdir.

BGYS kurumları departmanlarına ya da bölümlerine göre ayırt etmeden bir bütün olarak ele alan, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini teminat altına almak için ortaya çıkarılan bir kurallar bütünüdür. Kurumların belirli departmanlarına endekslenemeyen tamamına nüfuz etmesi gereken BGYS, bilginin bütünlüğüne endekslenip erişilebilirliğini ve gizliliğini ikinci plana atıldığında yine başarısızlıkla sonuçlanabilmektedir. Zira bilgi güvenliğinin sağlanması için gerekli olan sacayaklarından biri çok sağlam diğer ikisi sallantıda olduğu zaman denge sağlanamaz ve BGYS tam anlamıyla fonksiyonlarını icra edemez.

BGYS' nin kurumdan kuruma farklılık göstermeyen ulusal hatta uluslararası bir standarda dönüşmesi gerekliliği, ISO27001 standardını ortaya çıkarmıştır. ISO 27001 finansal veri, hassas müşteri bilgileri veya entelektüel varlıkları koruma altına alan sağlam bir sistemdir. Bu sistem kurumların bilgi varlıklarını yönetmesine ve korumasına katkı sağlar ki kurum tüm konsantrasyonunu kendi öz faaliyetine kanalize edebilsin. ISO 27001 kurumlara sadece bilgi güvenliğini teminatını vermez aynı zamanda tedarikçilere, müşterilere ve piyasaya kurumun bilgi güvenliğini sağlama konusundaki yeteneğini açık bir şekilde ifade eder. Bu bağlamda kurumun itibarını sağlamlaştırır ve kurumun geleceğe güvenle bakmasına katkıda bulunur.

ISO 27001 standardının kurumların bilgi güvenliğini teminat altına alırken vazgeçilmez iki enstrümanı vardır. Bunlar; varlıkların sınıflandırması ve risk analizidir. Varlıkların sınıflandırması esasen kurumun sınıflandırılmasıdır. Zira kurumda bilgisayarlar, yazıcılar, yazılımlar, ısıtma cihazları hatta personel bile kurum varlıklarından olarak kabul edilmektedir. Bu sebepten varlıkların sınıflandırılması ve varlık değerlendirmesi yani hangi varlığın kurum için vazgeçilmez olduğu hangi varlığın yokluğunda kurumun temel fonksiyonlarını idame ettirebileceği konularının tespiti ISO 27001' in temel yapıtaşlarını oluşturmaktadır. Kurumun bütün varlıklarının dökümünün yapılması ve sınıflandırılmasıyla genel bir fotoğrafının çekilmesinin ardından risk analizi safhası başlamaktadır. Risk analizinde genel olarak kurumun yüzleşebileceği tehditler sıralanır ve bu tehditlerin gerçekleşme olasılıkları ortaya konur. Bu işlemin ardından gerçekleştikleri takdirde kurum bünyesinde oluşturacakları etki hesaplanır. Son olarak hangi risk unsuruna nasıl muamelede bulunulacağı tespit edilir ve harekete geçilir. Yukarıda özetlenen ISO 27001 BGYS uygulanırken kurumların dikkat etmesi gereken birkaç husus aşağıda yer almaktadır:

- Üst yönetim kararlılığı

ISO 27001 BGYS uygulamalarında sık yapılan hatalardan biri yönetimin algısıdır. Sadece birkaç departmanı ilgilendirmeyen tüm kurumu ele alan bir yönetim sistemi olan bilgi güvenliği yönetim sisteminde başarı sağlanabilmesi için üst yönetimin ISO 27001 gerekliliklerine kendinin tabi olması ve kurumun içinde uygulanmasının takipçisi olduğunu tüm kuruma ilan etmesi gerekmektedir. Bunun için bildiriler, uyarılar, hatırlatmalar, yaptırımlar tercih edilebilir.

- Bilgi güvenliği ekibinin kurulması

Herhangi bir birime tali görev olarak bilgi güvenliği sorumluluğu verilmesi yerine bizzat bu hususla ilgilenen bilgi güvenliği ekibi/ biriminin kurulması hem kurumun bu konudaki samimiyetini ve azmini gösterir hem de uzun vadede bilgi güvenliği çalışmalarının devamlılığını teminat altına alır. ISO 27001 sertifikasını edinme sürecinde ve sonrasında bu tür birimin varlığı kaçınılmazdır. Zira kurum için bir sertifikadan öte bir yaşam tarzı şekline dönüşmelidir.

- Çalışan farkındalığı ve eğitimi

Bilgi güvenliğinin temin edilmesinde en zayıf halka olarak adlandırılan personel düzenlenen saldırılarda ilk hedeflerden biri olmuştur. Siber saldırıların bir kısmı personel dalgınlığından veya eğitimsizliğinden kaynaklanmaktadır. Bu açıdan personelin farkındalığı büyük önem arz etmektedir. Personel farkındalığı oluşturmak için eğitim ve seminerler düzenlenmesinin yanı sıra bildiriler yayınlanması, afişlerin asılması deneme maillerinin atılması kurumların uygulayabileceği yöntemlerden birkaçıdır.

- Sertifikasyon süreci

ISO 27001 sertifikasyon sürecinde aslan payı kuruma düşmektedir. Danışmanlık firmaları kuruma varlıklarını, risklerini tespit etmesinde ve bundan sonraki aşamalarda sadece rehberlik edebilirler. Bunun dışında bütün yük kurumun omuzlarına düşmektedir. Bu bağlamda ISO 27001 sertifikasını edinmek isteyen bir kurumun baştan sona bir değişim geçirmesi gerektiğinin ve bunu yaparken danışmanlık firmalarının rehberlikten başka hiçbir fonksiyonu olmadığının farkında olmalıdırlar.

KAYNAKLAR

Abu Talib, M., El Barachi, M., Khelifi, A., and Ormandjieva, O. (2012). Guide to ISO 27001: UAE Case Study. *Issues in Informing Science and Information Technology*, 332- 346.

Allahverdi, M. ve Alagöz, A. (2011-3). Kurumsal Bilgi Sistemi ve Muhasebe Bilgi Sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi*, 47-61.

Allen, M. (2005). Eğitimin Ötesinde. *Executive Excellence Dergisi, Sayı: 104*, 15-16.

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

Bingöl, U. (2010). *İSO 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 Bankası Anonim Şirketi.

Budak, Ö. S. (2015). *Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki Ve Teknik Liseler Örneği.* Atatürk Üniversitesi.

Canberk, G. ve Sağıroğlu, Ş. (Cilt: 9 Sayı: 3 , 2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine. *Politeknik*, 165-174.

Cybersecurity Ventures. (2016). *Cyber Security Market Report Q3 2016.* Northport NY: Cybersecurity Ventures.

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

Danışmanlık, S. M. (2017). *2017 Nisan- Haziran Dönemi Siber Tehdit Durum Raporu.*

Doğantimur, F. (2009). *Iso 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği.* Ankara: T.C. Maliye Bakanlığı Stareji Geliştirme Başkanlığı.

Emhan, A. (2009). Risk Yönetim Süreci ve Risk Yönetmekte Kullanılan Teknikler. *Atatürk Üniversitesi İktisadi ve İdari Bilimler Dergisi, 23*(3).

Enginoğlu, G. A. (2013). Bilgi Yönetimi Ve Kalite Yönetim Sistemleri Arasındaki İlişkinin Açıklanmasına Yönelik Bir Araştırma. *SOSYAL ve BEŞERİ BİLİMLER DERGİSİ,* 5(1).

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı.* Ankara: ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim A.Ş.

Eskiyörük, D. (2007). *UEKAE BGYS0004- BGYS Risk Yönetim Süreci Kılavuzu.* Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Güneş, Ş. (2009). *Kurumsal Risk Yönetimi ve Türkiye' de Farkındalığına İlişkin Bir Uygulama.* İstanbul: İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü.

ISO/ IEC 27001. (2013). *Information Technology- Security Techniques- Information Security Management System- Requirements.* BSI Standarts Publication.

İnternet: Hinson, G. (2017, 11 16). *The ISO27K İnformation Security*. http://www.webcitation.org/query?url=http%3A%2F%2Fwww.iso27001security.com%2FISO27k_Standards_listing.pdf&date=2017-11-16 adresinden alınmıştır

İnternet: It Governance. (2013). *Case Study- Wirefast*. itgovernance: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.itgovernance.co.uk&date=2018-02-28 adresinden alınmıştır

İnternet: Özbilgin, İ. G. ve Özlü, M. (t. y.). ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve Ağ Yönetimi Politikası: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.academia.edu%2F31607289%2FISO_27001_Bilgi_G%C3%BCvenli%C4%9Fi_Y%C3%B6netim_Sistemi_ve_A%C4%9F_Y%C3%B6netimi_Politikas%C4%B1&date=2018-02-28 adresinden alınmıştır

İnternet: Şen, Ş. (t. y.). *ISO 27001 Kurumsal Bilgi Güvenliği Standardı.* http://www.webcitation.org/query?url=http%3A%2F%2Fab.org.tr%2Fab13%2Fsunum%2F216.pdf&date=2018-02-28 adresinden alınmıştır

Kahraman, S. (2006). *Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi Ve Aselsan A.Ş' De Uygulaması.* Eskişehir: Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Kandemirli, B. M. (2012). *Bilgi Teknolojileri Güvenliği ve Sigorta Şirketinde SO/IEC 27001 Standartları Çerçevesinde Bilgi Güvenlik Yönetim Sistemi Uyguluması.* İstanbul: Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü.

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

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

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

Öztürk, G. (2008). *Bilgi Güvenliği Politikası Oluşturma Kılavuzu.* Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Rossi, R. (2009). *How Writing Began.* New York: Marshall Cavendish Benchmark.

Sagıroğlu, Ş., Ersoy, E. ve Alkan, M. (2007). *Bilgi güvenliğinin kurumsal bazda uygulanması. Bildiriler Kitabı* . Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Kkonferansı.

STM. (2015). *Siber Güvenlik Tehdir Raporu.* Ankara: STM.

STM. (2016). *2016 Ekim- Aralık Dönemi Siber Tehdit Durum Raporu.* Ankara: STM.

Şen, Ş. ve Yerlikaya, T. (2013). *ISO 27001 Kurumsal Bilgi Güvenliği Standardı.* Trakya: Akademik Bilişim 2013 Konferans Bildirileri Kitabı.

TS ISO/IEC Guide 73. (2012). *TS ISO/IEC Guide 73.* Ankara: Türk Standardları Enstitüsü.

Usgt. (2011). *Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu.* Ankara: Tübitak.

Vural, Y. ve Sağıroğlu, Ş. (2007). *Kurumsal Bilgi Güvenliği: Güncel Gelişmeler.* Bildiriler Kitabı uluslararası katılımlı bilgi güvenliği ve kriptoloji konferansı .

Vural, Y. ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniv. Müh. Mim. Fak. Der.*, Cilt: 23, 507- 522.

WEF, W. E. (2016). *The Global Risks Report 2016 11th Edition.* Geneva: World Ekonomik Forum.

Yahyaoğlu, G., Korkmaz, M. ve Akman, G. (2011). Bankacılık ve Risk Yönetiminin Bir Banka Üzerinde Uygulanması ve Sonuçlarının Hukuksal Açıdan Değerlendirilmesi Konusunda Uygulamalı Çalışma. *Akademik Bakış Dergisi*, 2-3.

Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı. *DENETİŞİM*, 45-59.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: ÖTEGEN, Mehmet
Doğum Yılı ve Yeri	: 1987 / Seyhan
Telefon Numarası	: 0 (312) 508 72 46
Mail	: mehmetotegen@gmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	Gazi Üniversitesi-İşletme	2011
Lise	Özgören Lisesi	2005

İş Deneyimi

Yıl	**Yer**	**Görev**
2014 - Halen	İller Bankası	Uzman Yardımcısı

Yabancı Dil

İngilizce

Yayınlar

-

Hobiler

Kitap okumak, seyahat


İLBANK
TÜRKİYE'NİN YAPICI GÜCÜ