BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ: BİLGİ GÜVENLİĞİ UYGULAMA MÜLAKATLARI

İsmayil Gökhan AKAY

Yüksek Lisans Tezi

Danışman
Yrd. Doç. Dr. Sevgi GÖNÜLLÜOĞLU

BİLECİK, 2014
Referans No: 10035551

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ: BİLGİ GÜVENLİĞİ UYGULAMA MÜLAKATLARI

İsmayil Gökhan AKAY

Yüksek Lisans Tezi

Danışman
Yrd. Doç. Dr. Sevgi GÖNÜLLÜOĞLU

BİLECİK, 2014

Referans No: 1003551

T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS JÜRİ ONAY FORMU

05 /06 /2014

Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun 21.05.2014 tarih ve 117/9 sayılı kararıyla oluşturulan jüri tarafından 05.06.2014 tarihinde Tez Savunma Sınavı yapılan İsmayil Gökhan AKAY'ın "Bilgi güvenliği yönetim sistemleri: Bilgi güvenliği uygulama mülakatları" konulu tez çalışması İşletme Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

TEZ DANIŞMANI : Yrd. Doç. Dr. Sevgi GÖNÜLLÜOĞLU

ÜYE : Doç. Dr. İsa İPÇİOĞLU

ÜYE : Yrd. Doç. Dr. Tolga TORUN

ONAY

Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun ...../...../..... tarih ve ...../...../..... sayılı kararı.

İMZA/MÜHÜR

Madde 43-(3) Yüksek lisans tez sınavı jürisi ve tez savunma sınav tarihi, ilgili ABD/ASD başkanlığının önerisi ve EYK kararı ile belirlenir. Önerinin uygun bulunmaması halinde tez jürisini ilgili EYK belirler. Jüri, biri öğrencinin tez danışmanı ve en az biri enstitünün başka bir ABD/ASD'den ya da başka bir yükseköğretim kurumundan olmak üzere üç veya beş asıl, birisi ilgili ABD/ASD'den, diğeri de enstitüye bağlı başka ABD/ASD'den veya başka bir yükseköğretim kurumundan olmak üzere iki yedek öğretim üyesinden, öğretim üyesi bulunmadığı takdirde doktora/sanatta yeterlik derecesine sahip öğretim elemanları ya da sanatçı öğretim elemanlarından oluşur. ABD/ASD başkanı, jüri üyelerini uzmanlık alanlarını göz önünde bulundurarak önerir. Jürinin üç kişiden oluşması durumunda ikinci tez danışmanı jüri üyesi olamaz.

TEŞEKKÜR

Hazırlamış olduğum tez çalışmasında; konu seçiminden, araştırma metotlarına kadar beni her zaman açık görüşlülükle destekleyen ve cesaretlendiren değerli Danışman Hocam Yrd. Doç. Dr. Sevgi GÖNÜLLÜOĞLU'na tez çalışmalarım esnasındaki yardımlarından dolayı ve akademik hayattaki yönlendirmelerinden dolayı kendisine teşekkürü bir borç bilirim.

Yapmış olduğum araştırmalar esnasında bana sabırla destek olan eşim Nurdan AKAY'a, kızım Aliye AKAY'a ve sevgili aileme teşekkür ederim.

Tez araştırmam esnasında mülakat yaptığım kuruluşların çalışanlarına, bize tüm samimi duygularıyla yardımcı oldukları için teşekkür eder, araştırmam esnasında emeği geçen ve bana yardımcı olan herkese çok teşekkür ederim.

İsmayil Gökhan AKAY

Bilecik, 2014

ÖZET

“Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları”

İsmayil Gökhan AKAY

Günümüzde bilgi teknolojilerinin gelişimi birçok kolaylığı ve imkânları bizlere sunarken, birçok tehdidi de beraberinde getirmektedir. Bilgi teknolojilerindeki gelişmelere paralel olarak da bilgiye sahip olmanın değeri de gittikçe artmaktadır. Bilgi güvenliği; istenilen yer ve zamanda, talep edilen miktarda, yetkilendirilmiş kişilerin bilgiye erişimini içerir. Ayrıca bilginin muhafaza edilmesi, bir yerden başka bir yere taşınması ve yapılan bu işlemler esnasında herhangi bir değişime uğramadan ve gizlilik içerisinde yürütülmesini amaçlar. Bilgi güvenliğinin temel ilkeleri; gizlilik, erişilebilirlik ve bütünlüktür. Bilgi güvenliği denildiğinde sadece teknik personeli ilgilendiren ve teknik donanımla ilgili konular akla gelir. Bilgi güvenliği konusunda en önemli etken insandır. İnsan faktörünün de sistem içerisinde etkin olabilmesi için en önemli ihtiyaç bilgi güvenliği eğitimleridir. Bilgi güvenliği sistemleri kurulurken hedeflenen en temel hedef çalışanlar üzerinde farkındalık yaratmaktır. BGYS kurmayı hedefleyen bir kuruluş, kendi dinamiklerine göre uluslararası geçerliliği olan bir standardı kendine rehber seçmeli ve çalışmalarını da bu doğrultuda yürütmelidir. Standartlar bizlere nelerin yapılması gerektiğini açıklamaktadır. Nasıl yapılacağı konusunu ise bizlere yardımcı yayınlar ve danışmanlık firmaları öğretmektedir. Bu araştırmamızda dünyada kabul görmüş en güncel BGYS standartları hakkında kısaca bilgiler verdik. Dünya genelinde en kapsamlı BGYS standardı olarak kabul görmüş olan ISO27001 BGYS standardının mevcut sürümü ve yeni sürümü birlikte değerlendirilerek BGYS kurulum, kontrol, denetleme ve iyileştirme faaliyetleri açıklanmıştır. Yenilenen ISO27001 standardının “annex sl” yapısı ve yenilenen kontrol maddeleri tanıtılmıştır. ISO27001 standardının, diğer yönetim sistemleri ile uyumu karşılaştırılmıştır. BGYS kurulumu ile ilgili çok fazla detaylı kaynak olmamasından dolayı, BGYS sertifikası sahibi iki kuruluşla BGYS kurulumu hakkında mülakatlar gerçekleştirdik.

Anahtar Sözcükler

Bilgi Güvenliği Yönetim Sistemleri, Annex Sl, ISO27001, Farkındalık, Bilgi Güvenliği Eğitimi, BGYS Denetimleri, BGYS Sertifikası, Kurumsal Bilgi Güvenliği

ABSTRACT

"Information Security Management Systems: Information Security Application Reviews"

İsmayil Gökhan AKAY

Not only does improvement in technology of information present many comfortand capability, but also brings many threats along with a today. Besides that, the more technology of information has improvement, the more value of having information increases. Information technology includes authorized person's reaching information that is required in quantity of a given time and place. Furthermore, protecting and keeping information aims both transferring it in one place to another and executing that process in secrecy by not changing any part of it. Fundamentals of information security a resecrecy, unity and reach ability information security suggestsonly topics that are related technical person and hardware. The most important factor in information security is human. Besides, the most require done to be able to use human factor effectively is information security teachings. Hence, most fundamental aim in establishing information technology systems is toraise awareness on working groups. An institution, that aims to execute ISMS, must select a Standard that is validinter nationally itself and execute its concern in that pattern. Standards explain what is required to reach firms target. Additional documents and consultant firms teach also how it can be done. In this research, wetry to gives hort summary related to ISMS standards that are accepted globally. The most comprehensive ISMS standard, ISO 27001 that is accepted globally is evaluated by new and present product to gether and also ISMS setting, control, inspection and upgrading are explained. Renewed ISO27001 standard's annexsl structure and renewed control parts are presented. Conformity of ISO27001 standard and other management systems is compared. We review two firms having ISMS certificates in that there is no detailed resource.

Keywords

Information Security Management Systems, Annex Sl, ISO27001 Standard, Awareness, Information Security Education, ISMS Inspections, ISMS Certificate, Enterprise Information Security.

İÇİNDEKİLER

İKİNCİ BÖLÜM
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ STANDARTLARI

ÜÇÜNCÜ BÖLÜM

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ GEREKSİNİMLER STANDARDI

DÖRDÜNCÜ BÖLÜM

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURULUMU VE YÖNETİMİ

BEŞİNCİ BÖLÜM

ISO27001 BGYS SERTİFİKASI HAKKINDA YAPILAN MÜLAKATLAR

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR

ASCII.	Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi (American Standard Code for Information Interchange)
BGS.	Bilgi Güvenliği Sistemi
BGYS.	Bilgi Güvenliği Yönetim Sistemi
BOME.	Bilgisayar Olaylarına Müdahale Ekibi
BSI.	İngiliz Standartlar Enstitüsü (British Standards Institute)
BT.	Bilgi Teknolojileri
BTK.	Bilgi Teknolojileri ve İletişim Kurumu
CEN.	Avrupa Standartlar Komitesi (European Committee for Standardization)
CERT.	Bilgisayar Olaylarına Müdahale Ekibi (Computer Emergency Response Team)
CGEIT.	Sertifikalı Kurumsal Bilgi Teknolijeleri Yönetişim Uzmanı (Certified in the Governance of Enterprise Information Technology)
CISSP.	Bilgi Sistemleri Güvenlik Uzmanlığı Sertifikası (Certified Information Systems Security Professional)
CISM.	Sertifikalı Bilgi Güvenliği Yöneticisi (Certified Information Security Manager)
COBIT.	Bilgi Sistemleri Denetim ve Kontrol Birliği (Control Objectives for Information and Related Technology)
CRISC.	Risk ve Bilgi Sistemleri Kontrolü Onayı
ENISA.	Avrupa Ağ Ve Bilgi Güvenliği Ajansı
FTP.	Dosya Aktarım Protokolü (File Transfer Protocol)
HYS.	Hizmet Yönetimi Sistemi
GSM.	Mobil İletişim İçin Küresel Sistem (Global Systemfor Mobile Communications)
IAF.	Uluslararası Akreditasyon Formu

IEC.	Elektrik Sistemleri Uluslararası Konseyi (International Electro technical Commission)
IRCA.	Uluslararası Denetçi Eğitim ve Belgelendirme Birliği (International Register of Certificated Auditors)
ISACA.	Bilgi sistemleri denetim ve kontrol birliği (Information Systems Audit and Control Association)
ISACF.	Bilgi Sistemleri Denetim ve Kontrol Kurumu (Information System Auditand Control Foundation)
ISMS.	Information Security Management System (Bilgi Güvenliği Yönetim Sistemi)
ISO.	Uluslararası Standartlar Örgütü (International Organization for Standardization)
IT.	Information Technology (Bilgi Teknolojileri)
ITIL.	Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technology Infrastructure Library)
KOSGEB.	Küçük ve Orta Ölçekli İşletmeleri Geliştirme İdaresi Başkanlığı
OECD.	Ekonomik Kalkınma ve İşbirliği Örgütü (Organisation for Economic Co-operationand Development)
PUKÖ.	Planla – Uygula – Kontrol et – Önlem al
TCK.	Türk Ceza Kanunu
TÜBİTAK.	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜRKAK.	Türk Akreditasyon Kurumu
TSE.	Türk Standartları Enstitüsü
UEKAE.	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

GİRİŞ

Tarih boyunca insanoğlu hayatını idame ettirebilmek adına bir arayış içinde olmuştur. Geçmişte insanoğlunun tek derdi belki de yarına çıkabilme adına yiyecek bir lokma ve güvenli bir yer bulabilmekti. Bu isteklerini yerine getirirken bile, bir bilgi sahibi olması gerekiyordu. Zaman ilerledikçe yaşam içerisindeki bilgi birikimi artmış ve bu temel ihtiyaçlarını kolaylıkla sağlayabilir hale gelmiştir. Fakat o zamanda elde ettikleri ona yetmemeye başlamış ve yeni arayışlar içerisine girmiştir. Yeni bir şeyler elde ettikçe, elindekiler ona yetmez olmuş, hayatını daha kolay ve daha rahat yaşama beklentileri sürmüştür. Ne zamanki, kendi sahip olduklarını bir başkasında gördüyse, kendini farklı kılmak adına, yeni bir arayış içerisinde olmuştur. Günün birinde şu gerçeğin farkına varmıştır. Eğer bir kişinin bildiğini herkes biliyorsa, sen bir adım geride kalmışsın demektir. Yarında var olmak istiyorsan işine yarayacak bilgilere herkesten daha fazla ve daha hızlı sahip olmalısın. Bildiklerini de, daha iyisini öğrenene kadar başkalarından korumalısın. Hayatta kalmak istiyorsan doğanın bu kuralına uymalısın.

Günümüzde bilgiye sahip olmak, diğerlerinden bizi ayıran temel özellikler haline gelmeye başlamıştır. Elinde bilgiyi tutanlar, gücünde sahibidirler. Bilgi, sahip olunan varlıklar içerisinde en değerlisidir. Son yüzyılda bunun farkına varılmış ve yaşadığımız çağ bilgi çağı olarak adlandırılmıştır. Teknolojik alanda yaşanan hızlı gelişmeler insanlığın başını hızlı bir şekilde döndürmeye devam etmekte, insanlığı gittikçe şaşırtmaktadır. Bize sunulan bu yeniliklerle gitgide hayatımız bir yandan kolaylaşırken diğer yandan farkında olmadan zorlaşmaya başlamıştır.

Artık ihtiyacımız olan her şeye daha çabuk ve daha kolay ulaşabilir hale geldik. Bu sayede zamanımızı daha etkin kullanma ve daha az zahmetle daha kaliteli bir yaşam sürme imkânları elde ettik. Fakat bizlerde daha değerli bir yaşam içinde, daha fazla varlıklar içerisinde yaşadığımız için bizlerde ister istemez birilerinin hedefi haline gelmeye başladık. Nasıl evimizden çıkmadan dış dünyadaki işlerimizi bir telefonla veya bir bilgisayarla hızlı bir şekilde halledebiliyorsak, aynı sürecin bizler için tersten işlememesi de kaçınılmazdır. Bizimde evimize aynı kapılardan daha hızlı ve daha kolay bir şekilde girilebilir hale gelmiştir. Önceleri kapımızı kilitleyip evimizde güvenli bir

şekilde otururken, şu anda kilitlediğimiz evimizden başkalarının dünyalarına bizler giriyor ve çıkarken de kapıyı çoğu zaman çekmeyi unutuyoruz.

İçinde bulunduğumuz zaman dilimi bilgi ve iletişim çağı olarak anılmaktadır. Bu çağı yönetenlerde bilgiye sahip olanlardır. Bilgiye sahip olmak sadece bu anın hâkimi olmayı sağlar. Eğer yarınlar içinde söz sahibi olmayı düşünüyorsanız, sahip olduğunuz bilgi ve beceriyi güvenli bir şekilde muhafaza etmeniz gerekir. Birey olarak sahip olduğumuz bilgi birikimini korumak daha kolay iken; bir topluluk, bir kurum, bir firma olduğumuzda bunun korunması daha zor bil hal alır. Bunun sebebi sahip olunan varlıkların artmasıyla, her hangi bir ihlal olayında kayıpların artması risklerini çoğaltacaktır. Risk tabanlı yaklaşımlarla belli standartlar takip edilerek bilgi güvenliği hassasiyeti daha kolay sağlanabilmektedir. Son yıllarda ortaya çıkan uluslararası standartlar bu alanda rehber niteliğindedir. Bu standartlar arsında şu anda ihtiyaca cevap veren en kapsamlı olanı ISO27001 Bilgi güvenliği yönetimi sistemidir. Bu standarttın zorunlu olan maddeleri sağlandıktan sonra geriye kalan koşulları sağlamak kurumlara kalmıştır.

Bilgi güvenliği yönetim sistemlerine geçmeden önce bilgi kavramının üç temel unsuru öğrenmek gerekir. Bunlar gizlilik, bütünlük ve erişilebilirliktir. Bu üç temel kavram herkes için farklı bir öneme sahiptir. Ortaya konan bilgi; karşı tarafın bizlerden ne beklediğine, nasıl ulaşmak istediğine ve ne zaman elde etmek istediğine göre farklılıklar gösterir. Örneğin online bilet satışı yapan bir firma için erişilebilirlik çok daha fazla öneme sahip iken, bütünlük ve gizlilik ikinci planda yer alacaktır. Yeni buluşların ortaya konulduğu bir araştırma şirketinde, internet üzerinden kesintisiz araştırmalar yapmak önemli olabilir fakat birinci öncelik yapılan araştırmaların gizliliği ve başka firmaların eline geçmesini engellemektir. Bir kütüphanede öncelik araştırmacının aradığını tamamıyla, bütünüyle bulabilmesidir. Gizlilik ve erişilebilirlik arka planda yer alır.

Bilgi muhafaza edildiği ortamlara göre de farklılıklar gösterebilir. Bir haber bir firmanın internet sayfasında, gazetesinde ve televizyon kanalında yer alabilir. Bu bilgiyi karşı tarafın nasıl ne zaman ve nasıl bir beklenti içinde elde etmek istediğine göre bilgiye biçtiği değer ortaya çıkar. Haberlerden elde edeceği bir bilgi kendisi için önem arz etmeyen bir kişi ek bir masrafa girmeden akşam haberleriyle televizyondan bu

bilgiyi elde etmek isteyebilir. Başka bir ajansta görevli haberci içinse haberde sürat ön plana çıkmakta ve gerekli ek masrafların (internet ücreti, mobil cihaz) yarattığı sonuçlar kabul edilebilir bir hal almaktadır. Her iki kişide istedikleri bilgiye erişmektedirler fakat her ikisinin de beklentilerinin farklı olması bilginin sunumunda da ve pazarlanmasında farklılıklar ortaya koymaktadır. Kişi ve kurumların bilgi sermayesi için; öncelikle karşı tarafın beklentilerini anlaması ve ardından bilgiyi sınıflandırarak bilginin sunumunda ve bilginin korunmasında tedbirler alması gerekmektedir.

Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel bilgilerin güvenliği de sağlanamaz. Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir (Schmidt, 2004:24). Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir. Kurumsal bilgi güvenliği insan faktörü, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı yönetilmesi zorunlu olan canlı bir süreçtir (Vural ve Sağıroğlu, 2007:192).

Bilgi güvenliği konusunda en kritik faktör, insan faktörüdür. İstediğiniz kadar gelişmiş teknolojiler kullanın, istediğiniz kadar kaliteli eğitimler verin yine de insan faktörü bilgi güvenliği farkındalığını yakalayamadığı sürece hala korunma altında değilsinizdir. Bilgi güvenliği kendini yenileyen her zaman yeniliklere açık bir süreçtir. En son standartlarda, en son teknolojiyle donatılan bir sistemde de dahi yarın için farklı tehditler vardır. Hiçbir zaman için bir sistem yüzde yüz etkin başarı sağlar demek mümkün değildir. Yarının ihtiyaçlarını karşılayabilmek için devamlı gelişen bir süreç içerisinde hareket etmemiz gerekir. Gelmiş olduğumuz nokta her zaman için yarının bir adım gerisidir.

İş yaşamımızda kullandığımız, iş gereği bizimle paylaşılan, çalışmalarımızla, türlü deneyimlerle elde ettiğimiz her bilgi değerlidir ve / veya özeldir. Günümüzde bilgisayar ortamlarında her türlü değerli bilgi tutulmaktadır. İnternet ve elektronik

iletişim; banka, alışveriş, eğlence alanlarında yaygın olarak kullanılmaktadır. Öyle ki, artık bir ilkokul öğrencisi de bir emekli de İnternet kullanıcısı olmuştur (Mitnick, 2005).

Son yıllarda çok fazla duymaya başladığımız bilgi güvenliği kavramı, öncelikle birey bazında başlayan bir süreçtir. Özellikle kurumsal bilgi güvenliği konusunda düşülen en büyük yanlış bilgi güvenliğinin teknik bir yapıdan ibaret olduğudur. Ardından bilinmesi gerekir ki, bilgi güvenliği sadece bir birimin; yetki, donanım ve teknik alt yapıyla maddi imkânlar nispetinde yapacağı bir işlem değildir. Bilgi güvenliği konusunda öncelikle üst düzey yöneticiler karalı olmalı ve ardından tüm personeli içine alacak bir eğitim süreci başlamalıdır. Hiçbir zaman unutulmaması gereken nokta: bir topluluğun gücü, içinde bulunan en zayıf halkası kadardır. En alt kademelerde önemsenmeyen çok basit hatalar geri dönüşü olmayan sonuçlar doğurabilir. Bizim eğitim için yapılmasını gereksiz gördüğümüz masraflar, kat kat fazlası bizi zarara uğratabilir.

Bunun yanında gereğinden fazla, bilgi güvenliği stratejisini kapsayan politikalar iş yaşantısını içinden çıkılmaz bir hale sokabilmektedir. İlk etapta zaten birçok çalışan için anlaşılması zor olan BGYS süreci, gereksiz tedbirlerle çalışanlar üzerinde olumsuz etkiler yaratmaktadır. Gereksiz yere uygulanan tedbirler, sistem içinde artan bürokrasi, kurumları atıl duruma düşürmekte ve iş verimliliğini aşağılara çekmektedir. Her kurum kendi iç dinamiklerine göre, oluşan ihtiyaçları da hesaplayarak bir BGYS kurulması gerekir. Bir başkasında işleyen sistem diğerinde aksaklıklara sebebiyet verebilir.

Onun için bu kararların üst yönetim kademesinde alınması gerekir. Bilgi güvenliği stratejileri ve bunları yönetecek uygun yöntemleri olmayan kurumlar, sadece güvenlik açısından değil, operasyonel ve diğer her türlü iş süreçlerinin yönetimi açısından da ciddi sıkıntılar, maddi ve/veya manevi kayıplarla yüzleşmektedir (Tipton ve Krause, 2007).

Bilgi güvenliği yönetim sistemini kurmak için alınan kararlar kuruluş için stratejik öneme haizdir. İlk etapta çalışanlara angarya gibi gözüken sistem gereksinimleri ve sorumluluklar, zamanla sistemin daha etkin ve daha hızlı çalışmasını sağladığı gözlemlenmektedir. BGYS kurmak için öncelikle istekli olmak gereklidir. Genellikle istekli olan firma ve kurumlar ya gerçekten ilgili olanlar yâda önceden bilgi

güvenliği ihlali olayı yaşayarak, bunun sonucunda daha fazla kayba uğramış kurumlardır.

Kapsamı belirlenmiş bir BGYS çalışmasının karar aşamasında olması gereken bir ön şartı da Üst Yönetim'in desteğidir. Kurum yöneticilerinin, bu çalışmaların kurumsal bir ihtiyaç olduğunu, mecburiyetten değil, gereklilikten yapılması gerektiğini kabul etmesi ve alt kadrolarına bu mesajı ve kararlılığını net bir şekilde iletmesi gerekmektedir. Çünkü sürecin en zorlu aşamalarında, gerek çalışanların motivasyonu gerekse zorlukların aşılmasında bu kararlılık anahtar rol oynayacaktır (Ottekin, 2011).

BGYS kapsamında yapılan araştırmalar genellikle fen bilimleri alanında teknik konuları kapsayan araştırmalardır. İçerik olarak uluslararası standartlardan bahsedilse de, uygulama olarak genelde teknik personeli içine alacak yapılara ve tekniklere değinilmektedir. Kamusal alanda bilgi güvenliği denince: E-devlet kapsamında atılan bilgi güvenliği adımları, Sağlık Bakanlığı'nın hazırladığı bilgi güvenliği politikaları ve birkaç belediyenin bilgi güvenliği sertifikasına sahip olmasından fazla atılımlar göze çarpmamaktadır. TÜBİTAK tarafından hazırlanan konferanslar ve bilgi güvenliği standartları kılavuzları da devlet destekli projelerde yetersiz kalmaktadır.

Son birkaç yıldır birkaç üniversitede lisansüstü eğitim seviyesinde bilgi güvenliği alanında bölümler açılmaktadır. Tabii bu tür bölümlerin açılması birer ihtiyacın sonucudur. Fakat bize göre asıl ihtiyaç bilgi güvenliği konusunun birey bazında tüm lisans seviyesindeki bölümlerden başlayarak, gelecek yıllarda da daha alt seviyelerde eğitim verilerek eğitim seviyesinin içinde yer almasıdır. Toplumun en küçük yapı taşı olan bireyin bilinçli bir şekilde eğitimini tamamlaması, günlük yaşantısında daha başarılı ve daha kaliteli bir yaşam yürütmesini sağlayacaktır. Farklı iş dallarında ve farklı seviyelerde görev alınacak olunsa da, bireyde her zaman için bilgi güvenliği farkındalığı yaratılması gerekir. Farkındalık oluşturabilmek içinse her seviyede eğitimler vererek, bu eğitim sonuçlarını davranışa dönüştürmek gerekir.

Genellikle bilgi güvenliği ihtiyacını, yaşamış olduğumuz kayıplardan sonra hissetmekteyiz. Başkaları için önem arz etmeyen bir bilgi, bizde telafisi olmayan değerli bir varlık halini alabilir. Buradan bilginin kişiler ve kurumlar üzerinde yarattığı riskler sonucunda izafi bir anlam içerdiğini de görmekteyiz. Bir banka şifresi bilgisinin kaybı, hesabında az bir miktar olan kişi için çok fazla bir risk oluşturmamaktadır. Bunun

yanında hesabında aynı miktarda varlıklara sahip iki kişinin ihlal olayı ile edindikleri risk oranında aynı değildir. Risk faktöründe değişken olan birçok etken vardır. Kişilerden birinin öğrenci, bir diğerinin aylık belli bir gelire sahip oldukları düşünülürse; oluşacak kayıp maddi oranda aynı olmasına karşın taraflar üzerinde yaratacağı çarpan etkisi farklı olacaktır. Kişilerin kart şifrelerini oluştururken, şifre güvenliği konularındaki hassasiyetlerinde oluşacak risk oranını etkilemektedir.

Bu çalışma hazırlanırken öncelikle literatür taraması yapılmış, yabancı kaynaklar ve ülkemizde yapılan çalışmalar dikkatle incelenmiştir. Konferans, bildiri ve bilgi güvenliği üzerine hazırlanmış internet siteleri taranmıştır. Bilgi güvenliği ihlal olayları ile ilgili dikkat çekici örnekler ortaya çıkmıştır. Sosyal mühendislik, kavramı araştırmalarımız arttıkça sıkça karşımıza çıkmaya başlamıştır. Uluslararası standartlar hakkında yapılan araştırmalar ile çalışmamız yeni bir boyut kazanarak, kabul gören en son ve en geniş kapsamlı BGYS standardı olan ISO27001 konusunda ayrıntılara yer vermeye başladık. Bu standardın aile grubunda yer alan 27K standartlarıyla olan ilişkisinden, diğer BGYS standartlarıyla olan farklı yönlerinden, ülkemizde ve dünyada bu sertifikaya sahip olma oranlarına değindik. Bu çalışma yürütülürken ISO27001 standardının yurt dışında yeni sürümünün çıkması araştırmamızın kapsamını genişletti. Mevcut sürümde hazırlamış olduğumuz çalışmalara ek olarak, yeni sürümünden çeviriler yaparak, her iki versiyonunu da karşılaştırılarak tanıtılmasına karar verdik. Yeni sürümle beraber, yönetim sistemlerinde görmeye başladığımız "annex sl" daha yakından tanıma ve tanıtma fırsatı bulduk. Çalışmamız esnasında danışmanlık ve eğitim firmalarının ülkemizde kurum ve firmalar üzerine olan etkisi ve belge alımında oynadıkları roller belirmeye başladı. Birey bazında başlayan bilgi güvenliği eğitiminin, siber savaş tehlikesi altında kurumları, devletleri ve devletler üstü organizasyonları etkileyecek derecede önemli olduğu ortaya çıkmıştır. Yasal mevzuatlarda göz önüne alındığında; standartlar çerçevesinde oluşturulan BGYS'nin kurumlar için angarya olmaktan çok ileride oluşabilecek sorumluluk ve cezai yaptırımlardan koruyucu bir can simidi olacağı unutulmamalıdır. Sertifika almak zorunluluğu bir kaç sektör için zorunluluk içermektedir. Genel olarak gönüllülük esasıyla kurumların itibar ve prestij getirisi vizyonları gereği sertifikalar alınmaktadır.

Araştırmamız esnasında BGYS hakkında, ülkemizde ve dünyada akademik anlamda çok fazla kaynak olmaması araştırmanın ilerlemesini yavaşlatmıştır. Bunun

yanında araştırmalar esnasında bir konu daha dikkatimizi çekmiştir. Yurt dışında BGYS kuracak firmalar için ticari anlamda basılan kitaplar mevcut iken (yaklaşık 2000€ civarında) , ülkemizde bu açığı danışman firmalar doldurmaktadır. Yapılan araştırmalarda birçok kişi, ülkemizde ISO27001 sertifikası alan firmalara ulaşamamaktan ve bu kurumların kendi isimlerini olası bir hacker saldırılarına karşı gizli tuttuklarından bahsetmektedir. Bu iddiaların bazı kısımlarının doğruluğunu bizlerde kabul etmekteyiz. Fakat araştırmamız esnasında belge sahibi birçok kurumun kendi reklamını basın aracılığıyla yaptıklarını gözlemledik. Standartlarla ilgili internet sitelerinde belge sahibi hemen hemen tüm firmalara dünya çapında ulaşabilmenin olanaklı olduğunu gözlemledik. Bu alanda yapılan çalışmalarda genellikle araştırmacıların kendi ürettikleri bir X firması üzerinden örnekler verilmektedir.

Biz ise araştırmamızda bu eksikliği fark ederek sertifika sahibi, süreci yaşamış kurumlar üzerinde çalışarak, bu süreci daha anlaşılabilir hale getirmek istedik. Belge sahibi birçok firma ile yazışmalar yapıldıysa da birçoğundan olumsuz cevap vermek için dahi geri dönüş olmadı. İlk olarak Pendik Belediyesi, ardından Keçiören Belediyesi bizimle mülakat yapmayı kabul etti. Yapılan mülakatlar neticesinde her iki kurumunda BGYS sürecinde danışman firmaların büyük rol oynadıkları ortaya çıktı.

Belediyelerle yarı biçimsel mülakat tekniğini uygulayarak; önceden hazırlamış olduğumuz soruları bilgi işlem personeline sorarak ve mülakat esnasında gelişen yeni konulara da cevaplar bularak araştırmada bulunduk. Bu araştırmada güdülen asıl amaç; BGYS kurmak isteyen kurum ve firmalara akademik anlamda yapılan bir çalışmayla, yaşanmış örnekler vererek anlaşılması kolay, cesaret verici bir yol haritası çizmektir. Bilgi güvenliği konusunun bireyden başladığını hatırlatarak, eğitim sistemimizin içinde bilgi güvenliğine olan ihtiyaç vurgulanmıştır.

ISO27001 Bilgi güvenliği yönetimi standardının gereksinimleri; zorunlu olan maddeleri ve uygulanması kuruluşun isteğine bağlı olan maddeler olarak karşımıza çıkmaktadır. Bu gibi ayrıntıların farkına varan ve denetim tecrübeleriyle bir adım öne çıkan danışmanlık firmaları sertifikasyon alanında ülkemizde ayrı bir pazarda konumlanmıştır. Verilen danışmanlık hizmetleri kuruluşların vazgeçilmezi haline gelmiştir. Danışmanlık firmalarının asıl tercih edilmelerinin sebepleri biraz daha farklıdır. Bu süreç için kuruluşlar ayrı bir personel görevlendirme durumundan

kurtulmaktadırlar. Başarısızlık durumunda üçüncü bir taraf yaratarak kendilerini sürecin başarısızlığından ayrıştırmaktadırlar. Danışmanlık kuruluşları, çalışanların üzerinden sorumluluğu bir nebze almaktadırlar.

Her türlü sertifikasyona uyum sağlayabilen bu kuruluşlar, yeni ortaya çıkan standartlara karşı en hızlı tepkileri vermektedirler. Personellerini yeni durumlara göre eğitimlerden geçirerek, gerekli sertifikaların alımını sağlarlar. Eğitim hizmetleriyle ülkemizde eğitim kurumlarının yapması gerektiğine inandığımız faaliyetleri belirli bir ücret karşılığında icra etmektedirler. Yapılan denetim ve test faaliyetleri yine bu kuruluşların aracılığıyla devam ettirilmektedir. Danışmanlık ve eğitim faaliyetlerinin, akademik kuruluşların bünyesinde toplanabileceğini ve verilen hizmetlerin neleri kapsadığını gösterebilmek adına yaptığımız mülakatlarla desteklediğimiz bu çalışma sadece bilgi güvenliği değil farklı alanlarda da çalışma yapmak isteyen ve bu çalışmalarını belgelemek isteyen kişi ve kuruluşlara yol göstermesi ve cesaret vermesi amaçlarıyla yazılmıştır.

BİRİNCİ BÖLÜM

BİLGİ VE BİLGİ GÜVENLİĞİ KAVRAMLARI

Gelişen teknolojiyle beraber insanoğlu daha farklı beklentilere girmiş ve yeni ihtiyaçları belirmeye başlamıştır. Bu ihtiyaçları karşılama içinse en çok gereksinim duyduğu araç bilgi olmuştur. Son yüz yılda artık bilgiye olan ihtiyaçlar gereklilik halini almış, ihtiyaçlar hiyerarşisinde üst basamaklara doğru tırmanmaya başlamıştır. İnsanın düşünerek, tecrübe ederek kazandığı bilgi ve tecrübeler yaşamının en değerli varlığı olmaya başlamıştır. Bilgi kimileri için tek başına çabalayacak elde edilmiş bir varlık iken, kimileri içinse başkalarının tecrübelerinden yararlanılarak daha kolay elde edilmiş bir varlık haline dönüşmüştür.

Zaman içerisinde değişmeyen tek şeyin, değişim olduğunun farkına varanlar kendi devirlerinin kazananları olmuşlardır. Sahip oldukları bilgi ile toplumda bir adım öne çıkmaya başlamışlardır. Bilgi kendini diğer güç araçları arasında göstermeye başladı. Savaşlarda bilgiyi elinde tutan ve yeniliklere açık olan taraf; beklenmedik ve daha önce hiç görülmemiş stratejilerle üstünlükler kurmaya başlamıştır. Bilgi sahibi olma artık hak ettiği değere kavuşmuştur.

Artık yeni yeni kavramlar ortaya çıkmış, yeni beklentilere girilmiştir. Bilgiye sahip olmak için eğer bilgi üretilmiyorsa, başkasının elindeki bilgiyi elde ederek daha kolay yoldan güç sahibi olma formülleri denenmiştir. Bilgi güvenliği kavramlarının kökeni geçmişteki casusluklara kadar dayanmaktadır. Son yüz yıla girildiğinde ise gelişen teknolojiyle beraber bu ataklar giderek artmış ve toplumun yapı taşını oluşturan insana kadar dayanmıştır.

Geçmişte ülkeler arası olan bu rekabet manevraları günümüzde kurumlar, şirketler hatta kişiler seviyesine inmiş durumdadır. Böylelikle dilimizde yeni kavramlar türemiş, toplumda farkındalıklar oluşmaya başlamıştır. Bilgi güvenliği, kurumsal bilgi güvenliği, bilgi çağı, bilgi güvenliği sistemleri, bilgi güvenliği standartları, bilgi güvenliği ihlalleri bunlardan sadece öne çıkan bazılarıdır.

1.1. BİLGİ KAVRAMI

Bilgi kavramı geçmişten günümüze edinilen tecrübelerle daha da anlam kazanmıştır. Bilginin sözlük anlamına baktığımızda: Öğrenme, araştırma ya da gözlem yoluyla elde edilen gerçek, malumat, kurallardan yararlanarak kişinin veriye yönelttiği anlamdır. Her bilim dalı bilim dalı bilgiyi alanı ve çalışmalarına göre tanımlamaktadır. Buna karşın bilgi sadece bilim dallarına göre değil, zamana ve değişen koşullara göre de değişen bir kavramdır. Önceleri bilgi insanı şekillendiren, haber değeri taşıyan bir olgu iken günümüzde bilgi bir üretim faktörüdür ve alınıp satılma özelliğine sahiptir. Genel olarak bilgi, bir seçim yapmamız söz konusu olduğunda gereksinim duyduğumuz şeydir. Geçmişten bugüne kadar tartışılan bilginin tanımı zor, ayrıca neyin bilgi olduğu neyin bilgi olarak kabul edilemeyeceği; bilgi, inanç ve gerçek ilişkisi hala tartışılmaktadır (MEB, 2013).

1.2. BİLGİ KAVRAMININ TEMEL İLKELERİ

Bilgi kavramı gizlilik, bütünlük ve erişilebilirlik ilkelerinden oluşur. Bilginin kullanımına göre bu ilkelerde kendi arasında farklı önem derecelerine ulaşabilir. Çok önemli, milli araştırmaların yapıldığı bir kurumda öncelik gizlilik ilkesindedir. Orada üretilen bilgiye erişilebilirlik ve bilginin bütünlüğü daha az önem arz etmektedir. Medya sektöründe öncelik erişilebilirliktedir. İnternet üzerinden yayın yapan bir kurum için öncelik bilginin karşı tarafa devamlı ve en hızlı şekilde iletilmesidir. Bazen küçük bir alt yazı, diğerlerine fark atmayı sağlar. Verilen bilgide gizlilik aranmaz, bütünlük beklenmeden karşı tarafa aktarım yapılabilir. Bir davayı yürüten hâkim içinse öncelik bütünlük ilkesindedir. Bazen bir dava yıllarca sürebilir. Bazen bazı konular ifadeler alınırken gizliliğini yitirebilir. Amaç doğru bilgiler ışığında hayati karalar vermek olunca elde edilecek bilgilerde daha da önemli hale gelir.

Bilgi farklı ortamlarda işlenip depolanabilir. Önceleri sadece konuşarak bireyler arasında yol alan bilgi, yazının keşfi ile daha etkili ve daha hızlı bir şekilde yol almaya başladı. Arşiv anlayışı da bu şekilde tarihte kendine bir yer edindi. Bugün bilgiyi kâğıt üzerinde basılı olarak, konuşarak sözlü olarak, elektronik bilgi depolama cihazlarında (cd/dvd, usb bellek vb.), internet ağı üzerinde sanal ortamda ve bulut ağı ortamlarında

saklayabiliyoruz. Bilgiye erişimde ise öncelikle mobil cihazlar, basılı yayınlar, mesajlar, kuryeler kullanılmaktadır. Farklı ortamlarda saklanan bilgiler korunmak için farklı uzman dalları gerektirse de, hepsi için ortak bilgi güvenliği standartlarını bilmemiz yine de yeterli olacaktır.

Bir bilgiyi saklamak kadar, yetkili olan kişilerin hizmetine sunabilmekte önemlidir. Varlıklara istenilen yer ve zamanda yetkilendirme ve sınıflandırma sonucunda kuruluşların kullanım yetkisine erişim denetimi denilir.

1.3. BİLGİ GÜVENLİĞİNİN TANIMI

Bilgi güvenliği de; mevcut bilginin herhangi bir değişime uğramadan, yetkisiz kişilerin eline geçmesine izin vermeden, istenilen yer ve zamanda kolaylıkla erişilebilmesine denir. Bilgi güvenliği başarıyı tamamlayan yönetim sistemi içerisinde yer alan bir araçtır. Bir kuruluş daha ilk planlama aşamasından itibaren bilgi güvenliği sistemlerini kurması gerekir. Kurulu bir firmaya bilgi sistemini sonradan entegre etmeğe çalışmak daha zor ve başarı oranı daha düşük bir durumdur. BGYS kurmak bir kuruluş için stratejik bir karardır. Bu sebepten; BGYS kurulma kararı alınırken öncelikle üst kademe yöneticilerinin kararlı ve ısrarcı olması gerekir. BGYS tüm kurumu kapsayacak şekilde hazırlanmalıdır. Kurumun dinamikleri, çalışanları ve ilişkili oldukları üçüncü taraflarda hesaba katılmalıdır.

BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir (Vural ve Sağıroğlu, 2008:509).

BGYS kurulması, ilk bakışta teknik detaylar içeren bilgi işlem biriminin değerlendirmesi gereken bir konu gibi algılanmaktadır. Bilgi işlem personelinin de bilgi ve vizyonu belli bir aralıktadır. Her birim çalışanı kendi bölümünde farklı bilgi kapasitelerine sahiptir. Tüm kurumu içine alarak yapılan bir toplantıyla, her birimin bilgi birikimleri, beklentileri, riskleri ve bu riskleri kabulü tartışılır. Varlıklar ortaya konur ve sonuçta tüm yönetim kademelerini içine alan bir politika hazırlanır ve

uygulanmaya başlanır. Böylelikle yönetim kademesi ileride doğabilecek birçok sorunu daha az maliyetle önceden çözmüş olacaktır. BGYS kurulu bir kuruluşta sorumluluklar ve roller önceden yazılı olarak ortaya konulduğu için herhangi bir sorunda sorumlular daha rahat tespit edilebilecektir. Yasal mevzuatlara uyum sayesinde hukuki anlamda bir ön alma yaşanmış olacaktır. Bunların yanında hiç beklenmedik bir anda doğal afetler sonucunda da eldeki mevcut birikimlerimiz yok olabilir. Yapmış olduğumuz BGYS sayesinde bununda önüne geçilmiş olur.

Bilgi güvenliği kavramları çalışanlar arasında, yürüyen bir sistemi yavaşlatma eylemi olarak algılanabilir. BGYS kurulurken tüm personeli bu sürece dâhil etmek ve eğitimler vererek personeli devamlı dinamik tutmak gerekir. Yapılan bütün çalışmaların merkezinde insan olduğu için, farkında olmadan bile yapılan bir hata tüm kurumun işleyişine zarar verebilir. İlk bir yıl içerisinde kurulan sistemin etkileri yavaş yavaş kendini hissettirmeye başlayarak, artık çalışanlarda kurallar davranışa dönüşmeye başlayacaktır. Bilgi güvenliği kavramı dinamik bir olgudur. Bugün bizim için normal gözüken bir davranış, sistemin kurallarına göre gelecekte tehdit olarak algılanabilir. Değişen teknolojiyle beraber sisteminde devamlı olarak kendini yenilemesi, gerekli değişim ve eğitimlerle kendini koruması gerekir. Bilgi güvenliği konusunda en kapsamlı ve en son kabul gören standart ISO27001:2005'tir. Ancak zaman ilerledikçe bu sisteminde yeni açıkları ve ihtiyaçları doğmuştur. Kendini dinamik tutmak adına bu standart içinde düzenlemeler yapılmaktadır.

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemlerde olabilir. Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel güvenlik te sağlanamaz (Vural ve Sağıroğlu, 2008: 507; Vural, 2007:40). Kurumsal bilgi güvenliği de, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir (Baykara vd.,2013:233).

1.4. KURUMSAL BİLGİ GÜVENLİĞİ

Kurumlar kendi mevcut sistemlerinin ve yönetim süreçlerinin zarara uğramadan kesintisiz bir şekilde çalışabilmesi için BGYS kurması gereklidir. Öncelikle kendi içyapısında alınan önlemlerle kurum kendi sini oluşabilecek dış tehditlere karşı koruma başlatır. Ardından iç tehditlerle kurum içinde oluşacak kayıplara karşı tedbirler alınır. İç tehditler denilince sadece kurum içinden gelen art niyetli saldırılar algılanmamalı, kurum içerisinde yer alan herhangi bir bireyin istemeden yapmış olduğu bir davranış veya ihmalkâr hareketi de tüm kurumu etkileyen bir iç tehdit durumudur. Kurum içinden yapılan saldırılar, dışarıdan gelen saldırılara göre daha yıpratıcı ve geri dönüşü zor durumlar oluşturmaktadır. Yapılan eğitimlerde tam katılım ve bu eğitimlerin etkin ve dinamik olması istem dışı ve ihmal sonucu oluşan tehditleri en aza indirgeyecektir.

Kurumları hesaba katması gereken diğer tehdit muhatapları, hizmet sağladıkları üçüncü taraflardır. Verilen hizmet esnasında karşı tarafın bilgi güvenliğini sağlamakta kurumların görevidir. Bir banka müşterisinin istekleri öncelikle gizliliğin korunmasıdır. Her ne kadar kullanıcı işlem yaparken kendi bilgilerini gizli tutma sorumluluğunu yüklense de, kurum müşterilerin bilgilerini korumak için gizlilik tedbirlerini almak zorundadır. Müşteri taleplerine göre erişilebilirlik ilkesi ve bütünlük ilkesi farklılıklar gösterebilir. Örneğin bir müşteri internet hesabı veya telefon bankacılığı ile 24 saat bankacılık işlemlerini ek bir ücret ödeyerek yapabilmekte, bankamatikle yalnız para çekebilen müşteriye göre daha fazla bilgiye ve daha fazla erişim hakkına sahip olmaktadır.

Bu işlemlerin tümünde kurum üçüncü tarafların bilgi güvenliğini sağlamakla yükümlüdür. Bilgi güvenliği sağlanarak verilen bu hizmetler diğer kurumların prestij ve itibarını arttırmaktadır. Bazı sektörlerde yapılacak olan anlaşma maddelerinde bilgi güvenliği şartı vardır. Uluslararası kabul görmüş sertifika sahibi bir kurumla çalışmak, karşı tarafı da rahatlatacaktır.

Kurumsal bilgi güvenliği, çalışanlarında daha sistemli ve daha rahat çalışmalarını sağlayacak bir ortam hazırlar. Personel yapacağı bir davranışın sonuçlarını her daim önceden bilebilmektedir. Roller ve sorumluluklar neticesinde kimin ne kadar yetkiye sahip olduğu da bellidir. Yapılan her işlem geriye dönük olarak izlenebilir ve kimin tarafından yapıldığı tespit edebilir.

Kamu kurumları bilgi teknolojilerine ne kadar çok yatırım yaparlarsa, o kadar çok bilgi teknolojilerinin sunduğu imkânlardan faydalanmakta, vatandaşlar hizmetlerden hızlı ve sorunsuz olarak yararlanmakta ve bürokrasi hızlanmaktadır. Daha geniş açıdan bakıldığı zaman ise tüm bu faydalar ülke ekonomisine katkı yapmakta, yolsuzlukların önlenmesinde ve ortaya çıkartılmasında önemli rol oynamaktadır. Geçmiş yılların aksine bilgi teknolojileri kamu kurumları için bir masraf kapısı değil, bir fırsat kapısı olarak değerlendirilmektedir (Bahşi ve Karabacak, [?]:144).

1.5. VARLIKLAR

Varlık, bir kurumun sahip olduğu değerler bütünüdür. Bunun içinde elle tutulur maddi değerler olduğu gibi; bilgi, tecrübe, imaj gibi soyut değerlerde mevcuttur. Tüm kurum için öncelikle mevcut varlıkların tespiti gereklidir. Oluşan varlıklar tablosu ardından ihtiyaçlar belirlenir. Mevcut varlıklarımızı bilmemiz bizim için risk analizimizi daha kolay ve daha doğru yapmamızı sağlayacaktır. Bir varlığın yok edilmesi, değiştirilmesi veya el değiştirmesi için mevcut sistemimize saldırılar olabilir. Bunlara karşı önceden senaryolar dâhilinde hazırlanarak etkin koruma sağlamamız gereklidir.

Bilişim sistemlerinin hayatımıza girmeye başlamasıyla birlikte, bilgi varlıklarının muhafaza ve erişim tekniklerinde de değişimler gözlemlenmiştir. Önceleri basılı bir şekilde kâğıt üzerinde muhafaza ettiğimiz bilginin korunması, fiziki güvenlik tedbirleri ile sağlanabiliyordu. Şimdilerde ise bilgi ile ilgili hemen hemen bütün işlemlerimiz dijital platformlara taşındı. Personel güvenliği ve fiziki güvenlik tedbirleri ile yeterli seviyede koruma sağlayan bilgi güvenliği sistemlerinde de, yeni sorunlar ortaya çıkmıştır. Bu sorunlar, sistemlerin işletim güvenliği, erişim denetimleri, ağ güvenliği, donanım güvenliği ve uygulama sistemlerinin geliştirilmesi gibi yeni güvenlik sorunlarıdır.

Bir organizasyonda varlıkların belirlenmesi ve varlıklara değer atanması, risk analizi süreci için temel bir adımdır. Varlıklara değer atanmasının yapılabilmesi için bir envantere ihtiyaç vardır. Bir çok organizasyonda envanter denince ilk akla gelen bir çeşit "zimmet listesi" dir. BGYS ilk defa kurulmaya çalışılırken başlangıç noktası olarak bu "zimmet listesi" kullanılabilir. Özellikle fiziksel ve yazılımsal varlıklar için zimmet listesi faydalı olacaktır. Ancak zimmet listesi BGYS için gerekli ve yeterli

detaya sahip olmayabilir. Zimmet listesi, BGYS için çok önemli olan bilgi varlıklarının tespitinde yetersiz kalabilir. BGYS için varlık envanteri hazırlanırken öncelikle, tüm varlıkların kapsandığından emin olmak için gruplandırma yapmak varlıkların tanımlanması işini kolaylaştıracaktır. Bilgi varlıkları, yazılımsal varlıklar, fiziksel varlıklar, servisler vb. bir gruplandırma yapılabilir (Koç, 2008:8).

1.6. İNKÂR EDEMEME

İnkâr edememe; mevcut bir bilgi güvenliği sistemi içerisinde oluşabilecek herhangi bir olayın sorumlusunun tespitini sağlamadır. Olayın başlangıcından itibaren kaynağına ulaşılarak, zaman içindeki gelişiminin gözlemlenerek delileri ile ispat etmemizi sağlar. Hesap verilebilirlik; kişilerin almış oldukları kararlar ve eyleme dönüştürdükleri davranışlardan sorumlu olmasını içerir. Güvenilirlik; ortaya konan davranışların tutarlı olmasını açıklar.

BGYS kurulması kurumlar için önleyici bir güvenlik tedbiri niteliğindedir. Önceden alınan tedbirlerle bütün açıklar kapatılmaya çalışılır. Alınan tedbirlere rağmen risk içeren konular gözden geçirilir. Risk analizleri yapılır ve artık riskler ortaya konulur. Bu yapılan işlemlerin hepsi değerlendirilip bir karara bağlanır. Bu faaliyetlere göre politikalar belirlenir. Bu süreç içinde personele bilgi güvenliği ile ilgili eğitimler verilir. Bu zamana kadar geçen süreç BGYS'nin önleyici tedbirlerine girer. Bu alınan tedbirlere karşı hala herhangi bir ihlal olayı yaşanabilir. Bundan sonra yapılacaklarda bilgi güvenliği ihlal politikalarında, kontrol ve denetim bölümlerinde ele alınmaktadır.

1.7. BGYS'NİN ÖNLEYİCİ (KORUYUCU) ÖZELLİĞİ

BGYS sürecinin belki de en önemli özelliği önleyici (koruyucu) özelliğinin olmasıdır. BGYS öncelikle kurumun kendisini tam anlamıyla tanıyabilmesini sağlar. Kurumun Sahip olduğu varlıkların farkına varmasına ve onları etkin bir şekilde kullanabilmesine yardımcı olur. Kendi sahip olduğu değerlerin farkına varmayan bir kurum, kendisini ne gibi tehditlerin beklediğini düşünmekte bile zorluklar çeker. Olası bir ihlal olayının ya farkına varamaz yâda hesaplanamayan büyük kayıplar yaşadıktan

sonra müdahale etmeye çalışır. Kurum yöneticileri için varlıklar konusunda farkındalık oluşturur.

Bunun yanında tüm personelde oluşturduğu, bilgi güvenliği farkındalığı değeri de vardır. Tüm personel için verilen zorunlu eğitim faaliyetleri tüm sistemin en zayıf halkasını içten ve dıştan gelecek tehditlere karşı kuvvetlendirmektedir. Personelin bilgi eksikliğinden veya ihmalinden kaynaklanacak olası bir açıklık durumunun önüne geçilmiş olunur.

1.8. BİLGİ GÜVENLİĞİ EĞİTİMLERİ

BGYS kapsamında verilen eğitimler öncelikle bilgi işlem personelini kapsayan özel eğitimler olmalıdır. Ardından tüm kurum personelini kapsayan genel bilgi güvenliği eğitimleri verilmelidir. Üst yönetimi ve birim müdürlerini kapsayan yönetim kademesi için ayrı bir eğitim programı planlanmalıdır. Üst yöneticilerin alacağı eğitimlerin kapsamı biraz daha kapsamlı ve özel konuları içermelidir. Bu eğitimler yıl içinde planlanarak, belirli periyotlarla tekrarlanmalıdır. Ayrıca kuruma yeni katılış olduğunda bu personele de görev ve sorumluluklarına göre bilgi güvenliği toplantıları düzenlenmelidir. Kuruma sonradan dâhil olan bir varlık veya teknolojik bir gelişme özel önem arz ediyorsa bununla da ilgili gerekli personele eğitimler verilmelidir.

Kurumlarda "bilmesi gerektiği kadar, en az yetki, erişmesi gerektiği kadar" gibi ilkelere en öncelikli uyması gereken gruplar yöneticiler ve bilişimcilerdir. Oysa tam tersine bu ilkelerin en az uygulandığı ve en riskli eylemlerin yaşandığı(zorunlu veya keyfi, bilinçli veya bilinçsiz) birimler de bu iki gruptaki çalışanlardır. Kurumlarda en değerli ve en gizli bilgileri kullanan, taşıyan, kaydedenlerin çoğunlukla bu iki gruptaki çalışanlar olduğu bilinmektedir. Ayrıca, işlerinin niteliği gereği kurum genelinde en sık örnek alınan ve daha çok dikkat çeken birimler de gene bu iki birimdir (Tipton ve Krause, 2007).

Ülkemizde bilgi sistemi kullanıcılarının bilgi güvenliği farkındalığı seviyesini arttırmak amacı ile bilgi güvenliği ile ilgili güvenilir kaynaklara etkin ve hızlı bir şekilde erişim imkânı sağlanması ihtiyaç duyulan bir alandır. Farklı girişimler olmakla birlikte, hedeflenen kitlenin genişliği, konunun karmaşıklığı nedeni ile farklı bir bakış

açıları ile geliştirilen projelere sürekli ihtiyaç olacak gibi görünmektedir. Bu bakış açısı ile alana bakıldığında geniş bir kitlenin anlayacağı bir dile sahip olan ve günlük yaşamla ilişkilendirilmiş bir bilinçlendirme eğitimine ihtiyaç olduğu tespit edilmiş ve bu noktadan hareketle TÜBİTAK Bilgem UEKAE tarafından TR-BOME çalışmaları kapsamında "Bilgimi koruyorum " projesi başlatılmıştır (Gökçe ve Kültür, [?]:2).

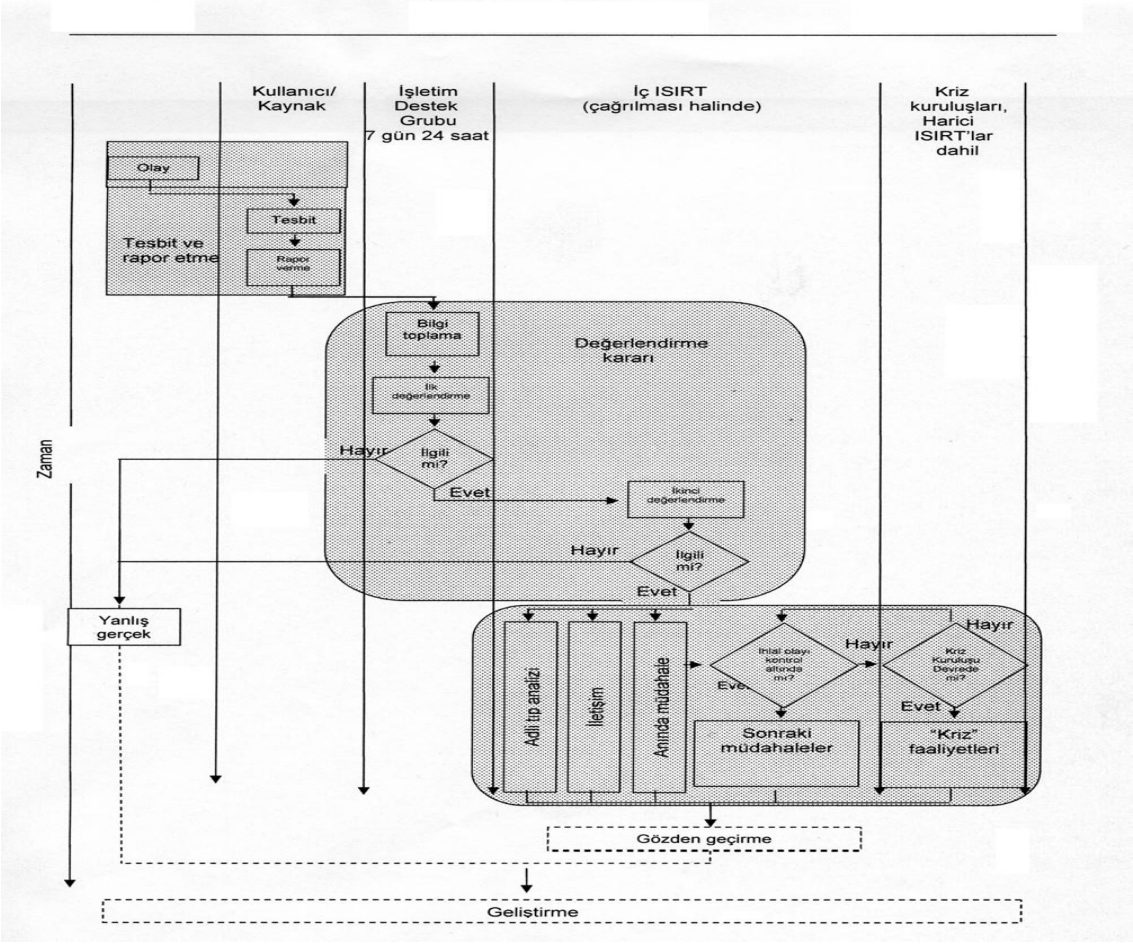
1.9. BİLGİ GÜVENLİĞİ İHLALİ

Bilgi güvenliği ihlal olayı; mevcut bilgi güvenliği politikalarının ve kontrollerinin başarısızlığa uğraması sonucu veya güvenlikle ilgili önceden hesaplanmayan, hizmet ve ağ durumundaki aksaklıkların hepsine denir. İhlaller sonucunda yönetim sisteminin bir kısmı veya tamamı sekteye uğrayabilir. Önemli olan ihlal olayı yönetimi vasıtalarıyla, hızlı bir şekilde olayı tespit etmek, raporlamak, değerlendirmek ve tepki göstererek mevcut sistem prosedürlerini uygulayabilmektir. Yapılan raporlamaları eğitim faaliyetinin içine dâhil ederek personelin nelerle karşılaşabileceğini daha iyi anlatmak gerekir. Bilgi güvenliği ihlal olaylarını önem durumuna, ortaya çıkış şekline göre ve daha önceden bilinirliğine göre sınıflandırarak ayırmak gerekir.

"%100 güvenli" ve "0 risk" kavramları günlük yaşamda gerçekçi ve uygulanabilir değildir. Bilgi güvenliği hiçbir veriyi, iş sürecini tamamen güvenli kılamaz veya risklerini sıfırlayamaz. Gerçekçi bir bilgi güvenliği yaklaşımı; o kurum veya o toplum için güvenliği gereken düzeyde sürekli sağlamak, risk analizlerinin sonucuna göre ilgili riskleri olabilecek en alt düzeye indirgemek ve kalan riskleri de kontrollü bir şekilde izleyerek yönetmektir. Sağlık, finans, vb sektörlerin süreç yönetiminde olduğu gibi bilgi güvenliği yönetiminde de risk odaklı yaklaşım esastır (Tipton ve Krause, 2007).

Her zaman, alınan tedbirlere rağmen ihlal olaylarının yaşanabileceği unutulmamalıdır. Tehdit algısı, gelecekte başka teknik ve metotlarla ilk olarak bizi bulabilir. Dinamik bir yapıya sahip bilgi güvenliği sistemleri, içinde bulunduğu zamanın ihtiyaçlarını karşılamasını bilir ve kendini koruma için çaba gösterir. Hiçbir BGYS yüzde yüz koruma sağlayamaz. Bilgi güvenliği ihlal olaylarını daha etkin yönetmek için

ISO 18044 Bilgi Güvenliği İhlal Olayı Yönetimi Standardından da yararlanmanızda fayda vardır.



Şekil 1: Bilgi Güvenliği Olayı ve İhlal Olayı Akış Diyagramı

Kaynak: ISO 18044 Bilgi Güvenliği İhlal Olayı Yönetimi Standardı

1.10. RİSK YÖNETİMİ KAVRAMLARI

Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığı olarak da tanımlanabilir. Risk yönetimi ise, kurumun karsı karsıya bulunduğu risklerin tanımlanması, bu risklere değer biçilmesi, risklerin kabul edilebilir bir seviyenin altına indirilmesi ve sürekli bu seviyenin altında kalmalarını sağlayacak mekanizmaların devreye sokulmasıdır. Başka bir ifade ile risk yönetimi; bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli

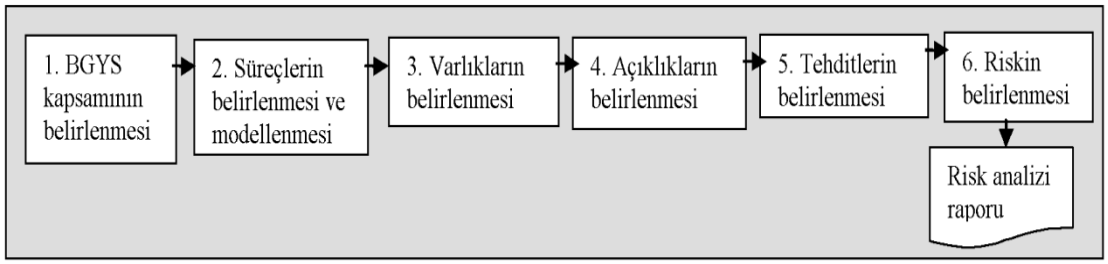
faaliyetlerdir. Risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir (Kumaş, 2009:34).

Risk analizi yöntemleri içerisinde günümüzde otomasyon içeren yazılımlar mevcuttur. Fakat biz her kurumun kendisi için özel bir analiz yapmasını önermekteyiz. Çünkü bir başkasına çare olan ilaç, herkese derman olacaktır mantığı yanlıştır. Aynı bu örnekte olduğu gibi piyasada mevcut olan hap şekline getirilmiş yöntemler belki o an için bizim derdimize çare bulabilirler. Fakat uzun vadede kullanmış olduğumuz bu yöntemler telafisi güç olan sorunlar yaratabilir. BGYS kurulumunda risk analizi gibi diğer konularda da bu tür otomasyon sistemleri kullanılmaktadır. Bu sistemlerden yararlanmak bize zaman kazandırırken, maliyetlerin artmasına da sebep olurlar. Bu tür sistemlerin tek başına sonuç sağlamasını beklemek yanlış olur. Bu sistemler yardımcı araçlar olarak kendi kurum yapımızın gerekleri göz önüne alınarak kurum içi katılımlarla çalışmalarımızı tamamlamamız gerekir.

ISO27001 bilgi güvenliği yönetim sistemi gereksinimleri standardında uygulanması zorunlu olan maddeler içerisinde; risk değerlendirme metodolojisini, risk değerlendirme raporunu ve risk işleme planının yazılı hale getirilerek yapılası gerektiği belirtilmektedir. Fakat nasıl yapılacağı ve örneklerle anlatımı mevcut değildir. Bu konuda daha fazla ayrıntıya ulaşmak için ISO27005 Bilgi güvenliği risk yönetimi standardı kılavuzundan ve ISO31000 Risk yönetimi standartlarından yararlanmanızda fayda vardır. Mülakat yaptığımız kurumlardan risk analizleriyle ilgili örnekler istesek de, bize risk analizlerinin kurumlar için en önemli ve en çok gizli tutulması gereken çalışma olduğunu söyleyerek her hangi bir örnek vermediler. Kurumdaki sorumlu kişilerin dışında her hangi bir kişinin bu bilgilere sahip olmasının bütün BGYS'ni tehlikeye atacağını ve yapılan bütün çalışmaların bir anlam ifade etmeyeceğini belirttiler.

Risk analizi sürecinde, varlıklardaki açıklıklar ve bu açıklıkları kullanan tehditler ortaya konulduğu için, varlık envanterinde sadece bilgi işlemin işlettiği teknolojik varlıkların yer alması risk analizinin eksik sonuçlar vermesine yol açacaktır. Bu tip eksik risk analizleri, bilgi güvenliğinin daha çok teknik boyutlarına yoğunlaşacak ama sosyal ve süreçler ile ilgili boyutlarını ihmal edecektir. Bilgi işlem birimlerinin konuya sadece teknik açıdan yaklaşmalarını engelleyeceği ve süreçleri de dikkate alarak

çalışma yapmalarına imkân vereceği düşünülmektedir. BGYS için süreç tabanlı risk analizi üzerine yapılan bu araştırmada da risk analiziyle ilgili açıklamalar yaparak örnek risk analizi metodunun genel akış diyagramı sunulmaktadır (Karabacak ve Özkan, ?:3).



Şekil 2: Öngörülen Yönetim Genel Yapısı

Kaynak: (Karabacak ve Özkan, [?]:3).

ISO 27000 standardı BGYS sözlüğüne göre de risk, bir olay ve sonucun olasılıklarının birleşimi olarak tanımlanır. Somut bir olgu değildir. Risk analizini; kaynakları belirlemek ve risk tahmininde bulanabilmek amacıyla bilginin sistematik kullanımı olarak nitelendirir. Risk paylaşımını; risk hakkında karar verici ve diğer paydaşlar arasındaki bilgi alışverişi veya paylaşımı olarak açıklar. Risk kıstaslarını; riskin önem derecesinin belirlenmesinde kullanılan çalışma kuralları olarak tanımlar. Risk değerlendirmeyi; risk analizi ve risk derecelendirmesini kapsayan genel faaliyetler dizisi olarak tanımlar. Bir riskin olasılığı ve sonuçları için değer atama faaliyetine risk belirleme diye açıklar. Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kıstasları ile karşılaştırılması faaliyetlerine risk derecelendirme diye açıklar. Risk yönetimini bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak nitelendirmektedir. Risk iyileştirmeyi de; risk değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması faaliyetleri olarak tanımlar.

Risk yönetimi, bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla koruyucu önlemlerin ve maliyetlerinin dengelenmesi ve organizasyonun hedeflerine ulaşması için gerekli kritik sistemlerin korunması gibi konularda BT yöneticilerinin yararlandığı süreçtir. Bu süreç risk analizi, risk işleme ve değerlendirme ve takip alt süreçlerinden oluşur (Evrin ve Demirer, 2011:38-43).

Belirtilen bir zaman dilimi için, yönetim kademesi tarafından sonuçlarından doğacak zararlara katlanmayı kabul ettiğimiz risklerde, kabul edilebilir risklerdir. Örneğin kurumun bir felaket kurtarma sistemi mevcut değildir. Bizde bu sistemin olmadığını fakat şuan için bunu kurmanın kuruma oluşturacağı maliyetle, sistemde oluşturabileceği kayıpları değerlendirdiğimizde bu riski kabul etmenin ve belirtilen bir sürede bu riskle ilgili çalışmalar yapmanın bize daha avantajlı olacağına karar vermemiz gibidir. Risk işlemeden sonra kalan risklerde artık risk olarak tanımlanır. Risk kabul kriterleri yasal gerekliliklere göre hazırlanmalı ve artık risklerle beraber yönetimin onayına sunulmalıdır.

1.11. BİLGİ SİSTEMLERİ GÜVENLİĞİ

Bilgi güvenliği yönetim sistemi kapsam bakımından birçok konuyu içermektedir. Bilgi sistemleri de bu alt bölümlerden sadece bir tanesidir. Bilgi sistemleri daha çok teknik konuları içeren bilgi işlem personelinin uzmanlık alanına giren konuları içerir. Teknolojinin değişimiyle paralellik gösteren ve hassasiyeti fazla olan bölümler içerir. Bu bölümdeki sorumlulukların, kontrol tedbirlerinin ve müdahale planlarının önceden belirlenip, senaryolar eşliğinde pekiştirilmesi gerekir.

1.11.1. Yazılım Güvenliği

Yazılım güvenliği, öncelikle yasal mevzuatlara uyumu gerektirir. Kullanılan yazılımların lisan belgesine sahip olması gerektiğini açıklar. Kurum içinde ihtiyaç olan yazılımların bireysel olarak değil, yetkili kişiler tarafından gerekli prosedüre göre kurulmasını öngörür. Bir yazılım ile ilgili güncellemeler ve değişiklikler yapılması yetkilendirilen personel tarafından olması gerekir.

Yazılım güvenliği dediğimizde gömülü olarak kullanılan yazılımların kontrollü olarak sisteme dâhil edilmesi ve bakım faaliyetlerinin devam ettirilmesi konularını da kapsar. Yazılım geliştirme ve yazılım satın alma konuları da teknik yeterliliğe sahip personel tarafından yapılmalıdır.

1.11.2. Ağ Güvenliği

Ağ güvenliği; kurum içinde kullanılan ağ sistemlerinin görevli personel tarafından kurulmasını ve bakımlarının yapılmasını ön görür. Kablosuz iletişimle ilgili gerekli şifrelemeler yapılarak kullanılmasını açıklar. Merkezi Girit'te olan Avrupa ağ ve bilgi güvenliği ajansının (ENISA) 2011 bilgisayar ve ağ güvenliği raporuna göre; cep telefonu ve cep telefonundan internete bağlanılmasıyla ilgili olaylarda 300.000 kişinin etkilendiğini ve özellikle GSM baz istasyonlarının çok az sürede tükenen güç kaynaklarından dolayı uzun kesintilerde haberleşmenin aksama olduğunu belirtmektedir.

1.11.3. Donanım Güvenliği

Kurumlarda bilgi güvenliği konusunda alınması gereken tedbirlerin başında bilgi giriş çıkışının kontrol edilmesi gelmektedir. Yetkilendirilen personelin dışında hiç kimse kuruma bilgi dâhil edemez ve bilgiyi dışarıya çıkaramaz. Bilgi giriş çıkış noktaları önceden belirlenmelidir. Kullanılan yazıcılarda kimlerin ne kadar, hangi seviyede bilgiyi dışa aktarabileceği verilen yetkilerle sınırlandırılmış ve raporlamaya açık bir şekilde takibe açık bir şekilde hazırlanmalıdır.

Taşınabilir veri depolama ortamları ve cihazlardaki veri kayıt cihazları yetkilendirilen personel dışında kullanılmamalıdır. Kullanılan cihazların bakım ve onarım faaliyetleri yetkili kişiler tarafından belirli prosedürler ışığında yapılmalıdır. Yeni eklenen donanım ve arızaya çıkan donanımın kontrolleri yapılarak sisteme giriş çıkışı sağlanmalıdır.

1.11.4. İnternet Güvenliği

Her kuruluş kendi ihtiyaçlarına ve kendi dinamiklerine göre farklı bir Bgys yapısına sahiptir. Gizlilik ilkesini ön plana çıkartan ve kendini koruma sistemlerinin korumasına güvenmeyen bir kurumda internet bağlantısı yasaklamaya kadar gidebilecek kararlar alınabilir. Bu yasaklama en kolay tedbirdir. Zor olan kurumunuzun kapılarını dış dünyaya açarak hala güvende kalabilmektir. İnternet kullanımında öncelikle yasal mevzuata uyum önemlidir. Yasaklı siteler ve uygulamaların kullanımı kurumlarda sistem yöneticisi tarafından yasaklanmalıdır.

Sanal ortamda yapılan işlemlerin kişileri ilgilendirdiği ve bu hareketlerin sistem tarafından takip edildiğini kullanıcılara bildirmek gereklidir. Geriye dönük internet kayıtlarının tutulması gerekir. Kurumun sanal ortamda sahip olduğu Web sitesi ve e-posta hizmetleri gibi hizmetleri de Bgys kapsamında işletilir. Verilen hizmetlerde Bgys de belirtilen şartlar sağlanmalıdır.

1.11.5. Kullanıcı Hesabı Güvenliği

Çalışanların kullandıkları kurum bilgisayarlarını kullanıma başladıklarında, sahip oldukları bir kullanıcı hesabı ile çalıştırmalarını gerektirir. Bu sayede hangi cihazda, kim, ne zaman, ne kadar süre ile çalışma yapmış ve sistemde nerelere girmiş ve hangi hareketleri sergilemiş bunun raporlamasını sağlar. Kullanıcı yetkileri belirli politikalarla belirlenmelidir. Kullanıcı hesapları güçlü şifrelerle korunmalıdır. Görev değişikliklerinde ve yeni katılımlarda personele kullanıcı hesabı bilgileri imza karşılığı verilmeli ve alınmalıdır.

1.11.6. Şifreleme Güvenliği

Günlük yaşantımızda kullandığımız en basit bilgilerimizin yer aldığı alanlarda dahi şifreleme sistemi kullanmaktayız. Kurum içinde yapılan uygulamalarda ve hesap işlemlerimizde de şifreleme ihtiyacı duymaktayız. Kurum varlıklarına erişimde kullanılan şifreleme işlemleri belirli sürelerde sistem tarafından şifre yenilemeyi zorunlu hale getirmelidir. Şifre yenileme ile ilgili uyarılar belirli sürelerde kullanıcılara sunulmalıdır.

Güçlü şifreler kullanılması hakkında eğitim faaliyetlerinde bilgilendirmeler yapılmalıdır. Karakterler, büyük harf, küçük harf ve sayıların ortaklaşa oluşturacağı şifreler konusunda örneklerle bilgilendirmeler yapılmalıdır. ASCII kodları kullanılarak oluşturulacak şifrelemelerle ve sanal klavyeler kullanılarak yapılan işlemlerde keylog (klavye tuş takibi) programlarına karşı alınabilecek tedbirler anlatılmalıdır.

1.12. SOSYAL MÜHENDİSLİK

Bilgi güvenliği sistemleri denildiğinde insanların ilk aklına ilk olarak teknik konular gelmektedir. Teknolojinin ve bilimin gerçekleşmesi için gereken ilk unsur

insandır. İnsanlar olmadan ne bir yeniliğe adım atılabilir nede keşfedilen yeniliğin bir anlamı olur. İnsanların hizmetine sunulan teknoloji ne kadar insanlığa hitap edebiliyor ve ne kadar insana erişebiliyorsa o kadar faydalıdır. İnsan davranışları teknolojinin gelişimine de yön veren en önemli unsurdur. Bireysel kullanıcı talepleri doğrultusunda kitlelere hitap eden yeni icatlar ortaya çıkmaktadır.

Bilgi güvenliği konusunda da durum aynıdır. En son teknolojiyle donatarak koruma altına aldığımız sistemlerimiz, bir bireyin isteyerek veya istemeden yaptığı en ufak bir davranış sonucunda yeterliliğini yitirebilir. Sistemdeki en ufak bir dişlinin dahi hasar görmesi tüm sistemin çalışmalarını sekteye uğratabilir. Onun için bilgi güvenliği konusunda yapılması gereken en büyük yatırım insana yapılan yatırım olmalıdır. Bireysel kullanıcılar eğitim faaliyetleri marifetiyle, özel yaşantılarında ve iş yaşantılarında bilgi güvenliği bilinci kazanmalıdır.

İnsanoğlunun zaaflarını kullanarak istediğiniz bilgiyi, veriyi elde etme sanatına sosyal mühendislik denir. Sosyal mühendislikte yöntemler verinin kaynağına, verinin gizliliğine, verinin nasıl korunduğuna göre değişmektedir. İyi bir sosyal mühendis anlık analiz yaparak ya da uzun zamanlı bir araştırma ile ilgili senaryoyu bilgisi ve hayal gücüyle tasarlar ve uygulamaya koyar. Sosyal mühendislikte metotlar uygulanacağı kriterlere göre değişmektedir. Kurbanın merakı, vicdanı, inancı, güveni, acıma duygusu, zaafları(makam, mevki, hırs, para, cinsellik, ego) gibi duygularını kullanarak veri hırsızlığı yapılabilir (Bilgiguvenligi, 2014).

İnsanlara güven telkin ederek yaklaşma ve bir sonraki adımda da onların iyi niyetlerinden yararlanarak onları aldatma olayları son yıllarda günlük yaşantımızda dahi karşımıza rahatlıkla çıkabilecek bir olay haline geldi. Yapılan bu sahtekârlık işlemlerinin, teknolojik gelişmelere paralellik göstererek kendini bilgi çağının şartlarına göre yenilemesi sonucunda ortaya çıkardığı bu kavrama sosyal mühendis kavramı denilmektedir. Çoğu insan bu tür eylemlere maruz kaldıklarını hiçbir zaman fark etmeyebilir. Genellikle bir başkasının da başına gelen bir olay öğrenildiğinde, kendi yaşanmışlıklarıyla kıyaslayıp kendisinin de mağdur olabileceğini düşünür.

Sosyal mühendisler öncelikle etkileşime geçeceği hedef kitleye güven aşılar. Toplumun saygısını görecek niteliklere sahip olduğunu insanlara gösterir ve hedef kitleyi etkiler. İkna yeteneği yüksek kişilerdir. İnsanların zayıf yönlerini araştırırlar ve

her insanın zayıf bir noktasını tespit ederler. Her insan kendisinin bu tür saldırılara karşı hazır olduğunu düşünür ve kimsenin ona zarar veremeyeceğine inanır. Ama unutulan nokta şudur ki; yapılan saldırı hiç beklenmeyen anda ve hiç beklenmeyen kişilerden gelmektedir. Saldırı yapan kişi güvenimizi kazanmış olan ve hiçbir zaman ondan böyle bir şey beklemeyeceğimiz kişilerdir.

Hiç bir sistem insandan bağımsız değildir. Bilgisayar sistemleri, insanlar tarafından tasarlanır, bakımı ve işletimi insanlar tarafından yapılır ve sistemden faydalanan ve sistemi kullananlar da insandır. İnsan bileşeni aynı zamanda bir güvenlik sisteminin en zayıf halkasıdır. Bundan dolayı insan faktörünün istismarına dayanan sosyal mühendislik saldırılarının gerçekleşme olasılığının her zaman olduğu ve göz ardı edilemeyeceği açıktır. Sosyal mühendislik saldırılarının başarısı, bilgisayar ve ağ sistemlerindeki yerel zayıflıkların varlığına bağlı olduğundan, yerel açıklıklara verilmesi gereken önemi artırmaktadır. Sosyal mühendislik saldırılarının etkisini en aza indirgemenin yolu güvenlik politikalarının güncel tutulmasından ve personelin uygun bir şekilde bilgilendirilmesinden geçer (Bilgigüvenliği, 2014).

1.13. SİBER GÜVENLİK

Gelişen teknoloji ile beraber hayatımıza yeni kavramlarda girmeye başlamıştır. İnternet ağının dünyayı biri baştan bir başa sarması sonucunda yeni bir dünya ortaya çıkmaya başlamıştır. Gözümüzle görüp, elimizle dokunamasak ta bu dünyanın etkilerini çok net bir şekilde günlük hayatımızda hissedebilmekteyiz. Sanal ortamda hazırlanan özel ağ yapısı sayesinde, günlük hayatımızda yaptığımız birçok işi daha kolay ve daha hızlı yapabilir olduk. Dünyanın her hangi bir yerindeki bir insanla sanki yanı başımızdaymış gibi rahatlıkla görüyor, konuşabiliyoruz. Bankalarda kuyruk bekleyerek uzun uğraşlar sonucunda yaptığımız bir işlemi, şimdilerde evimizden çıkmadan bir bilgisayarla yâda cebimizdeki bir telefonla rahatlıkla yapabilmekteyiz.

Siber dünyada daha hızlı ve daha kolay işlerimizi yapabilmemize karşın, siber dünyanın daha fazla ve daha etkin tehlikeleriyle de karşılaşmış oluyoruz. Biz nasıl evimizden çıkmadan dünyanın bir ucundaki sanal bir mağazadan alışveriş yapıp, kapımıza kadar alabiliyorsak; dünyanın her hangi bir yerindeki bir kişide rahatlıkla evinden dahi çıkmadan bizim evimize girebilir veya bizim banka hesaplarımıza bile

müdahale edebilir. Siber güvenlik kavramı; siber dünyadaki bilgi güvenliği konularını içerir. Bilgi güvenliği ve ihlali ile ilgili kavramların sanal ortamda yaşanması durumunu açıklamaktadır. Siber güvenlik konusu da bir birey bazında olabileceği gibi, ülkeler üstü yapıları ilgilendiren düzeyde de olabilir. Her hangi bir siber güvenlik olayının yaşanması sonucunda; kaybedilecek olan varlıkların niteliğine göre siber güvenlik için alınacak tedbirleri de değişiklik göstermektedir. Siber güvenlik olaylarının ülkeleri etkileyecek düzeyde yaşanması durumu da siber savaş kavramlarını ortaya çıkarmıştır.

> *Siber savaş bir devlet tarafından, bir devlet adına veya o devleti desteklemek üzere başka bir ülkenin bilgisayar veya bilişim ağlarına veri eklemek, değiştirmek yâda bozmak veya bilgisayarları, ağ üzerindeki cihazları yâda bilgisayar sisteminin kontrol ettiği nesneleri kesintiye uğratmak veya onlara hata vermek amacıyla yetkisiz giriş yapılamasıdır. Bilgisayarlar aksayınca boru hatları yakıt iletemez. Gazınız, elektriğiniz, suyunuz, telefonunuz kesilir. Kara, deniz, hava trafiği durur. Hastaneler hizmet veremez. Bankadan para çekemezsiniz. Gazeteler çıkmayınca, ekranlar kararınca olup bitenden haber alamazsınız. Dağıtım sistemleri çöker, marketlere ve çarşıya mal gelmez. Yağmalamalar başlayabilir (Clarke ve Knake,2010:119).*

Yıllarca A.B.D. yönetiminin üst kademelerinde görev yapmış bir kişi Siber savaşın etkilerini bu şekilde kitabında açıklamakta ve bizleri ne gibi tehditlerin beklediği konusunda uyarmaktadır. Siber güvenliğin sağlanması adına NATO bünyesinde de ülkeler üstü çalışmalar yürütülmektedir. 2013 yılında Cambridge üniversitesi tarafından yayınlanan "Siber Savaşta Uygulanacak Hukuk Hakkında Tallinn El Kitabı" NATO desteğiyle uluslararası bağımsız uzmanlar tarafından hazırlanmıştır. Atılan bu adımlar siber güvenliğin gelecek yıllarda ciddi boyutlarda tartışılacağının birer örneğidir.

Dejan Kosutic'in dokuz adımda siber güvenlik kitabında; bilgi güvenliği standartları konusunda kısa bilgiler verilip, her kuruluşun iş sürekliliğini ve bilgi güvenliğini sağlaması için kendi dinamiklerine göre bir veya birkaç standardı kendilerine seçip uygulamalarını tavsiye etmektedir. Bu konuda ISO27032 Siber güvenlik için yazılmış olan kılavuzda faydalı bir kaynak olacaktır. Ülkemizde de siber güvenlik adına birçok konferans ve çalışmalar düzenlenmektedir. Bu konuda devlet adına araştırmaların birçoğu TÜBİTAK bünyesinde oluşturulmaktadır.

Ulusal siber güvenlik kapasitesinin arttırılmasına yönelik çalışmalar gerçekleştirmek amacıyla kurulan Siber Güvenlik Enstitüsü'nün (SGE) faaliyetleri 1997 yılında Bilişim Sistemleri Güvenliği (BSG) Birimi adı ile TÜBİTAK Ulusal Elektronik

ve Kriptoloji Araştırma Enstitüsü (UEKAE) altında başlamıştır. 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak faaliyetlerini sürdürmektedir. SGE; siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürütmekte; askeri kurumlara, kamu kurum ve kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştirmektedir. Bugüne kadar başarı ile gerçekleştirdiği pek çok proje ile ülkemizde siber güvenlik bilgi birikimi oluşturulmasına önemli katkı yapmıştır (TÜBİTAK BİLGEM, 2014)

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ STANDARTLARI

Günlük yaşantımızda birey olarak herkes kendi bilgi güvenliğini korumakla hükümlüdür. Bizim etkileşim içinde olduğumuz kuruluşlarda önce kendi kuruluşlarının ardında iletişim içinde oldukları kuruluş ve kişilerin bilgi güvenliğini korumaktan sorumludurlar. Bilgi güvenliğine önem veren kuruluşlar; diğer kuruluşlar ve kişilere daha fazla güvence verdikleri için, daha fazla tercih edilerek daha fazla kazanç sağlama imkânı sağlayacaklardır.

Her birey ve her kuruluş kendi imkânlarıyla bilgi güvenliğini koruyabilir. Fakat önemli olan bu güvenlik tedbirlerinin ne kadar etkili olduğunun kanıtıdır. Vaatlerle güvence altına aldığımız, kendi imkânlarımızla kurup, kendi imkânlarımızla denetlediğimiz bir sistemin başarısı da şüphelerle dolu olacaktır. Bizim için sıradanlaşmış bir olay, sistemin dışından bakan bir kişi için önem arz edebilir. Bizim alıştığımız ve kabullendiğimiz bir davranış genel geçer kanun ve standartlara göre farklılıklar içerebilir. Önemli olan bizim ne söylediğimiz değil, bizim için sistemin dışından bağımsız uzman kişilerin bizler için ne söylediğidir. Uzmanların bizim hakkımızda bir şeyler söyleyebilmesi içinde bizim herkes tarafından kabul görmüş, geçerliliği olan standartlara göre BGYS kurmamız ve işletmemiz gerekir.

Bu noktada uluslararası standartlar karşımıza çıkmakta ve bize kılavuzluk etmektedirler. Hizmet ve ürün sağlayan firmaların uzmanları ve bilimsel enstitülerin uzmanları en küçük özellikleri tanımlamaya başladıklarında ve detayları geliştirmeye başladıklarında standartlar konusu da önem arz etmeye başladı. Bu uzmanlar bazı konular hakkında görüş birliğine vardılar. Bu konular uzunca bir zamanı kapsayan kalite, güvenlik ve güvenilirlik gibi özellikler içermektedir. Yazılı ve yayınlanmış halde olan bu standartlar hizmet ve ürün üreten hem bireyler için hem de kuruluşlar içindir.1946 yılında kurulan ISO (Uluslararası Standartlar Örgütü), 159 ülke tarafından desteklenmektedir (Disterer, 2013:92).

Uluslararası bu kuruluşun ülkemizdeki temsilcisi TSE (Türk Standartları Enstitüsü) dür. TSE 1960 yılında kurulan, özel hukuk hükümlerine göre yönetilen tüzel kişiliğe sahip bir kamu kurumudur. Sanayi ve Ticaret Bakanlığına bağlı olarak

faaliyetlerini yürütür. Bir standarttın geçerli TSE standarttı olabilmesi için, kurul tarafından kabul edilmesi ve resmi gazete yayınlanması gerekir. İhtiyaçlara göre önceden var olmayan bir standart oluşturulabilir veya mevcut uluslararası standartlar çevirileri yapılıp kurulda kabul edilerek TSE standarttı olma özelliğini kazanabilir. Bunun yanında standart işlemleri için personel yetiştirme, eğitim ve seminerler verme gibi görevleri vardır. Uluslararası Elektronik Komisyonu (IEC) elektronik standartların sağlanması için 1906 yılında kurulmuştur. ISO ve IEC kuruluşları birlikte yürüttükleri ortak çalışmalarla tüm dünyada geçerliliği olan standartlar oluşturmaktadırlar.

1970 lerin başında ABD'de Department of Defense (Savunma Bakanlığı) Rand Report R-609 olarak da bilinen "Bilgisayar Sistemleri için Güvenlik Kontrolleri" başlıklı bir rapor yayınladı. Birçok bakımdan bu rapor bilgi güvenliğinin ilk tohumları sayılmaktadır (Gemci ve Bay, [?]:199).

Bilgi güvenliği ve bilişim alanında hazırlanan, en fazla kullanılan standartlar ve kontrol sistemlerine kısaca değinelim. Bunlar ITIL, COBİT, ISO20000 ve ISO 27ailesi standartlarıdır. Bu standart ve kontrol sistemlerinin uygulanabilmesi içinde, yardımcı olacak alt başlıkları ilgilendiren standartlar mevcuttur. Bunlar ISO/IEC 15408 Bilgi teknolojisi güvenliği için değerlendirme kriterleri, ISO9000 Kalite sistemi standartları ve ISO31000 Risk yönetimi gibi yardımcı olacak standartlardır. Herhangi bir standartla ilgili çalışma yapılırken, bütünlüğün ve en iyi sistemin icra edilebilmesi için birbiriyle bağlantılı olan tüm standartlar incelenip, bütün alt maddeler kendi kontrol sistemlerine göre göz geçirilmelidir. Bu sayede bir standartta göre hazırlanan bir sistem, diğer standartların süzgecinden geçilerek hazırlandığı için çifte kontrol sistemiyle elden geçirilmiş olur. ISO27001 standartları hazırlanırken diğer yönetim standartlarından da yararlanılmıştır. ISO9001 ve ISO14001 standartlarının ne kadar etkili olduğunu bu standarttın ek-c bölümünde yer alan karşılaştırma tablosunda görmeniz mümkün olacaktır.

2.1. COBIT (Control Objectives for Information Technologies)

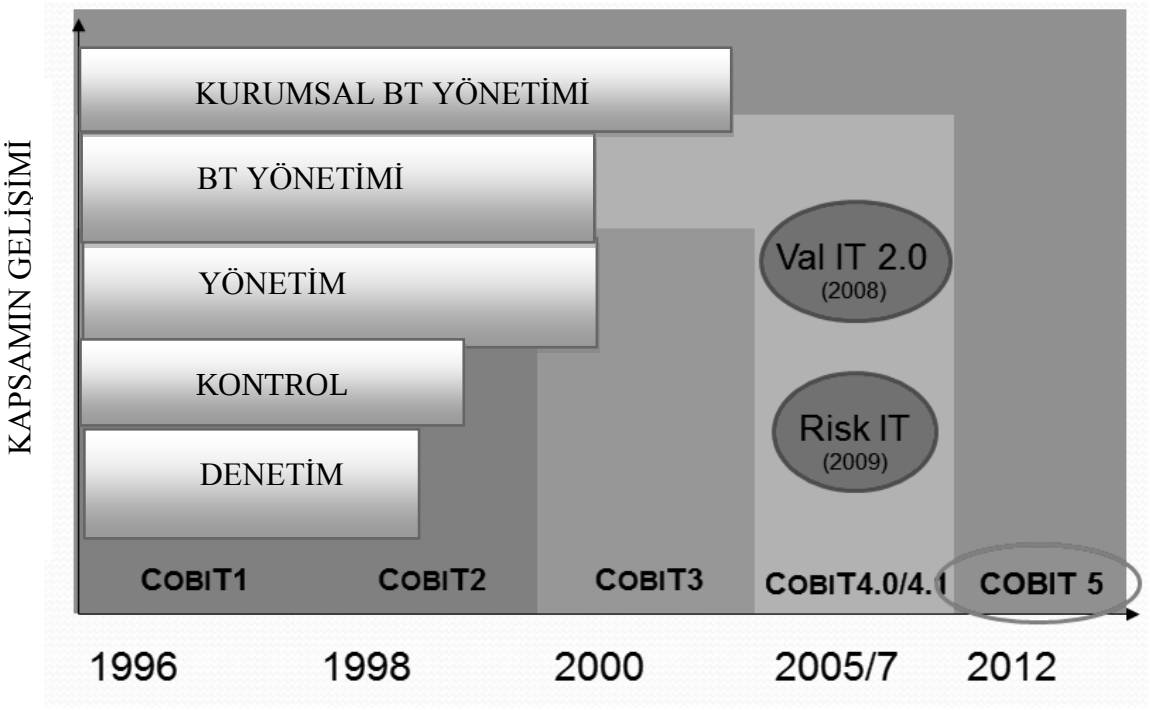
1969 yılında kurulmuş olan Bilgi sistemleri denetim ve kontrol birliği (ISACA) tarafından, 1996 yılında hazırlanmış olan bir denetim sistemidir. Türkçe karşılığı Bilgi

Teknolojilerine İlişkin Kontrol Hedefleri olan COBIT, zaman içerisinde kendini yenileyerek farklı versiyonlarla gelişen teknolojiye ayak uydurmaktadır. ISO standartları ile ITIL kaynaklarını temel alan bir sistemdir. Süreçten çok kontrol mekanizmalarıyla ilgilenir. Kuruluşlara neler yapması gerektiğini belirtir. Ama süreç tabanlı olmadığı için nasıl yapacaklarını anlatmaz. Bu durum bilgi sistemleri ve yönetim sistemlerinin birbirinden ayrı düşünülmemesi gerektiğini ve birbirini tamamlayan sistemler olduklarını bir kez daha göstermektedir. İş hedeflerinin, bilgi işlem hedeflerine dönüşmesini amaçlar. Aynı zamanda kaynakları, bilgi teknolojileri alt yapılarını; kaliteli, güvenilir ve hukuksal gereklilikleri yerine getirerek kullanmayı hedefler.

COBIT'in misyonu; işletme yöneticileri ve denetçiler tarafından günlük kullanılan, yeterli, geçerli, modern, uluslararası genel kabul görmüş bilgi teknolojisi kontrol amaçlarını araştırmak, geliştirmek, tanıtmak ve ilerletmektir. COBIT'in amacı, kâr maksimizasyonu, fırsat optimizasyonu, rekabetçi avantaj sağlamak için iş riski, kontrol gerekleri ve teknik konular arasındaki boşluklar arasında köprü kurmak için bir çatı oluşturmaktır (Uzunay, 2007:112).

COBIT hedefleri zaman içinde gelişen yeni ihtiyaçlar karşısında yetersiz kaldığını hissederek kendini geliştirerek yeni versiyonları ile karşımıza çıkmıştır. İlki 1996 yılında hazırlanmış olan COBIT hedefleri, 1998 yılında yönetim yönergelerinin de eklenmesiyle yeniden yayınlanmıştır. 2000 yılına gelindiğinde üçüncü bir versiyonuyla kendini yenileyerek yeniden basılmıştır. 2003 yılında bu versiyon online sürümü ile hizmete sunuldu. 2005 yılında Cobit3'de yayınlanan bütün kitaplar tek çatı halinde toplanarak COBIT 4.0 versiyonu yayınlanmıştır. 2007 yılında hedef açıklamaları basitleştirilerek, süreçler ile işletmenin, bilgi teknolojileri hedeflerinin ve bilgi teknolojileri süreçlerinin arasındaki ilişkiler yeniden tanımlandı. 2013 yılında yayınlanmaya başlamış olan COBIT 5.0 versiyonu daha kapsamlı ve daha uzun olarak tasarlanmıştır. ITIL ile bütünleşik bir kapsamda hazırlanmıştır.

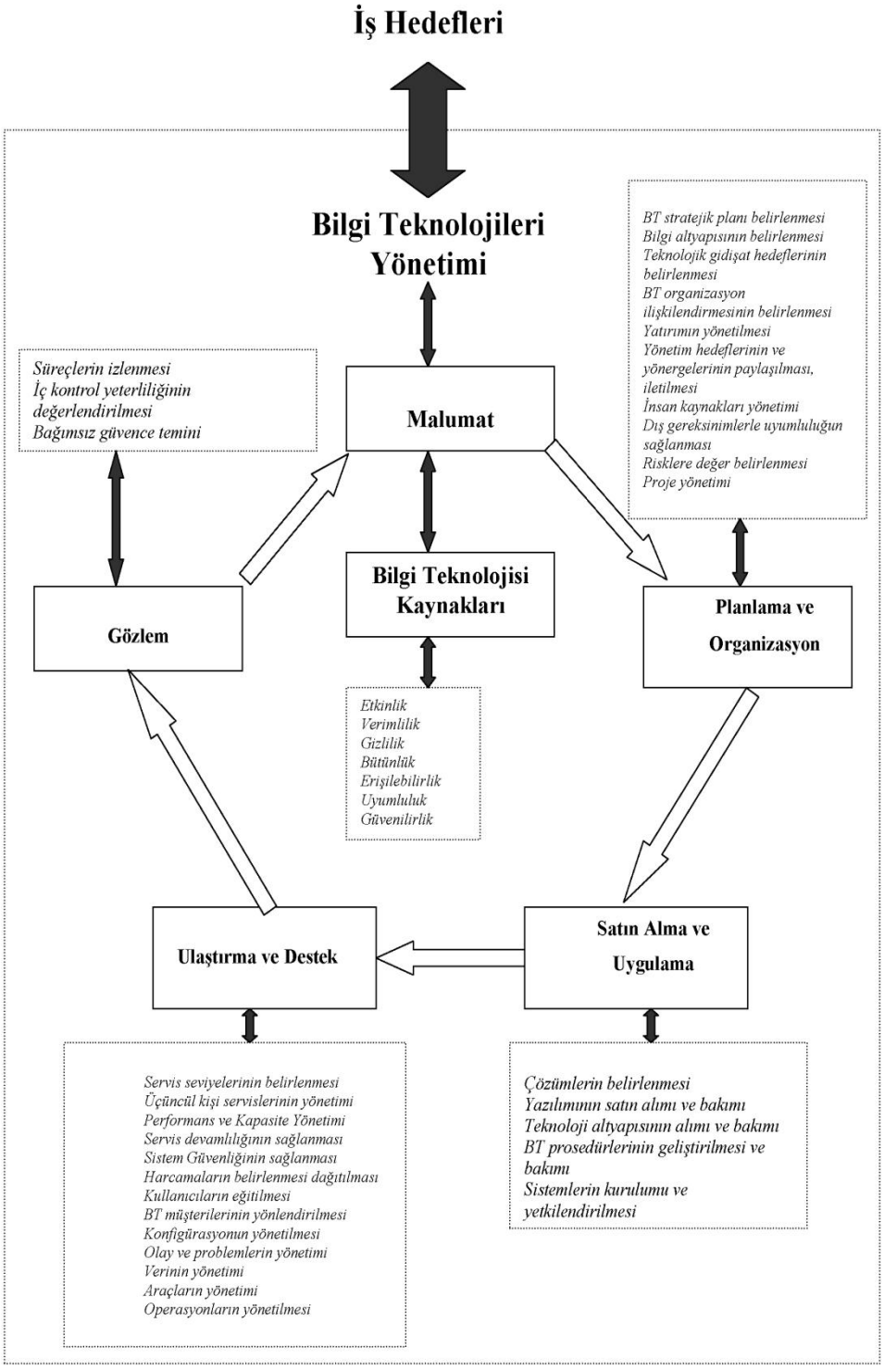
Tablo 1: COBİT Sürümlerinin Zaman İçerisindeki Yapısal Değişimleri



Kaynak : (Isaca, .2013).

Bu misyondan anlaşılabileceği gibi bu standart yönetme ve disiplin altına almayı diğer hedeflerin önüne almaktadır. Bu standarttaki temel amaç, bilgi teknolojilerini yönetmek ve denetlemek için yöneticilerin eline bilgi teknolojileri yönetimi konusunda daha fazla araç ve sistematik bir yaklaşım vermektir(COBIT Framework, 2000).

Kıssaca bilgi teknolojileri yönetişimi için sunulmuş bir modeldir. Bir standart değil, bir referanstır. Birçok standarttı özümsemiş, örneklemiş ve en iyi uygularını içerisine sindirmiştir. COBIT kurumumun iş (Bussiness) gereksinimini destekleyen bir araçtır. İş ve bilgi teknolojileri yönetimi arasındaki köprü görevini gören bir metodolojidir. COBIT kurum hedeflerine bilgi teknolojileri alt yapılarını etkin kullanarak ulaşmayı sağlayan bir araçtır (İsaca, 2009).



Şekil 3: Dört COBIT Alanının İş Hedeflerine Yönelik Akışı

Kaynak: COBIT 4.1., 2000:13.

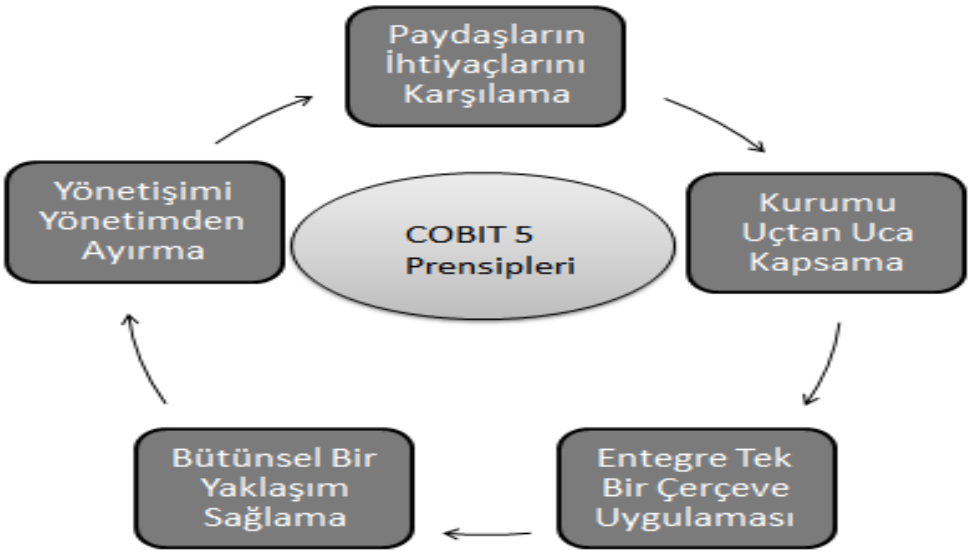
COBIT 5 yeni versiyonuyla üç kitaptan oluşmaktadır. COBIT çerçevesinin uygulanmasının anlatıldığı birinci kitap, yönetişim prensiplerinin olduğu ikinci kitap ve süreçlerin tasarımını anlatan üçüncü bir kitap mevcuttur. Birinci kitapta 5 ana prensipten oluşan COBIT çerçevesinin uygulanması yer almaktadır. Bu prensiplerden birincisi olan bütünleyici çerçeve ISO, ITIL ve diğer bilgi güvenliği standartlarının incelenmesi ve yeniden hepsini kapsayacak şekilde bir hazırlık yapılmasını kapsar. Tek ve entegre bir çerçeve oluşturmayı amaçlamaktadır. Bilgi teknolojileri alanında 110 000'den fazla bilgi teknolojileri uzmanının, ISACA bünyesinde yapmış olduğu çalışmalar neticesinde COBIT 5 oluşturulmuştur.

İkinci prensip olarak da risklerin en uygun hale getirilerek, kaynak kullanımını en iyi şekilde sağlayarak ve fayda farkındalığı oluşturarak paydaş değerleri odaklı bir strateji açıklanmıştır. Paydaşların ihtiyaçlarını karşılamak başlığı altında açıklanmaktadır.

Üçüncü prensipte ise; yeni versiyon ile tüm kurumu uçtan uca kapsayacak şekilde bir çalışma yapılması gerektiği anlatılmaktadır. Zaten COBIT gelişim çizelgesine baktığımızda yeni versiyonlarıyla beraber zaman içinde kapsamındaki değişimleri de görebilirsiniz.

Dördüncü prensip bütünsel bir yaklaşım oluşturmayı açıklar. Yeni versiyonla beraber diğer bilgi güvenliği standartlarından ve rehberlerinden de yararlanılmıştır. Bu sayede ortaya daha kapsamlı bir yaklaşım çıkmıştır. Kurumsal yapı, kişiler, beceriler, yetenekler, prensipler, politikalar, süreç, etik davranışlar, kültür, servis ve alt yapı gibi konular bu bölümde incelenir.

Beşinci prensipte yönetişimi yönetimden ayrılmak olarak karşımıza çıkmaktadır. Yönetim ile yönetişim kavramları arasındaki farkları ortaya koymaktadır. Yapılacak görevleri, oluşturulacak sorumlulukları net bir şekilde kim tarafından yapılacağını belirtir. Kimin sürecin neresinde, ne görevini üstlenmesini açıklar. Kurumsal hedeflerin belirlenmesi, kaynakların kullanılmasını kimin yapması gerektiğini açıklar.



Şekil 4: COBIT 5 Prensipleri

Kaynak: (Isaca, 2014)

İkinci kitapta süreç tasarımı rehberi yer almaktadır. Kurumsal yönetişim süreci de eklenerek bu bölüm COBIT 4.1'e göre yeniden düzenlenmiştir. Yönetim süreçleri ve yönetişim süreçleri diye ikiye ayrılmış olarak süreçleri tanımlamıştır.

Yönetim süreçlerinin içinde yeni olan bazı süreçler eklenmiş ve kimi süreçlerin yerleri değiştirilmiş başka bir başlık altında toplanmışlardır. Yeni oluşturulan süreçler; yönetişim çerçevesinin belirlenmesi ve yaşatma, yeniliklerin yönetimi, ilişkilerin yönetimi ve yönetim çerçevesini tanımlama, varlıkların yönetimi, iş süreçleri kontrolleri yönetimi, ilişkilerin yönetimi ve bilgi birikimi süreçleridir.

Yönetişim bölümünde de ISO38500 standartlarından faydalanılarak üç seviyede değerlendirmelerini yapmıştır. Değerlendir, yönet ve izle ilkelerinden oluşan yönetişim bölümü birinci seviyeyi tanımlar. Planla, oluştur, çalıştır ve izle ilkeleri ikinci bölüm olan yönetim bölümünü tanımlar. Planla, yap, kontrol et ve harekete geç ilkeleriyle üçüncü bölüm olan operasyon bölümü tanımlanmıştır.

Üçüncü kitap olan uygulama ve kurumsal bilgi sistemleri yönetişimin prensip tasarımı, yönetişimin sürekli geliştirilmesi bölümü diğer bölümlerde yer alan değişikliklerin etkisiyle değişime uğramıştır. COBIT 5 ile gelen yenilikler sistemin

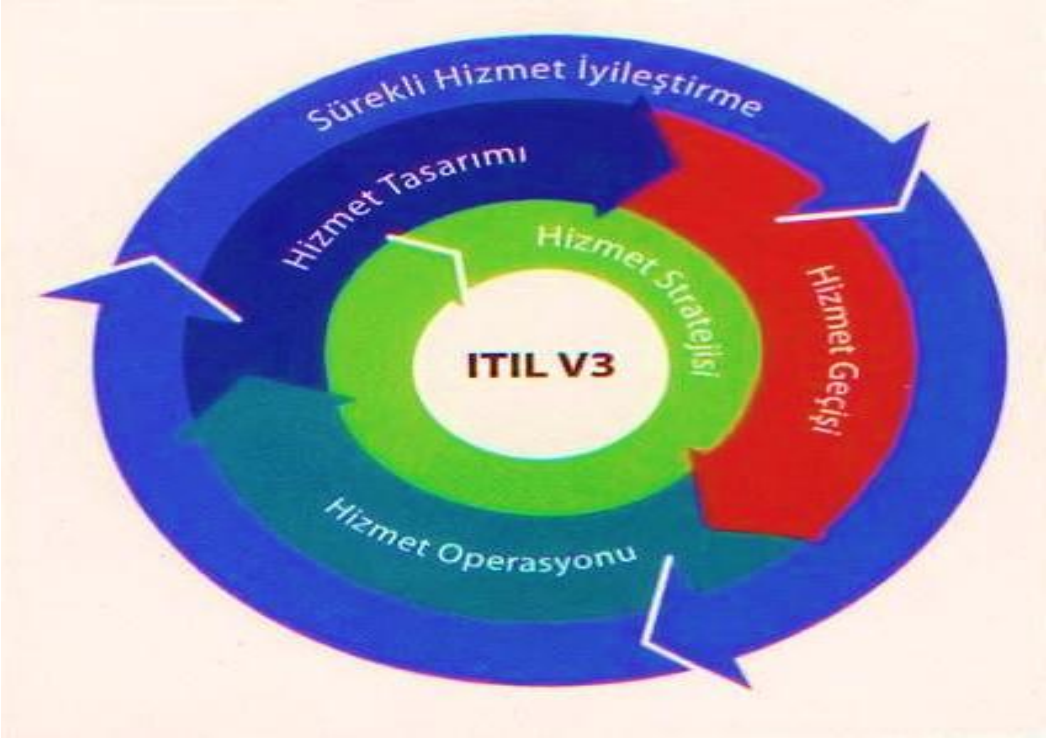
uygulama ve geliştirme süreçlerini etkilemiştir. COBIT hedefleri ISACA tarafından ücretsiz olarak kendi sitesinden bu kontrol hedeflerini yayınlamaktadır. 2014 yılı itibariyle Türkçe olarak da COBIT 5'in yayınlanması beklenmektedir. Yeni bir sürümün yayınlanmasıyla beraber, uyulacak hedeflerden yeniden şekillenmektedir.

Buna bağlı olarak da yapılan denetimler değişkenlik gösterecektir. Bankalar için zorunluluk haline getirilen COBIT hedefleri, kapsamının genişletilmesiyle beraber diğer sektörler içinde kullanım zorunluluğu getirebileceği düşünülmektedir. COBIT 5, işletmelere, teknolojik ortamlara, tüm iş modellerine ve kurumsal kültürlerde kullanılabilir. COBIT 5, Finansal işlem ve raporlama, risk yönetimi, güvence faaliyetleri, mevzuatla ilgili düzenlemelere uyumu, bilgi güvenliği, kurumsal bilgi teknolojileri yönetişim ve yönetimi konularını kapsamaktadır.

COBIT kaynakları ISACA tarafından hazırlanmaktadır. ISACA'nın kendi internet siteleri üzerinden yayınlamış oldukları bu kaynaklara erişim ücretsizdir. COBIT' in uygulanması sonucunda elde edilen bir sertifika yoktur.

2.2. ITIL (INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY)

ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi) uygulaması 1980'li yıllarda ortaya çıkmıştır. İngiltere'de Ticaret Bakanlığı tarafından yapılan çalışmalarla ortaya çıkmış ve tüm dünyada kabul görmüştür. Müşteri, tedarikçi, bilgi teknolojileri ve bilgi teknolojileri kullanıcıları arasındaki ilişkileri en uyumlu hale getirmek için hazırlanmıştır. Bunu yaparken de servis yönetimini ve servis sağlama süreçlerini dikkate alarak kaynaklar oluşturmuştur.



Şekil 5: ITIL Yapısına Genel Bakış

Kaynak: http://ise.atilim.er/ (12.04.2014)

Büyük küçük tüm bilgi teknolojileri örgütleri için kullanılabilen, en iyi uygulama ve deneyimlerin bir araya getirilmesiyle oluşturulan süreç merkezli bir yaklaşımı benimseyen bir kütüphanedir. ITIL yapısını kendisine uygulayan bir kuruluş için bir zorunluluk gerektirmez. ITIL kullanan bir kuruluş kendi örgüt kültürüne, teknolojik alt yapısına ve kuruluşun dinamiklerine göre yorumlanabilme ve esnetilebilmesine olanak sağlamaktadır.

ITIL sürecinin sonunda resmi olarak denetimler yapılmaz ve bir sertifika alınmaz. Özel olarak uyumluluk denetimleri yaptırılabilir. Tavsiyeler içeren yapısı çalışanlara ne yapmaları gerektiği ile ilgili ışık tutar ve bilgi teknolojileri çalışmaları için yardımcı bir kaynak niteliği taşır. ITIL zamanla yeni versiyonlarını geliştirmiş; 2001 yılında ikinci sürümünü, 2007 yılında üçüncü sürümü ve 2011 yılında üçüncü sürümün yenilenerek en son halini almıştır. Bu aşamadan sonra artık ITIL sonuna eklenen versiyon numarasını kullanmamaya başlamış ve sadece ITIL olarak kullanılmaya başlanmıştır.

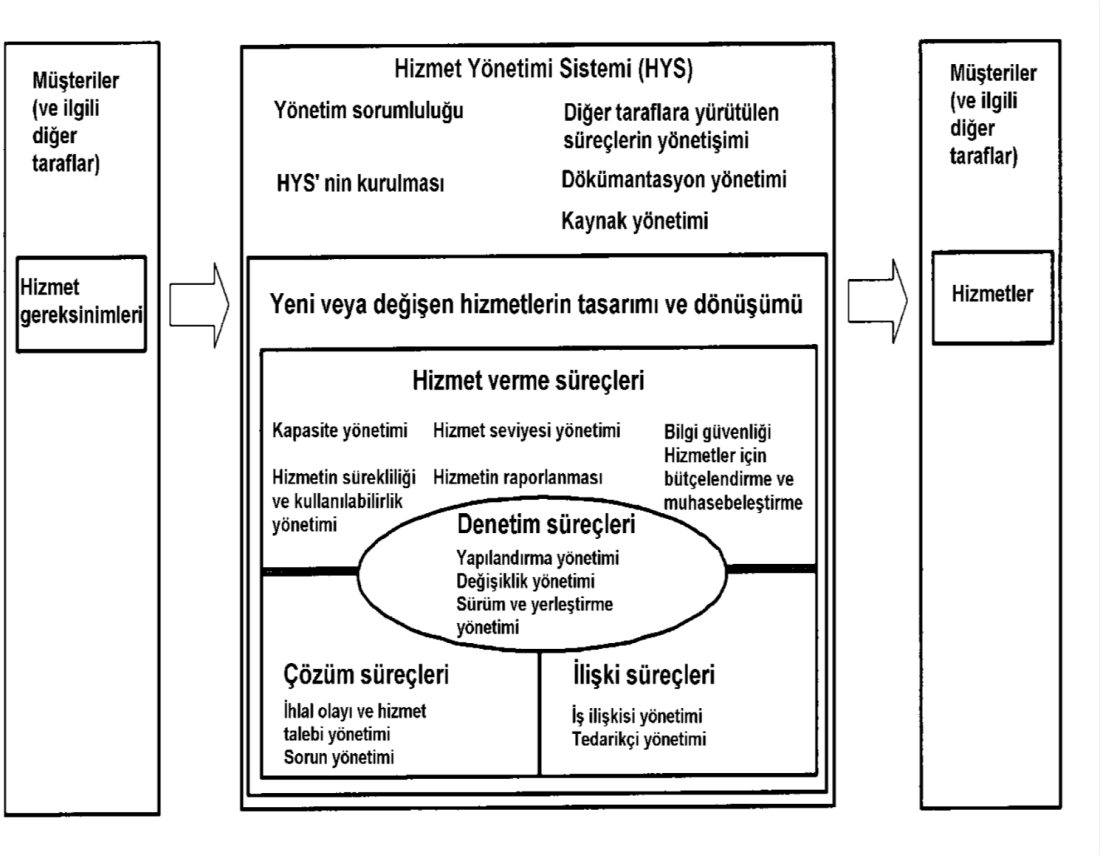
ITIL beş temel bölümden oluşur. Süreçler, anahtar kavramlar ve aktivitelerin yer aldığı birinci bölüm hizmet stratejisinin açıklandığı bölümdür. İkinci bölümde hizmet tasarımı yer almakta, üçüncü bölümde hizmet geçişi, dördüncü bölümde hizmet operasyonu anlatılmakta ve beşinci bölümde yedi adımda iyileştirmeleri hedefleyen hizmet iyileştirme sürekliliği PUKÖ döngüsüyle beraber işlenerek anlatılmaktadır. 2013 yılında ülkemizde Türkçe olarak yayınlanan "ITIL Terim ve Tanımlar Sözlüğü" ITIL çalışmaları yapacak olan yerli araştırmacılar için önemli bir kaynak niteliğindedir.

2.3. ISO/IEC 20000–1 BİLGİ TEKNOLOJİLERİ HİZMET YÖNETİM SİSTEMİ

2005 yılında ISO (Uluslararası standartlar örgütü)tarafından 2005 yılında iki bölüm olarak yayınlanmıştır. Birinci bölüm ISO/IEC 20000–1 Bilgi teknolojileri hizmet yönetim sistemi standardının gereksinimlerini içeren ve belge sahibi olmak isteyenlerin takip ettiği şartların yer aldığı bir standarttır. İkinci bölüm 20000–2 bu standartla ilgili uygulama prensiplerinin yer aldığı bilgi niteliğinde bir çalışmadır. Bu iki standartta 2011 yılında güncellenerek şu anda kullandığımız yeni sürümleriyle kullanıma sunulmuştur.

Bu standart ailesinin içinde ISO20000–3 Bölüm–3; ISO/IEC 20000–1 Standardının Kapsam Tanımı Ve Uygulanabilirliği Hakkında Kılavuz isimli bir standart daha vardır. Bu standartta 20000–1 standardının kimler tarafından kullanılabileceğini, hizmet sunumunda kullanılan hizmet kapsamı, tedarik zincirleri, hizmet yönetim sistemlerinin kapsamı ve bu kapsamlara göre senaryolar mevcuttur. Bu standart ailesinde yer alan diğer bir standartta ISO20000-5'tir. Bu standart ISO20000–1 standardının gereksinimlerini yerine getirmek isteyenler için örnek uygulama planları içermektedir.

ISO/IEC 20000–1 için örnek gerçekleştirme planı ismiyle anılır. Amacı 20000–1 standardını gerçekleştirmek için kullanılan aşamalı yaklaşım metodunu anlatmaktır. Hizmet sağlayıcılar isterlerse bu aşamaları kendine göre değiştirebilirler. İçerisinde aşamalı yaklaşımını yararlarını, boşluk analizi, hizmet iyileştirmesini, her aşamanın hedefleri ve önemli özelliklerinin nasıl olacağını açıklayan bölümler mevcuttur.



Şekil 6: Hizmet Yönetimi Sistemi

Kaynak: TS ISO/IEC 20000–1 Hizmet Yönetimi Standardı

ISO20000–1 Bilgi teknolojileri hizmet yönetim sistemi gereksinimleri standardının amacı müşteriler ve hizmet sağlayıcılar için hizmet gereksinimlerini ortaya koymak ve hizmetin geliştirilmesini sağlamaktır. Bu standardın amacı hizmet yönetimi sistemini kullanacak olan kuruluşlara sürecin her aşamasında yardımcı olmaktır. Sürecin en başından planlama aşamasından, politikaların oluşturulması, sistemin yaratılması, iyileştirmelerinin yapılması, kontrollerin yerine getirilebilmesi için oluşturulan tüm gereksinimler aşama aşama anlatılmaktadır.

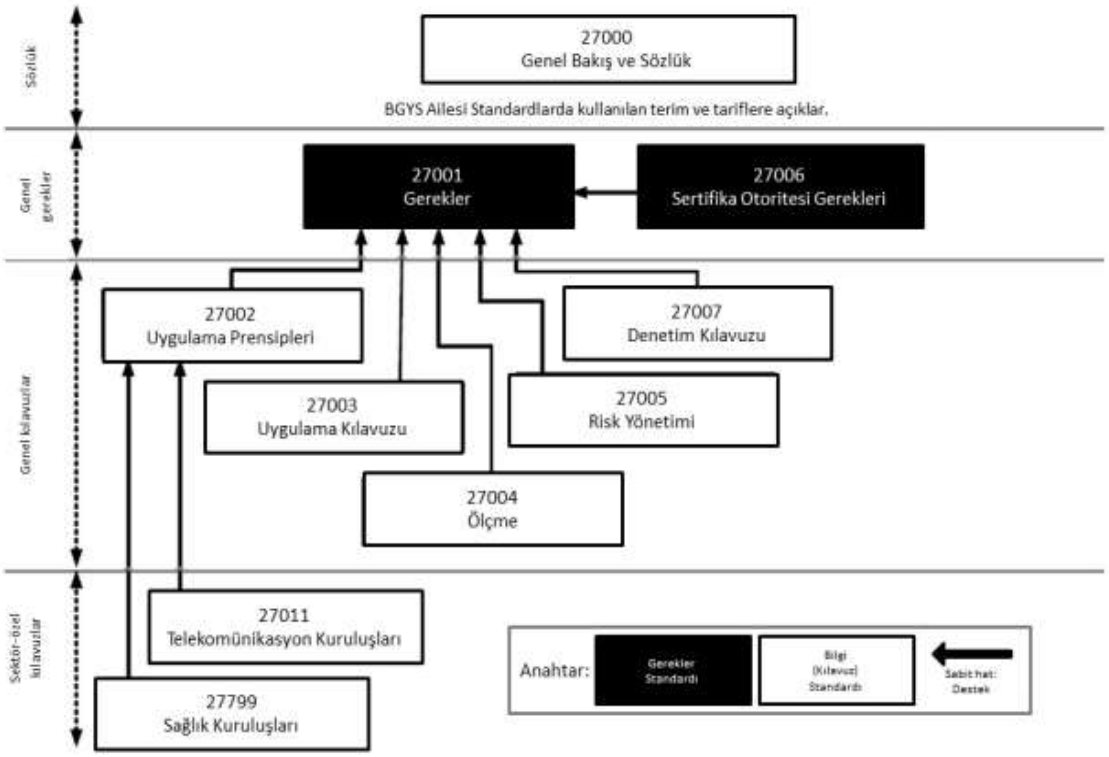
Üçüncü bölümde hizmet yönetim sistemi ve bilgi güvenliği yönetim sistemi içerisinde yer alan terimler ve kavramlar açıklanmaktadır. Dördüncü bölümde yönetim sorumluluğu, kaynak yönetimi, dokümantasyon yönetimi, hizmet yönetim sisteminin(HYS) kurulması ve iyileştirilmesi konularını açıklayarak HYS genel gereksinimlerini anlatır. Beşinci bölümde yeni veya değişen hizmetlerin; planlanması, dönüşümü, tasarlanması ve geliştirilmesi açıklanır. Altıncı bölümde hizmet seviyesi yönetimi, hizmetin raporlanması, kapasite yönetimi, bilgi güvenliği yönetimi,

hizmetlerin bütçelendirilmesi ve hizmetlerin muhasebeleştirilmesi gibi konularla hizmetin süreci anlatılır. Diğer bölümlerde de iş ilişkisi yönetimi, ihlal olayı ve hizmet talebi yönetimi, tedarikçi yönetimi, kontrol süreçleri ve sorun yönetimi gibi konular açıklanır.

2.4. ISO/IEC 27000 BGYS STANDARTLARI AİLESİ

Standartlar iş yaşantımızda kontrol ve denetim mekanizmalarının herkes tarafından kabul görmüş, güvenilirliğinin ispatlanmış olması için geliştirilmiş ve bir kurul tarafından onaylanarak yazılı hale getirilmiş kurallardır. Standartlarda kendi içinde önem derecelerine göre farklılıklar göstermektedir. Bir standarttın kapsayacağı alana ve ileride oluşabilecek ihtiyaçlara göre gelecekte oluşturulacak alt kısımlara ve hangi alanlarda işlevsel olacağına göre önem kazanmaktadır. Aslında ilk bakışta bir standarttın sayısal verileri bize o standart hakkında kısaca bilgi verebilir. ISO 9000 serisi gibi, ISO27000 serisi standartlar sonunda bulundurduğu 000 sayıları ile bize önemini göstermektedir. Bu şekilde yer alan diğer standartlarda kendi içinde bir aile standartları olarak adlandırılırlar.

27000'dan başlayarak 27999 arası standartlar bilgi güvenliği standartlarına ayrılmıştır. 2005 yılında çıkan ISO27001 standardından sonra oluşan ihtiyaçlar doğrultusunda bu standart ailesi sınırlarında yeni kılavuzlar ve yeni standartlar oluşturulmaya başlanmıştır. Farklı sektörlerin bilgi güvenliğine olan ihtiyaçları önceden düşünülerek sonradan oluşacak standartlar için yer ayrılmıştır. Bu alanlarda genelden özele doğru yavaş yavaş doldurulmaktadır. Zaman içinde yapılan standartlarında ihtiyaçlara karşılık veremediği gözlemlenmiş ve aynı standart numarası ile yeniden revizyona gidilerek hazırlanmıştır. Bu durumda standarttın sonuna numarasından sonra gelen yılı belirten sayılarda değişikliğe gidilmektedir. Gelişen yeni tehdit, açıklık ve doğan yeni ihtiyaçlar bu değişikliklere gidilmesine sebep olmaktadır. Çünkü standartlar dinamik yapılarını korudukları sürece zamana ve güncel tehditlere karşı direnebilirler.



Şekil 7: BGYS Ailesi Standardları Arasındaki İlişkiler

Kaynak: ISO/IEC 27000 BGYS Genel Bakış ve Sözlük

2.4.1. ISO/IEC 27000 BGYS Genel Bakış Ve Sözlük

ISO standarttı olarak 2009 yılında kabul edilerek kullanımına başlanmıştır. Ülkemizde TSE tarafından kabulü ve Türkçe olarak yayınlanması 2012 yılını bulmaktadır. Bilgi güvenliği yönetimi ile ilgili genel bir anlatım yapar. BGYS ailesinde kullanılan terimler ve kavramlarla ilgili açıklamalarda bulunur. BGYS kısaca bir giriş yaparak önemini vurgular. Planla, uygula, kontrol et ve önlem al (PUKÖ) proses yaklaşımını açıklar. BGYS standartlarını kapsamlarına göre birkaç bölüme alarak kısaca sınıflandırır. Genel bakışı ve terminolojiyi açıklayan standartlar, gerekleri belirten standartlar, genel kılavuzluk sağlayan standartlar ve sektöre özel kılavuzluk sağlayan standartlar diye ayırarak kısaca bu standartlar hakkında da bilgiler verir. Aşağıdaki şekilde bu standartta yer alan ve BGYS ailesi hakkında kısa bir bilgi verilmektedir.

Standartlar hakkında bilgi verirken öncelikle kılavuzluk niteliğinde, zorunluluk içermeyen standartlardan başlayarak anlatıma devam ettik. Bu standartların yanında,

Ulusal elektronik ve kriptoloji araştırma enstitüsü (UEKAE) tarafından hazırlanan kılavuzlarda BGYS sürecini önemli derecede açıklayıcı kaynaklardır.

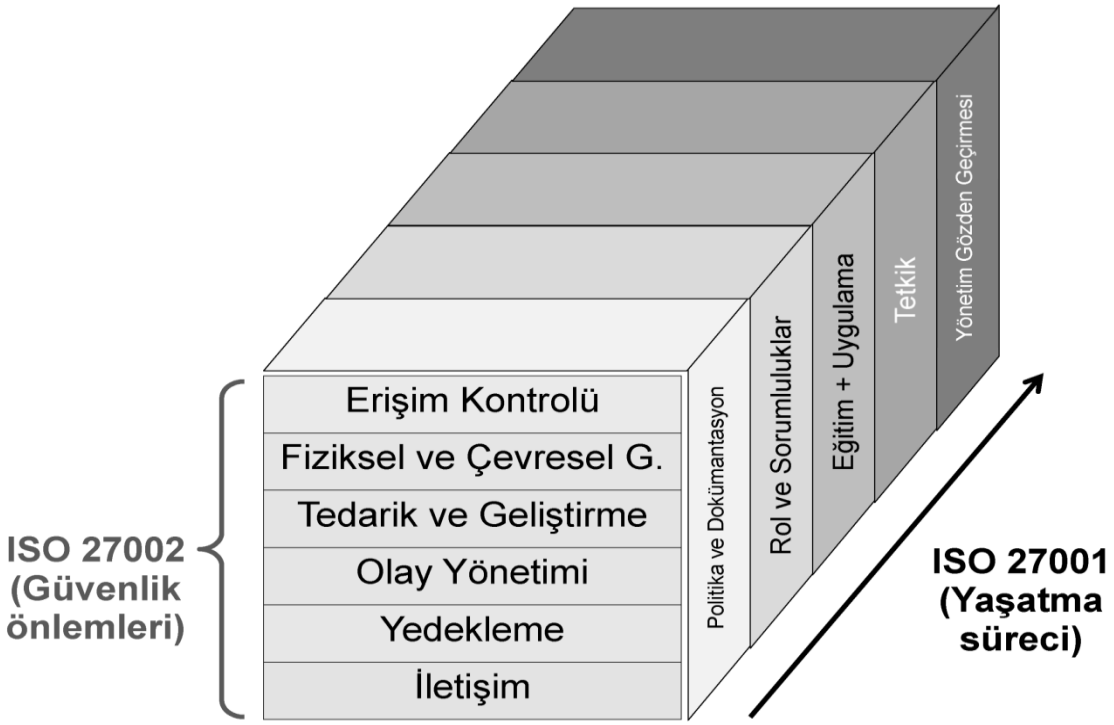
2.4.2.Genel Bakış Ve Terminolojiyi Açıklayan Standartlar

Bu Bölümde tüm standart ailesini etkileyen ve tavsiye niteliği taşıyan standartlara değineceğiz. Bu standartlar tek başlarına zorunluluk içermeyen standartlardır. Asıl amaçları temel ve sektöre- özel standartlar için yardımcı kaynak oluşturmaktır. ISO27000 BGYS genel bakış ve sözlük standarttı da bölüm içinde düşünülebilir.

2.4.2.1. ISO/IEC 27002 Bilgi Güvenliği İçin Uygulama Kodu

Birincisi 2007 yılında kullanıma başlanılan bu standart zaman içinde değişikliklere gidilerek 2013 yılında yeniden düzenlenerek yayınlanmıştır. TSE tarafından da kabul edilen bu standart, 2014 yılının Ocak ayında İngilizce olarak yayınlanmakta, çeviri işlemleri devam etmektedir. ISO 27001(2005) standardından sonra hazırlanan aile içindeki ikinci standarttır.

Bu standart 14 bölümde topladığı konuları, 35 alt kategoriye ayırarak, 114 kontrol maddesiyle bize sunulmaktadır. Bilgi güvenliği yönetimi, insan kaynakları, varlık yönetimi, erişim kontrolü, mobil cihazların güvenliği, ağ güvenliği, yasal gerekliliklere uyum, teknik yapıya uyum, bilgi transferi, iletişim güvenliği, kriptografik kontroller, sistemin gelişimi ve korunması, fiziksel ve çevresel güvenlik, bilgi güvenliği politikaları ve destekçilerle olan ilişkileri ele alan ve öneriler sunan bir standarttır. Bu kontrol maddelerini uygulama zorunluluğu yoktur.



Şekil 8: ISO 27001 –27002 İlişkisi

Kaynak: Ottekin (2011).

2.4.2.2. ISO/IEC 27003 Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu

Bu standart 2010 yılında yayınlanmış tavsiye niteliğinde olan bir standarttır. Bilgi güvenliği yönetim sisteminin başarılı tasarım ve uygulaması için kritik hususları kapsar. BGYS kapsamı, politikası ve tasarımı gibi konuları açıklar. Kurum analizi, risk değerlendirme ve işleme planlarını yönetme, BGYS projesini uygulama, kabul etme ve onaylama konularını içerir.

2.4.2.3. ISO/IEC 27004 Bilgi Güvenliği Yönetimi Ölçme

Bu standardın kapsamı ISO27001 standardında belirtilen bilgi güvenliğinin yönetilmesinde, uygulanmasında, kontrollerinde ve etkinliğinin değerlendirmesinde ölçümler yapılması konusunda tavsiyeler içerir. Ölçümlerin nasıl yapılacağı ile ilgili kılavuzluk sağlar.

2.4.2.4. ISO/IEC 27005 Bilgi Güvenliği Risk Yönetimi

Bu standart 2008 yılında yayınlanmıştır. Zorunluluk içeren bir standart değildir. Risk yönetimi konularında kılavuzluğu kapsar. Amacı bilgi güvenliği risk yönetimi gereklerinin tatmin edici bir şekilde yerine getirilmesi ve uygulanması konularında yardımcı olmaktır. Süreç odaklı risk yönetimi yaklaşımı konusunda yardımcı olur.

2.4.2.5. ISO/IEC 27007 Bilgi Güvenliği Yönetimi Sistemi İçin Kılavuz

2011 yılında hazırlanan bu standart tavsiye niteliğinde bir kılavuzdur. Bilgi güvenliği yönetim sistemlerinin denetimi konusunda ve BGYS denetçilerine yeterlilikleri konusunda yardımcı olur. BGYS kontrollerini yönetmek, iç ve dış denetimlere ihtiyaç duyan kuruluşlara kılavuzluk etmek için hazırlanmıştır.

2.4.3. Sektöre- Özel Hazırlanmış Standartlar

Bu bölümde yer alan standartlar belli bir sektör için hazırlanmış özel standartları kapsar. Bir önceki bölümde gördüğümüz genel bakış ve terminolojiyi açıklayan standartlarda da yararlanılarak bu standartlar hazırlanmıştır. Asıl amaçları ISO27001 sertifikasının alınabilmesi için yardımcı bir kaynak oluşturmak ve diğer bir genel gereksinim olan ISO27006 belgelendirme ve denetleme kuruluşları için gereksinimleri içeren standardın sağlanmasına yardımcı olmaktır.

2.4.3.1. ISO/IEC 27007 Denetçiler İçin Bilgi Güvenliği Kontrolleri

2011 yılında hazırlanan bu standart bilgi güvenliği sistemlerini denetleyen denetçi kişiler için hazırlanmıştır. Yapılan kontrol ve denetimlerde nelere dikkat edilmesi, denetimlerin nasıl yapılması ile denetçilere rehber niteliğinde bir kılavuzdur. Denetim esnasında ve öncesinde denetçilerin yapması gereken hazırlıklar, denetim esnasında denetlenen kuruluş ile yürüttüğü faaliyetler, denetim esnasında hazırladığı raporlar ve denetim sonunda hazırlayacağı sonuç raporları ile ilgili konuları içerir. Bu alanda denetim yapacak kişiler için tüm kalite yönetim sistemleri tekikinde denetçiler trafından kullnılan ISO19011 Kalite ve çevre yönetim sistemleri tetkik kılavuzu da önemli bir kaynaktır.

2.4.3.2. ISO/IEC 27011 Telekomünikasyon Kuruluşları İçin ISO/IEC 27002 Standardına Göre Bilgi Güvenliği Yönetimi Sitemi Kılavuzu

Bu standart 2008 yayınlanmış ve telekomünikasyon alanında faaliyet gösteren kuruluşlarda Bgy için yol gösterici bir kılavuzdur. ISO27001 standartının ek-a kısmında yer alan kontrol maddelerinin gereklerini yerine getirmeye yönelik bir çalışmadır. Kendi alanını ilgilendiren, başka herhangi bir sektörün konusuna girmeyen bölümleride mevcuttur. Siber saldırılara karşı ağ güvenliği ölçümleri, iletişim ve operasyonların yönetimi, fiziksel güvenlikle kontrol altına alınmış bölgeler, ekipman odalarının güvenliği gibi sadece kendi alanını ilgilendiren özel konulara değinmektedir.

2.4.3.3. ISO/IEC 27015 Bilgi Güvenliği Yönetimi Sitemleri Denetimi İçin Yönergeler

Bu standart 2012 yılında yayınlanmaya başlamıştır. Bu standarttın orijinal çeviri yapılmamış ismi finansal hizmetler için bilgi güvenliği kılavuzudur. Orijinal isminde de anlaşılacağı gibi finans sektöründe hizmet veren kuruluşların bilgi güvenliği alanında yapması gerekenler, nelere dikkat etmesi gerekir. Finans hizmetler sağlanırken kendi kuruluşunun ve üçüncü tarafların bilgi güvenliğini nasıl koruyacağı gibi konuları içerir.

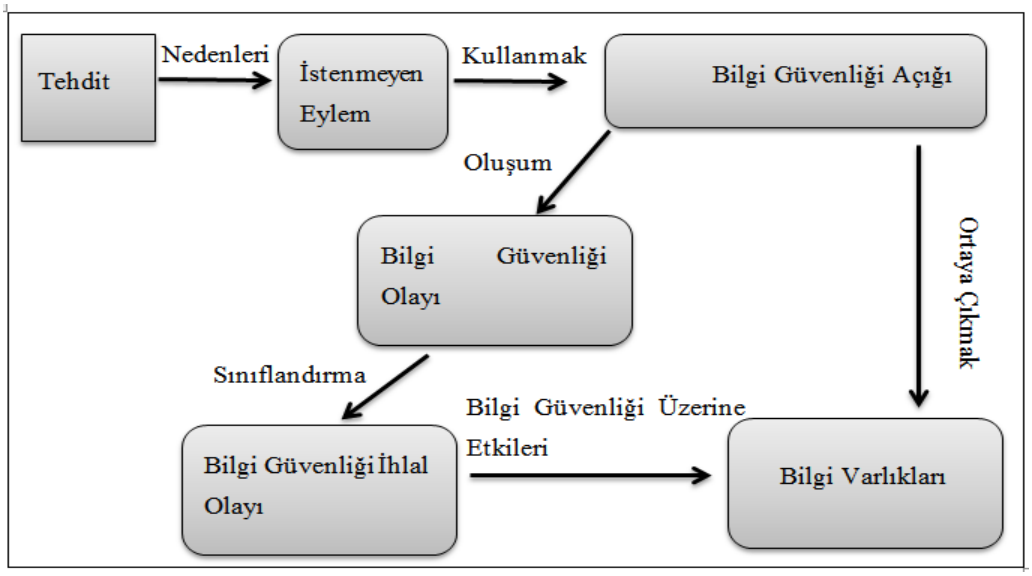
2.4.3.4. ISO/IEC 27032 Siber Güvenlik İçin Kılavuz

Bu standart 2012 yılında kabul edilmiştir. Siber güvenliğin uygulanabilmesi için rehber niteliğinde olan bir çalışmadır. Siber güvenliğin diğer güvenlik alanları ile olan ilişkilerini ve diğer standartlarla olan bağlantılarını açıklar. Ülkemizde son yıllarda kamu kuruluşları tarafından da siber güvenlik konusu ele alınmaya başlanmıştır. Bu konuda devlet destekli çalışmalar yürütülmeye başlanmıştır.

Siber güvenlik hakkında çalışma yapacak kişi ve kuruluşlara bir çerçeve çizme adına yardımcı olabilir. Bunun yanında siber güvenlikle ilgili; ülkemizde önden gelen üniversiteleri tarafından ve Tübitak işbirliği ile hazırlanan siber güvenlik çalıştayları ve konferansları yapılmaktadır. Siber güvenliğin uluslarası hukuk önünde nasıl olacağı ile Talinn tarafından hazırlanan, ‘Siber savaş hakkında uygulanacak hukuk hakkındaki’ el kitabı siber güvenlik alanında yapılacak çalışmlarda yardımcı bir kaynak oluşturacaktır.

2.4.3.5. ISO/IEC 27035 Bilgi Güvenliği İhlal Olayı Yönetimi

2011 yılında kabul edilen bu standart bilgi güvenliği ihlalleri ile ilgili yapılması gerekenleri anlatır. ISO 18044 bilgi güvenliği ihlal olayı yönetimi standartının yerini almıştır. Bilgi güvenliği olaylarını kategorilere ayırarak sınıflandırmayı açıklar. Bilgi güvenliği ihlalini tespit etmeyi, rapor etmeyi ve ortaya çıkan bilgi ihlal olylarından ders almayı açıklar. Tehditlere karşı hangi sıra ve metodla hareket edilmesi gerektiğini açıklar. Adım adım bilgi güvenliğine müdahale edildiğinde; ilk olarak tehditi durdurmaya yönelik, ardından tehditi kontrol altına almaya yönelik ve tehditi yok etmeyi gerçekleştecek adımlar atılmalıdır. Sırasıyla analiz ve raporlamaların yapılmasını ve takibin gerektiğini açıklar.



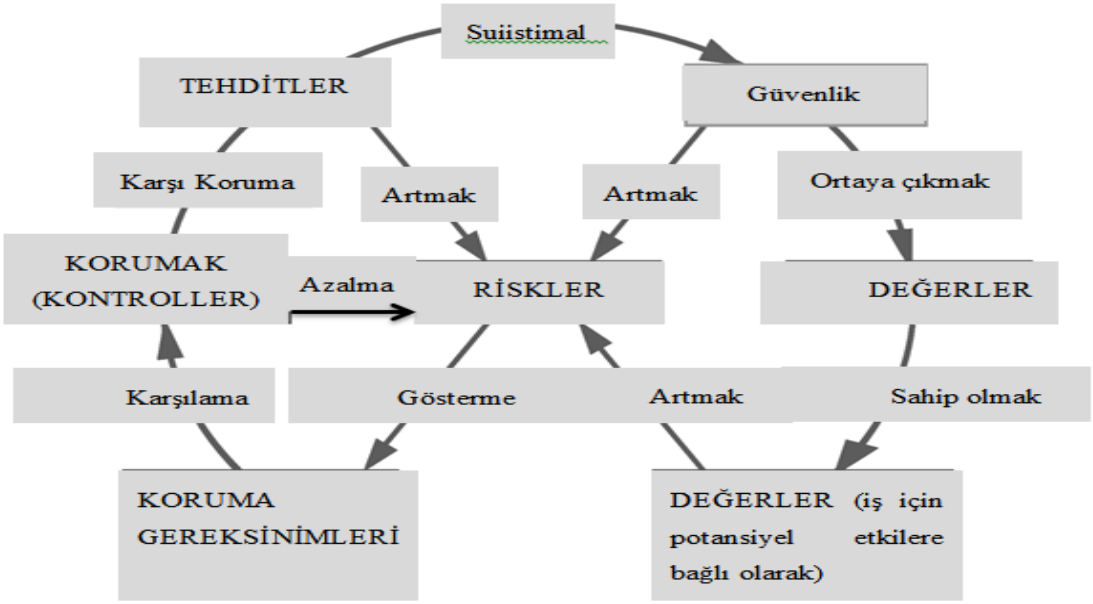
Şekil 9: Bilgi Güvenliği İhlal Zincirinde Nesnelerin Birbiriyle Olan İlişkileri

Kaynak: TS ISO/IEC 27035 Bilgi Güvenliği İhlal Olayı Yönetimi.

2.4.3.6. ISO/IEC 27799 Sağlık Sektöründe ISO/IEC 27002 Kullanımı İle Bilgi Güvenliği Yönetimi

Avrupa standardizasyon komitesi tarafından hazırlanan bu standart 2008 yılında kabul edilmiştir. Sağlık sektöründe faaliyet gösteren kuruluşların ISO27002 kurallarına uyumu ve ISO27001 ek-a da yer alan kontrol maddelerinin sağlanmasına yönelik bir kılavuzdur. Bu standart zorunluluk gerektirmez. Sağlık sektöründe oluşabilecek bilgi güvenliği tehditlerini tanımlar. Servis sağlayıcılardan doğacak, kurum içinden doğacak

ve kurum dışı tehditleri açıklar. İçeriden ve dışarıdan bilgilerin çalınabileceği, kullanıcı hataları, terörizm, bakım hataları, sistem hataları, iletişimin sızdırılması ve sağlık uygulamaları bilgilerinin izinsiz kullanılmasından doğabilecek sorunlar ve neler yapılması gerektiği ile ilgili bilgi verir. ISO27001 sertifikasını sağlık alanında faaliyet gösteren şirketler tarafından alınabilmesi için yardımcı bir kaynak oluşturur. Bu standarttın ek-b bölümünde yer alan ayrıntılı PUKÖ döngüsünün görevler ve dokümanlarla olan ilişkilerinin anlatıldığı diyagramlar mevcuttur. Tüm BGYS sürecini anlamak için açıklayıcı bir kaynak olmuştur. Bizde bu diyagramları orijinal haliyle size sunuyoruz.



Şekil 10: Riskler Ve Risk Kaynakları Arasındaki İlişkilerin Basitleştirilmiş Bir Risk Modelinde Gösterimi

Kaynak: TS EN ISO 27799 Sağlık Bilgi Güvenliği Yönetimi Kullanarak ISO/IEC 27002.

2.4.4. Temel Gereksinimleri İçeren Standartlar

Bu bölüm ISO27001 Bilgi güvenliği yönetim sistemleri gereksinimleri ve ISO/IEC 27006 Bilgi güvenliği yönetim sistemlerinin denetimini ve belgelendirmesini yapan kuruluşlar için gereksinimleri anlatan iki standarttı içermektedir. Bu iki standart belge sahibi olmak isteyen kuruluşlar için zorunluluk içeren gereksinimleri açıklar.

ISO27001 Bilgi güvenliği yönetim sistemleri gereksinimleri standarttı başlı başına ayrı bir konu olduğu için o standarttı ayrıntılı bir şekilde alt maddeleriyle beraber ilerleyen bölümde ele alacağız.

2.4.4.1. ISO/IEC 27006 Bilgi Güvenliği Yönetim Sistemlerinin Denetimini ve Belgelendirmesini Yapan Kuruluşlar İçin Gereksinimler

Kuruluşların BGYS kontrol ve denetimini yapan belgelendirme kuruluşları için standartların açıklandığı bir çalışmadır. BGYS belgelendirmesi yapan kuruluşların akreditasyonlarını sağlayabilmesi için hazırlanmış bir kaynaktır. Zorunluluk içeren standartlardandır. ISO 27001 gibi temel gereksinim içeren bir standarttır. ISO/IEC 17021:2006 standardında yer alan maddelerin takibi ile koordineli işleyen bir standarttır. Belgelendirme kuruluşlarının yeterlilik ve güvenilirliğini göstermeleri için bu standarttı uygulamaya geçmeleri gerekir. Bu standart öncelikle belgelendirme ile ilgili Bgys sürecinin başarıyla sonuçlanması neticesinde ortaya çıkacak yeni kavramların tarifiyle başlar.

Bir Bgys sistemini değerlendirmeden geçirerek tamamlayıcı dokümanlarla ve standartlarla denetimler yapan ve bu denetimler sonrasında başarılı olan kuruluşlara belgelendirme yapan bağımsız kuruluşları belgelendirme kuruluşu diye tanımlar. Bu standart içinde belge olarak tanımlanan kavram; belgelendirme kuruluşu tarafından, üzerinde akreditasyon şartlarına uygun olduğunu belirten ve üzerinde akreditasyon sembolü veya beyanı taşıyan belgeyi açıklamaktadır. Standarttın içinde yer alan işaret kavramı; ise ilgili ürün ya da kişilerin belirli bir standardın gereksinimlerine uyduğunu ya da bir kuruluş tarafından işletilen sistemlere olan yeterli güvenin mevcut olduğunu gösterir. Bir belgelendirme kuruluşunun ya da bir akreditasyon kuruluşunun gereksinimleri gereğince verilmiş bulunan ve hukuki olarak tescilli ticari işaret ya da hukuki olarak korunan başka bir sembol olarak açıklanır. Ayrıca işaretlerle ilgili kısa bilgi her TSE standart belgesinin ikinci sayfasında kısaca verilmektedir. Hangi işaretin TSE garantisini kapsadığı, hangi işaretin üretici beyanı olduğu ve hangi işaretin kalite faktör ve değerlerine uygunluğu ifade ettiği kısaca tanımlanmaktadır.

Beşinci bölümde belgelendirme kuruluşunun genel gereksinimlerine üç başlık altında değinmektedir. Hukuki yapı ve sözleşme konusu, sorumluluk ve finansman ve

tarafsızlığın yönetimi konuları ele alınmaktadır. Tarafsızlığın yönetimi konusunda alt başlıklar halinde belgelendirme kuruluşları ile belge almak isteyen kuruluşların ilişkileri açıklanır. Hangi faaliyetlerde beraber çalışma yapabileceklerini ve hangi vakte kadar bu faaliyetlerini yürütebileceklerini açıklar.

Kaynak gereksinimlerini anlatıldığı bölümde ise; yönetim ve personelin yeterliliği, kişisel kayıtları, dış denetçilerin ve dış teknik uzmanlarının kullanılmasını açıklar. Yönetim ve personelin yeterliliği dediğimizde belgelendirme kuruluşunun denetlemeler için oluşturacağı toplamsal yeterlilik, yönetim kademesi ve denetlemelerde çalışacak personelin seçilmesi, tedarik edilmesi ve yönetilmesini, yeterlilik analizini, sözleşmenin incelenmesini, değerlendirme yapacağı kuruluşun BGYS yapısı ile ilgili teknik ve hukuki gelişmelerini kapsar. Kaynaklar bölümünde denetçi firma çalışanlarının yeterliliğinin ve becerilerinin ölçülmesi ve hizmet sağladığı kuruluşlarla iletişimin devamlılığı anlatılır. Denetçilerin yeterliliği için tecrübe edilmiş yöntemler kullanılması anlatılır. Bunun içinde (Ek-B) de nelere dikkat edilmesi ifade ediliyor. Bu bölümde öncelikle ISO27001 Ek-A bölümünde yer alan kontrol maddelerinin farkında olması gerektiğini belirtir. Diğer maddelerinde ise denetçilere BGYS' ye ilişkin tipik bilgiler şu öneriler olarak sıralanır (ISO27006, 2010:32);

Denetçilerin, BGYS konuları ve aşağıdaki denetim konusunda bilgi ve anlayışa sahip olması önerilir:

- Denetim programlaması ve planlaması,
- Denetim türü ve metodolojileri,
- Denetim riski,
- Bilgi güvenliği süreç analizi,
- Sürekli iyileştirme için Deming döngüsü (PUKÖ: Planla Uygula Kontrol Et Önlem Al, PDCA: Plan Do Check Act),
- Bilgi güvenliği için iç denetimi.

Denetçilerin, aşağıdaki düzenleyici yapı konusunda bilgi ve anlayışa sahip olması önerilir:

- Fikri mülki haklar,

- Kurumsal kayıtların içeriği, korunması ve saklanması,
- Verilerin korunması ve mahremiyet,
- Şifreleme kontrollerinin düzenlenmesi,
- Sürekli iyileştirme için Deming döngüsü (PUKÖ),
- Anti-terörizm,
- Elektronik ticaret,

Yedinci bölümde; kaynak gereksinimlerinin diğer alt maddesinde belgelendirme kuruluşundaki personel ile onları eğitimleri üzerinde durulur. BGYS denetimi yapan denetçiler için eğitim, iş tecrübesi, denetçi deneyimlerinin seviyelerinin belirlenmesi ve denetçilerin yeterlilik için ne kadar süre, hangi iş süreçlerinde çalışarak yeterlilik seviyesine ulaşabileceği sınırlar belirtilmektedir. Dış denetçiler ve teknik uzmanların çalışmalarında ne gibi önlemler alınması gerektiği, çalışma yapılırken belgelendirme kuruluşu ile olan ilişkileri anlatılmaktadır.

Sekizinci bölümde bilgi gereksinimlerini açıklar. Belgelendirme dokümanları, belgelendirilen müşteri rehberi, gizlilik, kurumsal kayıtlara erişim, kamunun erişebileceği bilgiler, belgelendirmenin verilmesi, sürdürülmesi, süresinin uzatılması, belgelendirme kuruluşu ile müşteriler arasında bilgi alışverişini, kısaltılması, iptal edilmesi ve askıya alınması için işlemleri açıklar.

Dokuzuncu bölümde, süreç gereksinimleri ile ilgili hususlar ele alınmaktadır. İlk denetim ve belgelendirme faaliyetleri, teftiş faaliyetleri, yeniden belgelendirme, özel denetimler, müracaatlar, şikâyetler, belgelendirmenin kapsamının azaltılması, iptal edilmesi yâda askıya alınması, başvuruların ve müşterilerin kayıtları ile ilgili konular açıklanır.

Belgelendirme denetim kriterleri ile denetimin hangi kriterlere göre yapıldığının müşteriye bildirilmesi gerektiğini, belli politikalar ve prosedürler hazırlayarak denetlemelerin yapılması gerektiğini açıklar. Hizmet alan kuruluşla görüşme yapılarak görevlendirilen denetim ekibi tanıtılmalı ve ne gibi denetlemeleri hangi zamanda yapılacağı, karşılıklı planlamalarla yapılması gerektiği belirtilir. Hizmet alan kuruluşun BGYS içinde belirttiği sınırların ve kapsamın doğruluğunun ve geçerliliğinin kontrol

edilerek belgelendirme kuruluşu tarafından teyit edilmeli ve denetleme faaliyetleri bu kapsamda gerçekleştirilmelidir.

Denetim sürecinin nasıl belirlenmesi gerektiği açıklanır. Denetim süresini, BGYS'nin kapsamı; çalışan sayısı, bilgi sistemlerinin sayısı, karışıklığı gibi hususlar belirler. İlk başlangıç denetimi, teftiş denetimi yâda yeniden belgelendirme denetimine ilişkin süreler açıklanır. Çok sayıda yerde yapılan denetimlerin nasıl olacağı, denetim metodolojisi ve belgelendirme denetim raporu hazırlanırken nelere dikkat edilmesi gerektiği açıklanmaktadır. İlk belgelendirme denetimleri ve aşama safhaları, yönetim sistemlerinin birleştirilmesi, belgelendirme kararı, teftiş denetimleri ve yeniden belgelendirme konuları anlatılır. Hangi şartlar oluşursa özel denetimlerin yapılması gerektiği anlatılır. Belgelendirmenin hangi koşullarda askıya alınacağı, hangi koşullarda iptal edileceği, müracaatlar, şikâyetler ve başvuru ve müşteri kayıtlarının nasıl kayıt altına alınması gerektiğini açıklar. BGYS'nin karmaşıklığını anlayabilmek için bu standarttın Ek-A bölümünde yer alan şekli incelemeniz daha faydalı olacaktır.

Onuncu bölümde belgelendirme kuruluşunun yönetim sistemleri gereksinimleri açıklanır. ISO17024, ISO9001 ve ISO27001 standartlarının hangi maddelerine göre yönetim sisteminin hangi koşuları sağlaması gerektiği açıklanır.

Bu standarttın asıl amacı belgelendirme kuruluşlarının yeterliliklerini sağlayabilmeleri için gereken gereksinimleri açıklamaktır. Bu açıklamaları yaparken ekler bölümünde verdiği faydalı bilgilerle denetçi kuruluşlar için kontrol maddeleri sıralamaktadır. Bu bölümde yer alan kontrol maddeleri ve standarttın diğer bölümleri belgelendirme kuruluşlarının yanı sıra belge almak isteyen müşteri kuruluşlarında incelemesinde fayda vardır. Denetçilerin denetimlerde nelere dikkat edeceğini bilmek, denetçilerin kontrol çizelgelerini önceden bilmek denetleme geçirecek kuruluşlar içinde fayda sağlayacaktır.

Tablo 2: Bgys Kapsam Karmaşıklığı İçin Kriterler Tablosu

Karmaşıklık faktörü	Sınıf			Önemi
	Yüksek	Orta	Alçak	
İşçilerin sayısı + taşeron personeli	≥ 1000	≥ 200	< 200	.BGYS gerçekleştirmesinin kapsamı .Yönetim bilgi Sistemi . Üretim yönetimine ilişkin sistemler . Satış/dağıtım/ genel hizmete ilişkin sistemler . Bilgi teknolojisi/ bilgi hizmetleri ve ilgili sistemler . İnşaat/gemi yapımı/fabrika mühendisliği ilişkili sistemler
Kullanıcı sayısı	≥ 1 milyon	≥ 200.000	≥ 200.000	. Mali sistemler . Hükümetler, okullar, Medikal/ hastane sistemleri
Mekanların sayısı	≥ 5	≥ 2	1	.BGYS gerçekleştirmesinin kapsamı . Fiziki ve çevresel güvenlik (ISO/IEC 27001:2005, A.9)
Hizmetlerin sayısı	≥ 100	≥ 10	< 10	.BGYS gerçekleştirmesinin kapsamı . Fiziki ve çevresel güvenlik (A.9) .Erişim kontrolü (ISO/IEC 27001:2005, A.11) . Telekomünikas- yon ve işletme yönetimi (ISO/IEC 27001:2005, A.10)
İş istasyonlarının sayısı + PC + diz üstüler	≥ 300	≥ 50	< 50	.Erişim kontrolü (ISO/IEC 27001:2005, A.11)
Uygulama geliştirmesi ve bakım personelinin sayısı	≥ 100	≥ 20	< 20	.Bilgi sistemleri edinimi, geliştirilmesi ve bakımı (ISO/IEC 27001:2005, A.12)
Şebeke ve şifreleme teknolojisi	Harici/şifreli internet bağlantısı/sayısal imza/PKI gereksinimleri	Harici/sayısal imzasız ve standard tesislerde inşa edilmiş şifreleme kullanılarak internet bağlantısı/PKI gereksinimleri	Harici/şifresiz internet bağlantısı/sayısal imza/PKI gereksinimleri	. Telekomünikas- yon ve işletme yönetimi (ISO/IEC 27001:2005, A.10) .Erişim kontrolü (ISO/IEC 27001:2005, A.11)
Hukuki uygunluk açısından önem	Uygunsuzluk, muhtemel yargılamaya yol açar	Uygunsuzluk, iyi niyet hasarına ya da önemli mali cezaya yol açar	Uygunsuzluk, iyi niyet hasarına ya da önemsiz mali cezaya yol açar	.Mevzuat ve kılavuzlar (ISO/IEC 27001:2005, A.15)
Sektör özel riskin uygulanabilirliği (*bilgi güvenliği riskinin sektör özel sınıflarının örnekleri için A.2'ye bakılmalıdır*)	Sektör özel kanun ve yönetmelik uygulanır	Sektör özel kanun ve yönetmelik yoktur ancak önemli sektör özel risk uygulanır	Sektör özel kanun ve yönetmelik yoktur ve önemli sektör özel risk yoktur	.BGYS gerçekleştirmesinin kapsamı .Mevzuat ve kılavuzlar (ISO/IEC 27001:2005, A.15)

Kaynak: ISO27006 BGYS Denetimini ve Belgelendirmesini Yapan Kuruluşlar İçin Gereksinimler.

ÜÇÜNCÜ BÖLÜM

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ GEREKSİNİMLERİ STANDARDI

Son yirmi yılda hızla artan bilgi teknolojileri ürünleri, yaşam kalitemizi arttırırken etrafımızda oluşan tehditlerinde hızla artmasına sebep olmuştur. Mevcut güvenlik tedbirleri yaşanan teknolojik gelişmeler karşısında geçerliliğini kaybetmeye başlamıştır. Dün kullanılan tedbirler bugün için yetersiz duruma dönüşmektedir. Kuruluşlar için, teknolojilerin ve yeni tehditlerin incelenmesi, buna göre tedbirler almak öncelikle bilgi işlem personelinin sorumluluğundadır. Bunun yanında bütün kurum personeli ilgilendiren ve her bireyin sahip olması gereken bilgi güvenliği farkındalığı kavramı vardır.

Değişen teknoloji ve oluşacak yeni tehditler ne olursa olsun sahip olduğunuz bilgi güvenliği sistemi size ne yapmanız gerektiği ile ilgili bir yol haritası çizebilecek düzeyde olmalıdır. Bilgi güvenliği yönetimi her çağın gereklerine göre kendini yenileyebilir ve her ortam için yapılması gerekenleri ortaya koyar. Bugün için tehdidin adı veya metodu farklı olabilir. İsmi değişen tehditler karşısında yeni açıklıklarda doğabilir. BGYS bize zaten en başından itibaren neye nasıl davranacağımızı bildirdiği için kendini yenilemekte de gecikmeden oluşacak yeni tehditlere hızlı bir şekilde tepkiler verebilir.

Bilgi güvenliği yönetim sistemini öncelikle zincirin en zayıf halkası olan insan faktörünü kuvvetlendirmeyi amaçlar. Bilgi güvenliği eğitimleri sayesinde bütün çalışanlarda farkındalık yaratmayı amaçlar. Ardından kurum içinde herkesin sahip olduğu sorumlulukları ve rolleri açıklar. Kuruluşun sahip olduğu değerlerin ne olduğunu en ince ayrıntısına kadar ortaya çıkarır ve kayıt altına alınmasını sağlar. Kuruluşun hangi risklere açık olduğunu ve bu risklerin neler etki edeceği hakkında değerlendirmeler yapmamızı sağlar. Belirli politikalar belirlenerek; bir işin bir elden ve yazılı bir kurallar çerçevesinde yürütülmesini sağlar. Yasal mevzuata göre hazırlanmış yönetim ilkeleri, kanun dışı hareketlerde bulunmanın önünü kapamaktadır. Oluşabilecek herhangi bir sorunda geriye dönük izlemelerle sorumluların tespit edilebilmesini sağlar.

Bunun bilincinde olan kişiler için, caydırıcılık özelliği de taşımış olur. Kontrol tedbirleri sayesinde kendini devamlı dinamik tutmayı sağlar.

Bu saydığımız bütün özellikler bilgi güvenliği yönetim sistemi kurmak isteyen herkesin dikkat etmesi gereken özelliklerdir. Zamanla bu özelliklere yeni konularda eklenecektir. Şu an için bu özelliklere sahip olmayı gerektiren en kapsamlı BGYS standardı ISO27001'dir. Diğer bölümde verdiğimiz standartlar kimisi sadece kontrol tedbirlerini, kimisi süreci incelemekte ve tam olarak bütün konuları içine alamamaktadır. Zaten bu standartların hepsi birbirini tamamlayan ve eksik yanlarını örtmeye yarayan kılavuzlardır.

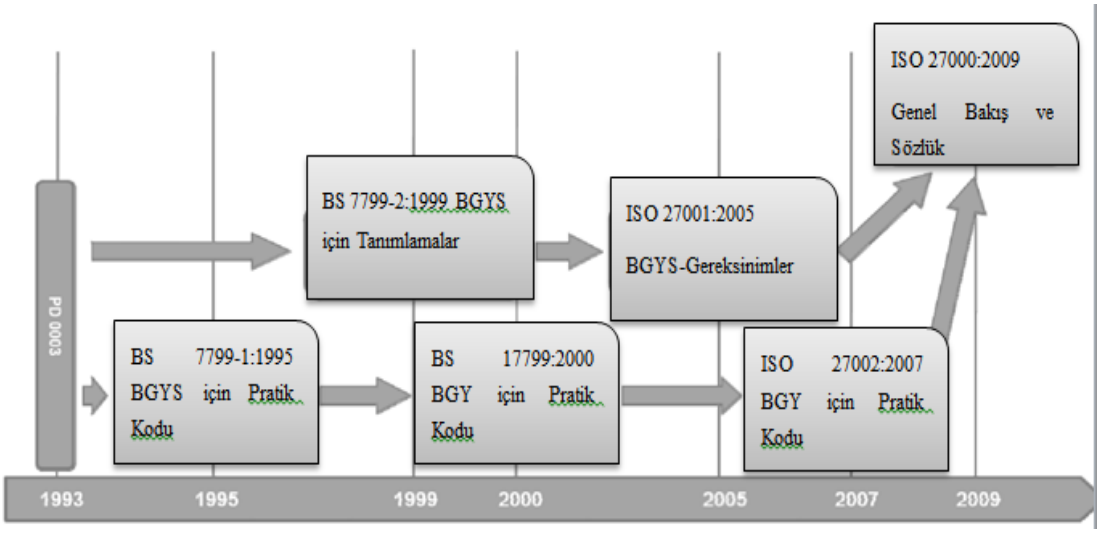
ISO27001'de kendi eksiklerini gidermek için her daim bir çalışma içindedir. Yapılan araştırmalar sonucunda bu standardın gereksinimlerini daha anlaşılabilir hale getirmek için sektör bazında da özel standartlar hazırlanmaktadır. Amaç her kuruluşun kendi sektörüyle ilgili konuların ayrıntılarla daha anlaşılabilir olmasını sağlamaktır. ISO 27001 standardı zamanın ihtiyaçlarına göre kendini yenilemeye gitmektedir.

ISO 27001 bilgi güvenliği yönetim sistemleri gereksinimi standardı zorunluluk içerir. ISO27 ailesi standartlarının hepsi bu standardın başarılmasına yardımcı olmak amacıyla hazırlanmıştır. Bu standardın şartlarını taşıdığını düşünen kuruluşlar iç denetimler ve bağımsız denetimlerle kendilerini belgelendirme kuruluşunun denetimine hazırlarlar. Belgelendirme kuruluşları yapılan denetimlerde standardın gereksinimlerini taşıdığını düşündüğü kuruluşlara sertifika hazırlayarak BGYS güvenilirliğini tasdiklemiş olur. Kuruluş üç sene boyunca bu standardın şartlarını sağladığı sürece bu belgenin sahibi olacaktır.

3.1. ISO 27001 STANDARDININ TARİHSEL GELİŞİMİ

ISO 27001 standardının geçmişine bakıldığında 1990'lı yıllarda yapılmaya başlanan çalışmaların tamamlayıcısı olarak görebiliriz. İngiliz bilim adamlarının yapmış olduğu bilgi güvenliği standartları çalışmaları bu standardın ilk temelleri olacak araştırmalardır. 1990'lı yıllarda ulusal bilgisayar merkezi tarafından PD003 bilgi güvenliği yönetimi için pratik kodlar içeren bir kılavuz yayınlanmıştır. İngiliz standartlar enstitüsü tarafından bu kılavuzdan uyarlamalar yapılarak 1995 yılında BS

7799-1 IT bilgi güvenliği için uygulama kodları standardı yayınlanmıştır. 1999 yılında da BS 7799-2 bilgi güvenliği yönetim sistemleri gereksinimleri yayınlanmıştır. 2000 yılına gelindiğinde ISO 17799 Bilgi güvenliği yönetimi uygulama kodları yayınlanmıştır.



Şekil 11: Bilgi Güvenliği Standartlarının Tarihsel Gelişimi

Kaynak: Disterer, 2013:93

2005 yılında ISO bu standartlarla ISO9001 kalite yönetimi sistemi standardını da dikkate alarak bir çalışma yapmıştır ve ISO27001 standardını ortaya koymuştur. Bu standart ailesi önemi anlaşıldıkça, yeni ek kılavuzlar yayınlayarak bilgi güvenliği konusunda en ince ayrıntıya kadar açıklamalarda bulunmaktadır. Sektörlerin özel yapısına göre ISO27001 standardının yorumlamasını yaparak tavsiye niteliğinde yardımcı standartlar geliştirmektedir.

ISO 27 ailesi standardı olarak adlandırılan bu standartlar bilgi güvenliği yönetim sistemleri kurulmasından, kontrollerine kadar bir süreci işleyen yönetim standartlarıdır. Bu süreci işlerken risk yönetimi konularını temel alarak eldeki varlıkları, onların tehdit edilme durumlarını, açıklıklarını ve etkinliklerine göre hazırlanan yazılı bir süreç yönetimi sistemidir. Önümüzdeki günlerde yeni versiyonu ile karşımıza çıkmaya hazırlanan ISO27001 standardı, zamanla kendini yenilediğini ve oluşacak yeni ihtiyaçlara göre yeniden şekillenebileceğini hepimize göstermiş olacaktır.

3.2. ISO27001 STANDARDININ YAPISI

ISO 27001 standardı yapısal anlamda incelendiğinde iki bölümden oluştuğunu gözlemlememiz mümkündür. Uygulanması zorunlu olan maddeler ana bölümü oluşturmaktadır. İkinci bölümde ise kontrol maddeleri mevcuttur. Bu kontrol maddelerinden uygulanabilirlik bölümünde yer almayan hususlar uygulama dışında kalabilir. İsteğe bağlı olarak uygulama dışı bırakmak doğru değildir. Bgys'nin yapısı itibariyle mevcut olmayan maddeler için geçerlidir.

Ana bölümü; bilgi güvenliği yönetim sisteminin yer aldığı dördüncü maddeyle başlar, yönetim sorumluluğunun yer aldığı beşinci madde, Bgys iç denetimlerinin açıklandığı altıncı bölüm, yönetim gözden geçirmesi yedinci madde ile devam eder ve Bgys iyileştirmelerinin açıklandığı sekizinci bölümle son bulur. İkinci bölümde ekler kısmını içine alır. Ekler kısmında kontrol maddeleri ve karşılaştırmalı tablolar mevcuttur.

3.2.1. ISO 27001 Standardının İlk (Ana) Bölümü

Zorunluluk gerektiren dört, beş, altı, yedi ve sekizinci maddeleri içerir. Dördüncü madde bilgi güvenliği yönetim sisteminin kurulması, yönetilmesi, genel gereksinimlerini ve dokümantasyon gereksinimlerini belirtir. Bu bölümün içinde sürecin PUKÖ modeline göre işlemesi gerektiği vurgulanır. BGYS kurma ve yönetme için gerekli olan adımları açıklar. Kapsamın belirlenmesi, politikanın tanımlanması, risk değerlendirme yaklaşımı, risklerin tanımlanması ve risklerin iyileştirmesi gerektiği belirtilir. Hangi dokümanları hazırlamamız gerektiği belirtilir. Dokümanların kontrol edilmesi gerektiği anlatılır.

Beşinci bölüm yönetimin sorumluluğunu açıklar. Yönetimin ne yapması gerektiğini, kaynakların sağlanmasını, eğitim faaliyetleri, farkındalık ve yeterlilik konularını belirtir. Altıncı bölümde BGYS iç denetimlerini, yedinci bölümde BGYS'yi yönetimin gözden geçirmesi ve sekizinci bölümde BGYS iyileştirmeleri, düzeltici ve önleyici faaliyetlerin yapılması gerektiği anlatılmaktadır.

Yukarıda hızlıca geçtiğimiz konular BGYS sürecinin tam olarak hepsini kapsamaktadır. ISO 27001 Standardı bize ekleriyle beraber otuz dört sayfada bunların

yapılması gerektiğini anlatmaktadır. Önemli olan nokta ise bu konuların nasıl yapılacağı ve nelere dikkat etmemiz gerektiğidir. Bu noktada neyi nasıl yapacağımızı bilemediğimiz zaman danışmanlık ve eğitim firmalarının desteğine ihtiyaç duymaktayız. Ülkemizde bu alanda hazırlanmış az sayıda akademik çalışma bize yetersiz kalmaktadır. Bu açığı kapatmak için hazır kullanılan otomasyon sistemleri de bir noktada yetersiz kalmaktadır. Her kuruluşun kendine has bir kurum kültürü olduğu düşünülürse herkesin hassas tarafları değişiklik göstereceği anlaşılacaktır.

Bu alanda hazırlanmış en kapsamlı çalışma TÜBİTAK bünyesinde yer alan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) tarafından hazırlanmış yardımcı kitapçıklardır. Bizde yukarıda birkaç paragrafla anlattığımız ana bölüm olan maddeleri diğer bölümlerde bahsettiğimiz kitapçıklar yardımı ile ayrıntılı bir şekilde açıklayacağız.

3.2.2. ISO 27001 Standardının İkinci (Ekler) Bölümü

Ekler bölümünde üç adet ek bulunmaktadır. Standardın ek-a bölümünde kontrol maddeleri yer almaktadır. 11 madde içinde yer alan, 133 adet kontrol aşamalarıyla karşımıza çıkmaktadır. Yeni sürümle beraber kontrol amaçları sayısı 14 olurken, kontrollerin sayısı da 114 olmuştur. Bu kontrol maddeleri BGYS kurulması sürecinin bir parçası olarak seçilmelidir. Bu bölümde yer alan kontrol maddeleri kuruluşun ihtiyaçlarını tam olarak karşılayamayabilir. Böyle bir durumda yeni kontrol maddeleriyle BGYS farklı konularda da gözden geçirilebilir.

OECD (Organisation for Economic Co-operation and Development) Ekonomik Kalkınma ve İşbirliği Örgütü prensipleri diye belirtilen OECD ağ ve bilgi sistemleri güvenliği kılavuzunun, ISO 27001 standardı ile karşılaştırılması Ek-b bölümünde yer almaktadır. Bu bölümde farkındalık, sorumluluk, tepki, risk değerlendirme, güvenlik tasarım ve gerçekleştirme, güvenlik yönetimi ve yeniden değerlendirme konuları incelenmektedir. Bu konuların OECD prensiplerine göre ve PUKÖ (planla-uygula-kontrol et-önlem al) evresine göre hangi bölümde nasıl yer aldığını karşılaştırarak, tablo halinde bize sunar.

ISO 27001 standardı ISO bünyesine baktığımızda da yönetim sistemleri içinde karşımıza çıkmaktadır. Bilgi güvenliği yönetimi için neler yapılması gerektiğini söyler,

nasıl yapılacağını ve teknik konuları açıklamaz. Diğer yönetim sistemleri ile uyum içinde çalışır. Ek-c bölümünde de ISO9001 kalite yönetimi sistemleri ile ISO14001 çevre yönetim sistemleri arasındaki benzerliklere değinilmekte ve tablo halinde karşılaştırılmaları yapılmaktadır. Yeni sürümün Ek-a bölümünde yer alan 14 kontrol amacı ve kontrol sayıları aşağıda verilmiştir.

Tablo 3: ISO 27001:2013 BGYS Gereksinimleri Standardının Ek-A Kontrol Amaçları

KONTROL AMAÇLARI	KONTROL SAYISI
A.5. GÜVENLİK POLİTİKASI	2
A.6. BİLGİ GÜVENLİĞİ ORGANİZASYONU	7
A.7. İNSAN KAYNAKLARI GÜVENLİĞİ	6
A.8. VARLIK YÖNETİMİ	10
A.9. ERİŞİM KONTROLÜ	14
A.10. KRİPTOGRAFİ	2
A.11. FİZİKSEL VE ÇEVRESEL GÜVENLİK	15
A.12. İŞLETİM GÜVENLİĞİ	14
A.13. İLETİŞİM GÜVENLİĞİ	7
A.14. BİLGİ SİSTEMLERİ EDİNİM, GELİŞTİRME VE BAKIMI	13
A.15.TEDARİKÇİ İLİŞKİLERİ	5
A.16.BİLGİ GÜVENLİĞİ İHLAL OLAY YÖNETİMİ	7
A.17. İŞ SÜREKLİLİĞİ YÖNETİMİ	4
A.18. UYUM	8

Kaynak: ISO 27001:2013

3.3. ISO27001 STANDARDININ DİĞER YÖNETİM SİSTEMLERİ STANDARDTLARIYLA İLİŞKİSİ

ISO yönetim sistemleri konusunda, her bir standardı bir birini tamamlayan farklı konulardaki ihtiyaçlara cevap verebilecek gereklilikler olarak görmektedir. Kendi resmi internet sayfasında yaptığı açıklamalarda da yönetim sistemlerini yıllara göre karşılaştırmalı olarak bizlere sunmaktadır. Bu tür karşılaştırmaların yapılarak halka duyurulmasındaki amaç kurumların bütün yönetim sistemlerine yapılarına göre ihtiyaç duyabileceklerini göstermektir. Bir standardın diğerinin yerini alamayacağını anlatarak,

mümkün olduğunca farklı standartlarla yönetim sisteminin denetlenmesini ve en ufak ayrıntıyı gözden kaçırmamayı hedeflemektedir.

Yönetim sistemleri dediğimizde ilk aklımıza gelen standart 1987 yılında ortaya çıkan ISO 9001 kalite yönetimidir. Ardından ISO14001 Çevre yönetimi sistemi, ISO 50001 Enerji yönetim sistemi, ISO 22001 Gıda güvenliği yönetim sistemi, ISO 16949 Otomotiv kalite yönetim sistemi ve ISO 13485 Tıbbi cihazlar için kalite yönetim sistemi gibi standartlar akla gelmektedir. Yönetim sistemlerinin 2011 ve 2012 yıllarına göre karşılaştırılması size daha iyi bir fikir sunması için aşağıda sunulmuştur.

Tablo 4: Yönetim Sistemlerinin 2011 ve 2012 Yıllarına Göre Dağılımı

Standart	2012 Yılı Sertifika Sayısı	2011 Yılı Sertifika Sayısı	Gelişim	Gelişim %
ISO 9001	1 101 272	1 079 647	21 625	2%
ISO 14001	285 844	261 957	23 887	9%
ISO 50001	1 981	459	1 522	332%
ISO 27001	19 577	17 355	2 222	13%
ISO 22000	23 231	19 351	3 880	20%
ISO/TS 16949	50 071	47 512	2 559	5%
ISO 13485	22 237	19 849	2 388	12%
TOPLAM	**1 504 213**	**1 446 130**	**58 083**	**4 %**

Kaynak: www.iso.org (19.04. 2014).

3.3.1. Yönetim Sistemleri Standartları İle Uyum Çalışmaları

Yönetim sistemlerinin birbirleri arasında oluşacak anlaşmazlıkları çözmek adına uzmanlar tarafından çalışmalar başlatılmıştır. Bir Yönetim sistemi standardında geçen bir kavram diğerinde farklı anlamlar taşımakta veya tam karşılığını bulamamaktadır. Bu kavram karmaşasının giderilmesi için annex sl adında bir yapı geliştirilmiştir. Bu yapı her sistemin iskelet yapısını oluşturacak şekilde hazırlanmıştır. Standardın ihtiyacına göre bölümlerin içeriği farklılık göstererek özel oluşturulabilir. Ekler bölümü farklılıklar içerebilir. Gerek duyulursa fazladan bölümler eklenebilir.

İlk olarak 2012 yılında ISO22301 İş sürekliliği yönetim sistemleri gereksinimleri standardı ile karşımıza çıkan bu yapı, bundan sonra hazırlanacak bütün yönetim sistemi standartları için söz konusu olacaktır. Bu sayede yönetim standartlarının tek bir kuruluş düzeni ve kapsam maddeleriyle uyumu sağlanmış olacaktır. Bu sayede yapılan bir çalışma diğer standartların hazırlanmasında rehber niteliğinde olacak ve sistemin kurulmasını hızlandıracaktır. ISO 27001 standardının güncellenen yeni versiyonunda bu annex sl yapısının kullanılacağı bilinmektedir. Annex sl yapısı IRCA (International Register Of Certificated Auditors)' nın resmi sayfasında yayınlanan broşürde anlatıldığı gibi aşağıda maddeler halinde sunulmuştur:

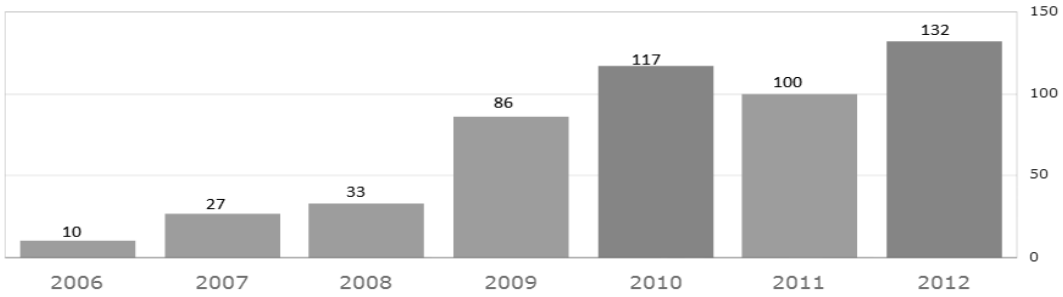
0. Introduction - Giriş
1. Scope - Kapsam
2. Normativereferences - Atıf yapılan standartlar ve/veya dokümanlar
3. Termsanddefinitions - Terimler ve tarifleri
4. Context of theorganization - Kurum Bağlamı / Kuruluşun içeriği
5. Leadership- Liderlik
6. Planning - Planlama
7. Support- Destek
8. Operation- Operasyon / işletim
9. Performanceevaluation- Performans değerlendirme
10. Improvement- İyileştirme

3.4. ISO27001 STANDARDININ ÜLKEMİZDE VE DÜNYADAKİ YERİ

ISO 27001Standardıile ilgili araştırmamızda, belge sahibi kurumların kimler olduğunu bulmaya çalışırken farklı sonuçlarla karşılaştık. Yapılan araştırmaları incelediğimizde genellikle belirli internet sitelerinde yer alan bilgilerin kullanıldığını görmekteyiz. Fakat bu tür siteler kuruluş sahibi veya belgelendirme kuruluşlarının kayıt yaptırması sonucunda bilgi sahibi olmaktadırlar. Kaynak olması açısından faydalı fakat

tam olarak kesin sonuçlar verememesi açısından yetersizdir. Sayılarla ilgili kesin bilgiler ISO'nun resmi internet sitesinden ulaşabilirsiniz.

Tablo 5: Ülkemizdeki ISO27001 Standardına Sahip Kuruluşların Yıllara Göre Dağılımı



Kaynak: www.iso.org (15.02.2014).

Bunun yanında bazı yayınlarda, ISO27001 belgesi sahibi kuruluşların isimlerine ulaşmanın çok zor olduğu anlatılmaktadır. Belge sahibi kuruluşların hacker (bilgisayar korsanı) saldırılarından korktukları için kendi isimlerinin duyulmasını istemediklerini anlatmaktadırlar. Biz bu tür iddiaların doğru olmadığını yaptığımız araştırmalarda açık bir şekilde gördük. Tüm belge sahibi kuruluşlara yönelik böyle bir ifade kullanmak yanlış olacaktır. Belge sahibi kurumlar; aldıkları sertifikalarla kendi isimlerinin duyulması için basın yayın organlarına mülakatlar vermekte, kendi internet sayfalarında aldıkları belgeyi yayınlamakta ve her fırsatta bu belgenin kurumlarına kattığı ayrıcalıkları anlatmaktadırlar. Diğer bir yandan belge sahibi kuruluşların sertifika alım süreci hakkında bilgi vermekten kaçınmaları da bizim tespitlerimiz arasında yer almaktadır. ISO27001 standardına sahip dünyadaki en fazla on ülkenin isimlerini, ülkemizin sayısal verilerini daha iyi anlayabilmeniz için aşağıdaki tabloda sizlere sunuyoruz.

Tablo 6: Dünyadaki En Fazla ISO27001 Standardına Sahip Olan Ülkeler

ISO/IEC 27001 SERTİFİKASINA SAHİP OLAN İLK 10 ÜLKE		
1	Japonya	7199
2	Birleşik Krallık	1701
3	Hindistan	1600
4	Çin	1490
5	Romanya	866
6	Tayland	855
7	İspanya	805
8	İtalya	495
9	Almanya	488
10	Amerika Birleşik Devletleri	415

Kaynak: www.iso.org (15.02.2014).

3.5. ISO27001 BGYS KURULUM ÇALIŞMALARI

Bu sertifikaya sahip olmak isteyen kuruluşun yapması gereken, ilk olarak üst yönetim seviyesinde bir karar almaktır. Ardından da ISO27001 standardını satın alarak gereksinimlerin kurumu için uygun olup olmadığını incelemelidir. Kurum eğer önceden başka bir yönetim sistemine sahip ise işi daha da kolaylaşacaktır. Diğer yönetim sisteminin gereksinim duyduğu dokümanlar bu standartta karşımıza çıkacaktır. Daha da önemlisi önceden yönetim sistemi kurulumu yapmış bir kurum mevcut tecrübesi ile birçok adımı kolaylıkla geçecektir. Standarttı yorumlamasını bilen personeller kuruma hız kazandıracaktır.

Sertifika sahibi olmak isteyen kuruluşlar standartları ellerine aldıklarında, kendilerinin ne yapması gerektiğini öğreneceklerdir. Fakat nasıl yapacakları konusunda kendilerine yardımcı olacak bir bölüm göremeyeceklerdir. Bu esnada kaynak ihtiyacı ortaya çıkacaktır. Ülkemizde BGYS kurulumu ile ilgili yeterli kaynak olmaması bizleri farklı alanlara itecektir. Ülkemizde BGYS kurulumu ile ilgili akademik anlamda en ayrıntılı çalışmalar TÜBİTAK bünyesinde hizmet veren kurumlarda yapılmaktadır. Devlet desteği ile UEKAE'nin yayınladığı yardımcı yayınlar kendi başına sistem kurmak isteyenler için en önemli kaynaktır. Bunun yanında akademik çevrelerde

yapılan araştırmaların sayısı giderek artmaktadır. Yapılan araştırmaların bazılarında da otomasyon sistemi kurarak, BGYS kurulum sürecini gerçekleştirmeyi anlatmaktadırlar.

Yurt dışı kaynaklarda incelemeler yaptığımızda bu alanda yapılmış daha fazla ve ticari amaçlar güden yazılı çalışmaların olduğunu görmekteyiz. Bu tür kaynak kitapların değeri ortalama iki bin dolar seviyesinden satılmaktadır. Aynı zamanda yurt dışı piyasalarında belirli programlarla temel girdileri yaparak BGYS kurulumunu yapmaya yarayan programlar (toolkit) kullanılmaktadır. Bunların değeri de yaklaşık olarak bin dolar civarındadır.

Ülkemizde BGYS kurulumun için kaynakların yetersiz olması ve akademik kurumlarında bu türde kurumlara bir desteği olmadığı için bu ihtiyacı kapamak için devreye danışmanlık kuruluşları girmektedir. Ulusal bilgi sistemleri güvenlik programı kapsamında az sayıda kamu kurumuna BGYS ile ilgili destek verilmektedir. Ülkemizde alınan ISO27001 sertifikalarının çoğu danışmanlık ve eğitim firmaları ile yürütülen ortak çalışmalar sonucunda alınmaktadır. Bu açığın ileride eğitim kurumlarımız tarafından doldurulması gerekmektedir. Bunun yanında sertifika sahibi olan kurumlara danışılarak veya personelinize BGYS konusunda eğitimler (iç tetkik, baş denetçi gibi) aldırarak kendi imkânlarınızla da bu süreci gerçekleştirebilirsiniz.

3.5.1. ISO27001 BGYS Belgelendirme

BGYS kurulum süreci yukarıda belirtilen kaynaklardan yararlanılarak tamamlandıktan sonra sistem uygulanmaya başlanır. Kurum içinde gelecek tepkiler ve oluşacak aksaklıklar gözlenir. Yaklaşık bir ay kadar sistemin çalışması gözlemlenir ve ardından kurum içi bir iç tetkik gerçekleştirilir. İç tetkik raporlarına göre yönetim gözden geçirilir ve karara bağlanır. Bu aşamadan sonra artık belgelendirme kuruluşlarına başvuru aşamasına gelinir.

Belgelendirme kuruluşu seçerken, dikkat etmemiz gereken kuruluşun akredite edilmiş olduğundan emin olmamız gerekir. Akreditasyon işlemleri için yetkili olan kurum IAF (Uluslararası akreditasyon formu)'dur. Ülkemizde bu yetki TÜRKAK (Türk Akreditasyon Kurumu) tarafından yürütülmektedir. TÜRKAK ülkemiz dışında yedi ülkede daha faaliyetlerini sürdürmektedir. TÜRKAK'ın resmi internet sitesine

baktığımızda hangi kuruluşların, hangi sertifika belgelendirme yetkisine sahip olduklarını ve ne zamana kadar yetkilerinin devam ettiğini görebilirsiniz. Ülkemizde TÜRKAK tarafından akredite olan, ISO27001 sertifikası vermeye yetkili sekiz kuruluş bulunmaktadır. Bu kuruluşlarla yapılan görüşmeler sonucunda bize en uygun teklifi veren kuruluşla anlaşmaya varılır.

Belgelendirme kuruluşu ilk olarak sistemin genel yapısını kontrol eder. Eğer genel konularda bir aksaklık yok ise ikinci aşama denetimlerine ayrıntılı bir şekilde başlar. İlk aşama denetimlerinde öncelikle ISO27001 standardının 4.3.1 maddesinde yer alan hususlar kontrol edilir. Yapılan ilk safha denetimlerinin sonucunda raporlar hazırlanır. Eksik görülen hususlar belirtilir ve eksik bir bölüm yoksa yeterli görülür ve ikinci safha denetimlerine geçilir.

İkinci safha denetimlerinde tüm sistem en ince ayrıntısına kadar gözden geçirilir. Belgelendirme kuruluşu, BGYS'nin hukuki ve düzenleyici uygunluğu sağlayabilecek düzeyde olmasını da sağlar. Başka yönetim sistemleri denetimi de aynı anda belgelendirme kuruluşu tarafından yapılabilir. Denetimi yapan ekip, belgelendirmeyi yapacak olan ekibe raporlarını sunar. Bu ekiplerin birbirinden farklı olması gereklidir.

Belge verilmesine uygun görülen kuruluşlara belgelendirme yapılır ve bu sertifikanın üç sene geçerliliği vardır. Her yıl kontrol denetimleri yapılır. Sertifika süresi dolunca yeniden belge almak için denetim yapılır. Sertifika süresi içinde her hangi bir şikâyet söz konusu olduğunda belgelendirme kuruluşu özel denetimler yapabilir. BGYS sahibi kuruluş, sertifika süresi boyunca belgelendirme kuruluşuna karşı sorumludur. Belgelendirme kuruluşunun istediği belge ve bilgileri temin etmekle yükümlüdür. Eğer bir aksaklık tespit ederse, belgenin iptalini sağlamakta yetkilerinin içindedir. Belge verdiği kuruluşun kalitesini tüm dünyaya karşı onaylamış olur. Her hangi bir yanlışlık yapılması akredite olmuş olan belgelendirme kuruluşunun itibarının zedelenmesine ve farklı yaptırımlarla karşı karşıya gelmesine sebep olabilir.

Yapılan denetimlerde ISO 27006 Bilgi güvenliği yönetim sistemlerinin denetimini ve belgelendirmesini yapan kuruluşlar için gereksinimler standarttı kullanıldığı için önceden bu standarttan da yararlanmakta fayda vardır. Bu standardın ekler kısmında hangi büyüklükte kuruluşta ne kadar süreyle, kaç denetçi tarafından bu tür işlemlerin yapılabileceği ile bilgilerde sunulmaktadır. Bu standardın ek-d bölümünde

yer alan kontrol tabloları da, ISO27001 standardının ek-a kısmında yer alan kontrol maddelerinin ayrıntılı olarak açıklanmış halidir.

Tablo 7: Kontrol Maddelerinin Denetim Örnekleri

ISO/IEC 27001:2005, Ek A'daki kontroller	Kurumsal kontrol	Teknik kontrol	Sistem testi	Gözle muayene	Denetim inceleme kılavuzu
A.10.8.3 Geçiş halindeki fiziki ortamlar	X	X	Mümkün		Fiziki koruma ya da şifreleme
A.10.8.4 Elektronik mesajlaşma	X	X	Mümkün		Örnek mesajların politikaya/prosedürlere uygunluğu teyit edilir
A.10.8.5 Ticari bilgi sistemleri	X				
A.10.9 Elektronik ticaret hizmetleri					
A.10.9.1 Elektronik ticaret	X	X	Mümkün		
A.10.9.2 Çevrim içi işlemler	X	X	Önerilen		Kontrol: bütünlük, erişim yetkisi
A.10.9.3 Kamunun erişimine açık bilgiler	X	X	Mümkün		
A.10.10 İzleme					
A.10.10.1 Denetim kütüğü	X	X	Mümkün		Çevrim içi ya da kağıda basılı
A.10.10.2 İzleme sistem kullanımı	X	X	Mümkün		
A.10.10.3 Kütük bilgisinin korunması	X	X	Mümkün		
A.10.10.4 Yönetici ve operatör kayıtları	X	X	Mümkün		
A.10.10.5 Arıza kaydı	X				
A.10.10.6 Saatin eş zamanlaması		X	Mümkün		
A.11 Erişim kontrolü					
A.11.1 Erişim kontrolü için iş gerekliliği					
A.11.1.1 Erişim kontrol politikası	X				
A.11.2 Kullanıcı erişim yönetimi					
A.11.2.1 Kullanıcı tescili	X				Tüm sistemlere her türlü erişim hakkı için yetkilere göre örnek işçiler/taşeronlar
A.11.2.2 İmtiyaz yönetimi	X	X	Mümkün		Personelin içerde yer değiştirmesi
A.11.2.3 Kullanıcı şifre yönetimi	X				
A.11.2.4 Kullanıcı erişim haklarının gözden geçirilmesi	X				
A.11.3 Kullanıcı sorumlulukları					
A.11.3.1 Şifre kullanımı	X				Kullanıcılara ilişkin kılavuz/politika doğrulanır
A.11.3.2 Refakatsız kullanıcı cihazı	X				Kullanıcılara ilişkin kılavuz/politika doğrulanır

Kaynak: ISO27006, 2010:33.

3.6. ISO 27001 STANDARDINDAKİ YENİLİKLER

ISO 27001 standardının şuanda kullandığımız versiyonu 2005 yılında yayınlanmıştır. 2005 yılından itibaren kullanılmakta olan bu standart zaman içinde yetersiz kaldığı ve yenilenmesi gerektiği hissedilmiştir. Diğer yönetim sistemleriyle olan etkileşimlerinde de yaşanan sorunlar farklı bir ihtiyacı doğurmuştur. Güncel tehditler ve uygulamada yaşanan zorluklar göz önüne alındığında, bu standardın kendini dinamik tutabilmesi için güncellenmesi gerektiği kararına varılmıştır.

Yapılan araştırmalar sonucunda oluşturulan taslak metinler halka arz edilerek gelecek teklif ve eleştiriler değerlendirilmiştir. Bu çalışmalar sonucunda 2013 yılının Eylül ayında ISO tarafından ISO27001 standardının yeni versiyonu İngilizce metin olarak yayınlanmıştır. Ülkemizde bu standardın 2014 yılında kabul edilip, yıl sonuna kadar da çevirisinin yapılıp Türkçe metin olarak yayınlanması beklenmektedir. Şu anda kullanılan standart 2015 yılının eylül ayına kadar geçerliliği devam etmektedir. Yeni versiyonun yayınlanmasından sonra kullanıma geçilmesi beklenmektedir. Bu konuda alt yapı çalışmaları tamamlandıktan sonra kararı verecek olan ve bizlere gerçek bilgiyi verecek olan kurum TÜRKAK'tır. Bu alanda danışmanlık veren kuruluşlarda yeniliklerle ilgili kendi iç eğitimlerini planlamakta ve değişen şartlara göre personelini bilgilendirmeye çalışmaktadırlar.

Bilgi teknolojilerinde ortaya çıkan yenlikler, kurumların işleyiş yapılarını ve BGYS'ni de değişime zorlamaktadır. 2005 yılında bu standart hazırlanırken çok fazla etkin olmayan veya hiç hayatta olmayan projeler şuanda kullanımda yeni bilgi güvenliği gereksinimleri doğurmaktadırlar. Bu konuda araştırma yapan birçok şirketin anket sonuçları da bu ihtiyaçları doğrular niteliktedir.

Ernst & Young'ın bilgi güvenliği anketi sonuçlarına göre şirketlerin sosyal medya, bulut bilişim, sanal suçlar ve süregelen tehditlerin oluşturduğu boşluğu kapatmak için bilgi teknolojilerine yaklaşımlarını değiştirmeleri gerekiyor. Raporda bu yaklaşımı değiştirirken şirketlerin aşağıdaki dört ana adımı yerine getirmeleri gerektiğine yer veriliyor:

1- Bilgi güvenliği stratejilerini iş stratejileri ile entegre etmek

2- Yeni teknolojiler hakkında detaylı bilgiler edinerek eskiden geçerli olan önyargıları kırmak

3- Bilgi güvenliğini sağlayan fonksiyonların sürdürülebilir ve etkin bir şekilde değiştirilmesine müsait bir ortam yaratmak

4- Yeni teknolojiler söz konusu olduğunda yeni fırsatlara ve risklere açık olarak bunların getiri ya da zararlarını şirket kullanımına göre düzenlemek.

3.6.1. Genel Yapıdaki Değişiklikler

Yenilenen standarda baktığımızda ilk gözümüze çarpan konu annex sl yapısı olmuştur. Bu yapı diğer yönetim sistemlerinde de uygulanmaya başlamış olan ve bundan sonra üretilecek olan yönetim sistemlerinin hepsinde olması planlanan yapıdır. Bu yapıyla ilgili temel bilgileri yukarıdaki bölümlerde vermiştik. Bu yapı sayesinde kuruluşta var olan bir yönetim sistemi, diğer kurulması planlanan yönetim sistemlerine rehberlik edecektir. Bu sayede planlama, dokümantasyon gibi konular mükerrer çalışmalarla angarya olmaktan çıkacaktır. Farklı yönetim sistemlerinin birbirleriyle olan anlam kargaşasının da önüne geçilmiş olur. Kullanılan ortak terimlerle bir standartta yer alan ifade bütün standartlarda aynı anlama karşılık gelmektedir. Bu yapı standardın özel ihtiyaçlarına göre eklemeler yapılmasına izin vermektedir.

Yeni standartla beraber gereksiz görülen bazı bölümlerde standarttan çıkarılmıştır. Ekler kısmında yer alan OECD Bilgi sistemleri ve ağların güvenliği için hazırlanmış prensiplerin kılavuzunu karşılaştırma bölümü (ek-b) ve diğer yönetim sistemleri standartları ile karşılaştırılması bölümü (ek-c) çıkarılmıştır. Yeni standartla beraber üçüncü maddede yer alan terimler ve tarifler kısmı kaldırılmıştır. Bu maddede ISO27000 standardına atıfta bulunarak bu gerekli terimleri orada bulabileceğimiz belirtilmektedir. Önleyici faaliyetler bölümü ve iyileştirici faaliyetlerde zorunlu olan dokümantasyon konusu iptal edilmiştir.

Ernst & Young tarafından gerçekleştirilen Küresel Bilgi Güvenliği Anketi sonuçlarına göre; yazışmaların dijital ortama taşınması, cep telefonu kullanımı, sosyal medyaya erişim ve bulut bilişim, şirket bilgilerinin şirket dışına sızmasını kolaylaştırabilecek ortam sağlıyor. Şirketlerin bilgi güvenliği konusundaki boşlukların

kapanması için tek yolun bilgi güvenliği altyapılarında köklü bir dönüşüme gitmek olarak gözüküyor. Bring your own device (BYOD) kendi cihazını getir akımı ile beraber bilgi güvenliği standartlarında bir ihtiyaç daha belirdi ve yeni sürümün ek kontrol kısmında yer alan 6.2.1. bölümünde bu konuyla ilgili politikalar oluşturulması gerektiği vurgulanmıştır. Bu akımla beraber kuruluş dışında da çalışma imkânlarının önü açılmaya başlayacaktır. Son günlerde ortaya çıkan bu akım hakkında CISCO tarafından dünya çapında küresel BYOD araştırması sonucunda şu sonuçlar ortaya çıkmıştır.

Sadece BYOD değil tüm mobilite girişimleri için önemli olan bazı alanlarda çoğu şirket hazırlıklı değildir. BYOD akımının çalışanlar tarafından genel olarak tercih edilmesinin ana sebebi, çalışanların işlerini nasıl, nerede, ne zaman ve hangi cihazla gerçekleştirecekleri üzerinde daha fazla kontrole sahip olmak istemeleridir. Ayrıca gün (veya gece) boyunca kişisel aktiviteleri ile iş aktiviteleri arasında geçiş yapabilmek istemektedirler. İşyerinde özel işleri yürütmek ve iş dışı saatlerde çalışmak, bilgi işlerini farklı kılan bir özellik haline gelmiştir. Bu eğilime güç veren şey ise mobilite ve özellikle de BYOD'dır. Çünkü çalışanlar özel cihazlarını her zaman yanlarında taşıyarak arkadaşlar, aile üyeleri ve meslektaşlarının her an kendilerine ulaşabilmelerini mümkün kılmaktadır. Ayrıca anlık mesajlaşma gibi mobil uygulamalar çalışanlara anında ulaşmayı ve iletişim kurabilmeyi sağlamaktadır. Kısacası, günümüzün bilgi çalışanı fiziksel ofise nadiren girse bile asla gerçekten "ofis dışında" olmaz (Cisco, 2012: 8).

Varlık sahibi kavramı yerine risk sahibi kavramı kullanılmaya başlanmıştır. Risk sahibi, risk işleme planını ve artık risklerin onayından sorumlu olacaktır. Risk işleme faaliyetinin yazılı hale getirilmesi zorunluluğu da ortadan kalkmıştır. Belgeler ve kayıtlar ifadeleri, dokümante edilmiş bilgi kavramı olarak değiştirilmiştir. Yeni standardın 6.1.3. bölümünde yer alan not kısmında risk yönetimi ile ilgili konuların ISO31000 risk yönetimi standartlarından yararlanılarak hazırlanması gerektiğini açıklamaktadır. 4.2. maddesiyle beraber ilgili tarafların ihtiyaçları ve beklentileri standarda eklenmiş oldu. Beşinci madde ile eklenen liderlik konusu üst yönetime daha fazla sorumluluk yüklemekte ve diğer gereksinimlerin sağlanmasında liderlik kavramının etkin olduğu vurgulanmaktadır. İletişim konusunu açıklayan yedinci madde

ile kimin, ne zaman, kiminle, ne hakkında iletişime geçmesi gerektiği vurgulanmaktadır.

Ek-a kısmında yer alan kontrol amaçları on birden on dörde yükselmiştir. Kontrol amaçlarının artmasına karşılık, kontrol sayıları yüz otuz üçten, yüz on dörde düşmüştür. Aşağıdaki maddeler yeni standardın ek-a kontrol maddelerine eklenen yeni on bir kontrol maddesidir.

- A.6.1.5 Proje yönetiminde bilgi güvenliği
- A.12.6.2 Yazılım yükleme kısıtları
- A.14.2.1 Güvenli yazılım geliştirme politikası
- A.14.2.5 Güvenli sistem mühendisliği prensipleri
- A.14.2.6 Güvenli yazılım geliştirme ortamı
- A.14.2.8 Sistem güvenliği testi
- A.15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası
- A.15.1.3 Bilgi iletişim teknolojisi tedarik zinciri
- A.16.1.4 Bilgi iletişim teknolojisi tedarik zinciri
- A.16.1.5 Bilgi güvenliği olaylarının cevaplanması
- A.17.2.1 Bilgi işleme olanaklarının erişilebilirliği

3.7. BGYS STANDARDLARININ YASAL MEVZUATLARLA OLAN UYUMU

Bilgi güvenliği yönetim sistemlerini belirli bir standardın gereksinimlerine göre hazırlamak, yönetim kademesini ileride doğabilecek hukuki sorumluluklara karşıda koruma altına almaktadır. BGYS kurulmasıyla farkında olmadan, istemesek bile hukuki birçok konuda tedbirlerde almış olmaktayız. BGYS kurulumu esnasında verilecek olan temel bilgi güvenliği eğitimleri sayesinde personel bilinçlenerek, yanlış veya eksik bildiği, yapması sonucunda hukuksal sorumluluklar doğabilecek hatalarının farkına varabilmektedirler. Erişim politikaları ve kullanıcılar için hazırlanan politikalar çalışanlar ve ilgili taraflar için uyarıcı bir özellik taşımaktadır. Hazırlanan politikaların personele tebliğ edilmesi, ileride ortaya çıkabilecek her hangi bir olumsuzlukta yönetim kademesinin elini güçlendirici nitelikte belgelerdir. Tutulan kayıtlar, kullanıcıların

sistemde olma bilgileri, erişimin yapıldığı cihaz bilgileri gibi bilgiler herhangi bir ihlal olayında delil niteliği taşımaktadır.

TCK hükümlerine göre; 243/1 maddesi "Bilişim sistemine girme ve kalmaya devam etme" suçunu konu almaktadır. Bu maddeye göre sisteme izinsiz girme, sistem içinde değişiklik yapma sonucunda cezai yaptırımlar uygulanacaktır. Sistem kelimesi aynı zamanda sosyal ağlar üzerinde yer alan kullanıcı hesaplarını da kapsadığı yönünde yorumlar vardır. TCK 244/1 "Bilişim sistemini engelleme veya bozma" aynı konuları kapsamaktadır. TCK 244/2 "Haberleşmenin gizliliğini ihlal ve haberleşmenin gizliliğini ifşa etme" suçları da bu kapsamda birbirleriyle bağlantılı suçlardır. Bu suçların kamu kurumlarına karşı yapılmasına göre cezai yaptırımda artırıma gidilmektedir.

5237 sayılı Türk Ceza Kanunu'nun Bilişim Alanındaki Suçları ve cezai yaptırımlarını içeren maddeleri, 5651 Sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ve 5809 sayılı elektronik haberleşme kanunu elektronik haberleşme sektöründe düzenleme ve denetleme getiren bir kanundur. Bu kanun maddelerinin yanı sıra birçok kanunda irdelendiğinde, BGYS standartları sayesinde özel bir çaba harcamadan birçok yasal mevzuat yerine getirilmiş olmaktadır. Örneğin ISO27001 standardına göre yazılım yükleme, geliştirme ve güncelleme gibi konular sorumlu personel tarafından, yasal mevzuata uygun bir şekilde yapılması gerekir. Bu sayede personelin bilmeden Fikri mülkiyet haklarını (IPR) ihlal etmesinin ve korsan ürün kullanmanın önüne geçilmektedir. Yapılan bir araştırmada Tolga MATARACIOĞLU 657 sayılı devlet memurları kanunu ile ISO27001 standardının gereksinimlerinin kıyaslamalı tablosunu şu şekilde çıkarmıştır.

Tablo 8: ISO/IEC 27001 Standardıyla Uyumlu Olan Ve 657 Sayılı Devlet Memurları Kanunu'nda Yer Alan Maddeler

No.	657 Sayılı Devlet Memurları Kanun Maddesi ve Açıklaması	ISO/IEC 27001 Standardı Karşılığı
1	**Madde 3 A Sınıflandırma:** Devlet kamu hizmetleri görevlerini ve bu görevlerde çalışan Devlet memurlarını görevlerin gerektirdiği niteliklere ve mesleklere göre sınıflara ayırmaktır.	**A.6.1.3** Bilgi güvenliği sorumluluklarının atanması: Tüm bilgi güvenliği sorumlulukları açıkça tanımlanmalıdır. Kurumda bilgi güvenliği rolleri tanımlanmalı ve bu rollere personel tahsis edilmelidir. **A.8.1.1** Roller ve sorumluluklar: Çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların güvenlik rolleri ve sorumlulukları kuruluşun bilgi güvenliği politikasına uygun olarak tanımlanmalı ve dokümante edilmelidir.
2	**Madde 7:** Devlet memurları her durumda Devletin menfaatlerini korumak mecburiyetindedirler. Türkiye Cumhuriyeti Anayasasına ve kanunlarına aykırı olan, memleketin bağımsızlığını ve bütünlüğünü bozan Türkiye Cumhuriyetinin güvenliğini tehlikeye düşüren herhangi bir faaliyette bulunamazlar.	**A.6.1.5** Gizlilik anlaşmaları: Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da açıklamama anlaşmalarının gereksinimleri tanımlanmalı ve düzenli olarak gözden geçirilmelidir. **A.15.1.4** Verinin korunması ve kişisel bilginin mahremiyeti: Uygun yasa, düzenlemeler ve varsa anlaşma maddelerinde belirtildiği gibi veri koruma ve gizlilik sağlanmalıdır.
3	**Madde 10:** Devlet memurları amiri oldukları kuruluş ve hizmet birimlerinde kanun, tüzük ve yönetmeliklerle belirlenen görevleri zamanında ve eksiksiz olarak yapmaktan ve yaptırmaktan, maiyetindeki memurlarını yetiştirmekten, hal ve hareketlerini takip ve kontrol etmekten görevli sorumludurlar.	**5.2.2** Eğitim, farkında olma ve yeterlilik: Kuruluş, BGYS'de tanımlanan sorumluluklara atanan tüm personelin istenen görevleri gerçekleştirmeye yeterli olduğunu, aşağıda belirtilenlerle sağlamalıdır: a) BGYS'yi etkileyecek işler gerçekleştiren personel için gerekli yeterlilikleri belirleme, b) Eğitim sağlama veya bu ihtiyaçları karşılamak için diğer eylemleri (örneğin, yeterli uzmanlığa sahip personel istihdam etme) gerçekleştirme, c) Alınan önlemlerin etkinliğini değerlendirme, d) Eğitim, öğretim, beceriler, deneyim ve niteliklere ilişkin kayıtlar tutma (Madde 4.3.3). Kuruluş aynı zamanda, ilgili tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin ve BGYS amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olmasını sağlamalıdır.
4	**Madde 12:** Devlet memurları, görevlerini dikkat ve itina ile yerine getirmek ve kendilerine teslim edilen Devlet malını korumak ve her an hizmete hazır halde bulundurmak için gerekli tedbirleri almak zorundadırlar.	**A.9.2** Ekipman Güvenliği: Varlıkların kaybını, hasarını, çalınmasını ya da tehlikeye girmesini ve kuruluşun faaliyetlerinin kesintiye uğramasını engellemek.
5	**Madde 16:** Devlet memurları görevleri ile ilgili resmi belge araç ve gereçleri, yetki verilen mahaller dışına çıkaramazlar, hususi işlerinde kullanamazlar. Devlet memurları görevleri icabı kendilerine teslim edilen resmi belge, araç ve gereçleri görevleri sona erdiği zaman iade etmek zorundadırlar. Bu zorunluluk memurun mirasçılarına da şamildir.	**A.9.2.7** Varlıkların kurumdan çıkarılması: Ön yetkilendirme olmaksızın teçhizat, bilgi veya yazılım bulunduğu yerden çıkarılmamalıdır. **A.8.3.2** Varlıkların iade edilmesi: Tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcılar, çalışmaları, sözleşmeleri veya anlaşmalarının sonlandırılmasıyla birlikte kendilerinde bulunan kuruluşun tüm varlıklarını iade etmelidirler.
6	**Madde 31:** Devlet memurlarının kamu hizmetleri ile ilgili gizli bilgileri görevlerinden ayrılmış bile olsalar, yetkili bakanın yazılı izni olmadıkça açıklamaları yasaktır.	**A.6.1.5** Gizlilik anlaşmaları: Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da açıklamama anlaşmalarının gereksinimleri tanımlanmalı ve düzenli olarak gözden geçirilmelidir. **A.15.1.4** Verinin korunması ve kişisel bilginin mahremiyeti: Uygun yasa, düzenlemeler ve varsa anlaşma maddelerinde belirtildiği gibi veri koruma ve gizlilik sağlanmalıdır.

7	**Madde 125 (bir kısmı ele alınmıştır):** Devlet memurlarına verilecek disiplin cezaları ile her bir disiplin cezasını gerektiren fiil ve haller şunlardır: B - Kınama: Memura, görevinde ve davranışlarında kusurlu olduğunun yazı ile bildirilmesidir. Kınama cezasını gerektiren fiil ve haller şunlardır: a) Verilen emir ve görevlerin tam ve zamanında yapılmasında, görev mahallinde kurumlarca belirlenen usul ve esasların yerine getirilmesinde, görevle ilgili resmi belge, araç ve gereçlerin korunması, kullanılması ve bakımından kusurlu davranmak e) Devlete ait resmi araç, gereç ve benzeri eşyayı özel işlerinde kullanmak f) Devlete ait resmi belge, araç, gereç ve benzeri eşyayı kaybetmek D - Kademe ilerlemesinin durdurulması: Fiilin ağırlık derecesine göre memurun, bulunduğu kademede ilerlemesinin 1 - 3 yıl durdurulmasıdır. Kademe ilerlemesinin durdurulması cezasını gerektiren fiil ve haller şunlardır: k) Açıklanması yasaklanan bilgileri açıklamak	**A.7.1.3** Varlıkların kabul edilebilir bir biçimde kullanılması: Bilgi işleme olanakları ile ilişkili bilgi ve varlıkların kabul edilebilir kullanım kuralları tanımlanmalı, dokümante edilmeli ve gerçekleştirilmelidir. **A.8.2.3** Disiplin süreci: Bir güvenlik kırılmasına yol açan çalışanlar için resmi bir disiplin prosesi olmalıdır. **A.15.1.4** Verinin korunması ve kişisel bilginin mahremiyeti: Uygun yasa, düzenlemeler ve varsa anlaşma maddelerinde belirtildiği gibi veri koruma ve gizlilik sağlanmalıdır.

Kaynak: www.bilgiguvenligi.gov.tr (13.03.2014).

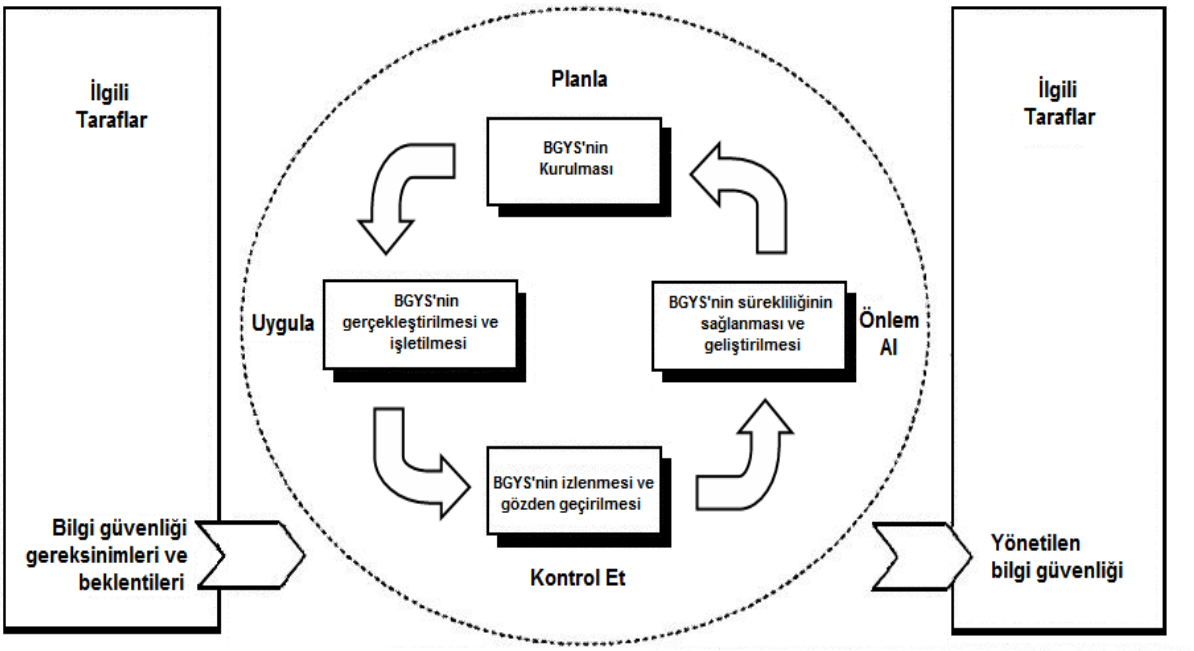
DÖRDÜNCÜ BÖLÜM
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ KURULUMU VE YÖNETİMİ

ISO 27001 Standardının gereksinimlerine uygun bir BGYS kurmak isteyen kuruluş öncelikle standardın kendi kurumuna uygun olup olmadığını değerlendirmelidir. Bazı kurumlar yapısı gereği bu tür gereksinimleri sağlayamayabilir yâda bu standardın gereksinimleri kendisine aşırı zorlayıcı gelebilir. BGYS kurulumunda bu standardın minimum olması gereken tedbirleri şart koştuğunu bilmenizde fayda vardır. BGYS kurulumuna karar vermek kurum için stratejik bir karardır. En üst yönetimden, en alt kademe çalışanlarına kadar tüm personelin katılımını gerektirir. Bilgi güvenliği şartları ve ilgili tarafların beklentileri sistemin girdilerini oluşturur. Bu süreç için PUKÖ döngüsünü kullanmamız bizim için faydalı olacaktır.

ISO27001 standardına göre; bir kuruluşun, etkin bir şekilde işlev görmek için, birçok faaliyetini tanımlaması ve yönetmesi gerekir. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir proses olarak düşünülebilir. Çoğunlukla, bir prosesin çıktısı doğrudan bunu izleyen diğer prosesin girdisini oluşturur. Bir kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak tanımlanabilir. Bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösteren şekil ISO27001standardın ilk bölümünde yer alır ve ardından da PUKO döngüsünü şu tabloyla açıklar.

Tablo 9: PUKÖ Döngüsünün Açıklamalı Anlatımı

Planla **(BGYS'nin kurulması)**	BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi
Uygula **(BGYS'nin gerçekleştirilmesi ve işletilmesi)**	BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi
Kontrol Et **(BGYS'nin izlenmesi ve gözden geçirilmesi)**	BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi
Önlem al **(BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)**	Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi

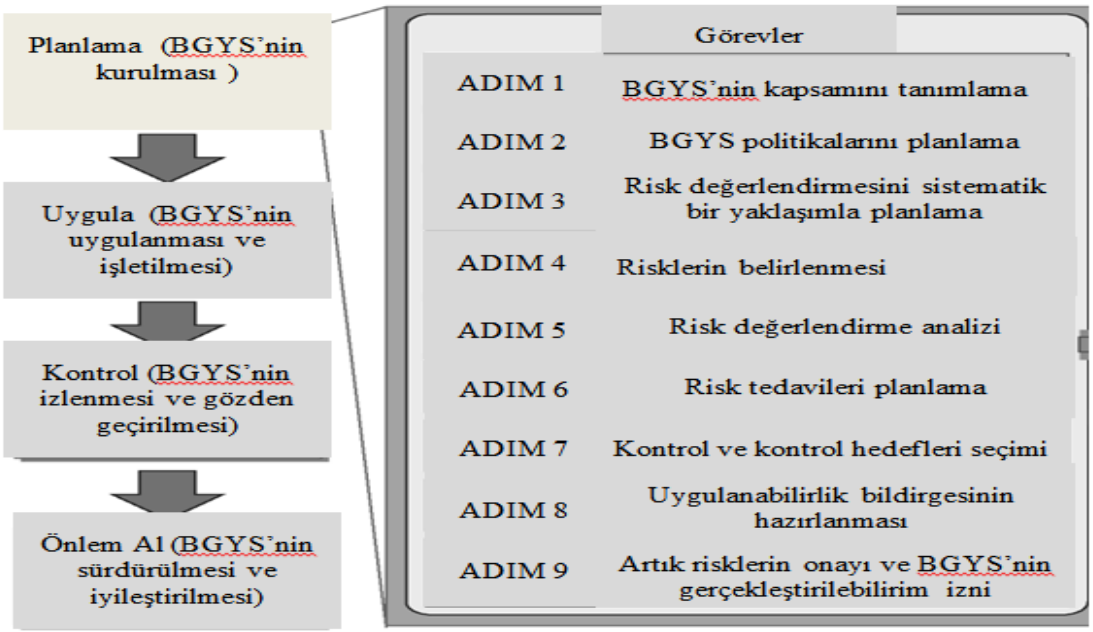


Şekil 12: BGYS Proseslerine Uygulanan PUKÖ Modeli

Kaynak: ISO27001 BGYS Standardı

Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ modelinde gösterildiği gibi (Planla – Uygula – Kontrol et – Önlem al) faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir. PUKÖ modeli özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır. BGYS kurulumu PUKÖ modelinin ilk adımını (Planla) teşkil etmektedir. Yerleşik bir sistemden bahsedebilmek için diğer adımların da uygulanması ve bunların bir döngü içinde yaşaması gerekir.(Önel ve Dinçkan, 2007:9)

BGYS kurmak için gereken görevler ve bağlantılı dokümanlar, PUKÖ döngüsüne göre ayrıntılı olarak ilerleyen bölümlerde şekillerle sunulacaktır. Öncelikle planlama aşamasında yapılması gerekenleri aşağıdaki şekilde inceleyebiliriz.



Şekil 13: BGYS Kurulumunda Yapılması Gereken Görevler (Planlama Aşaması)

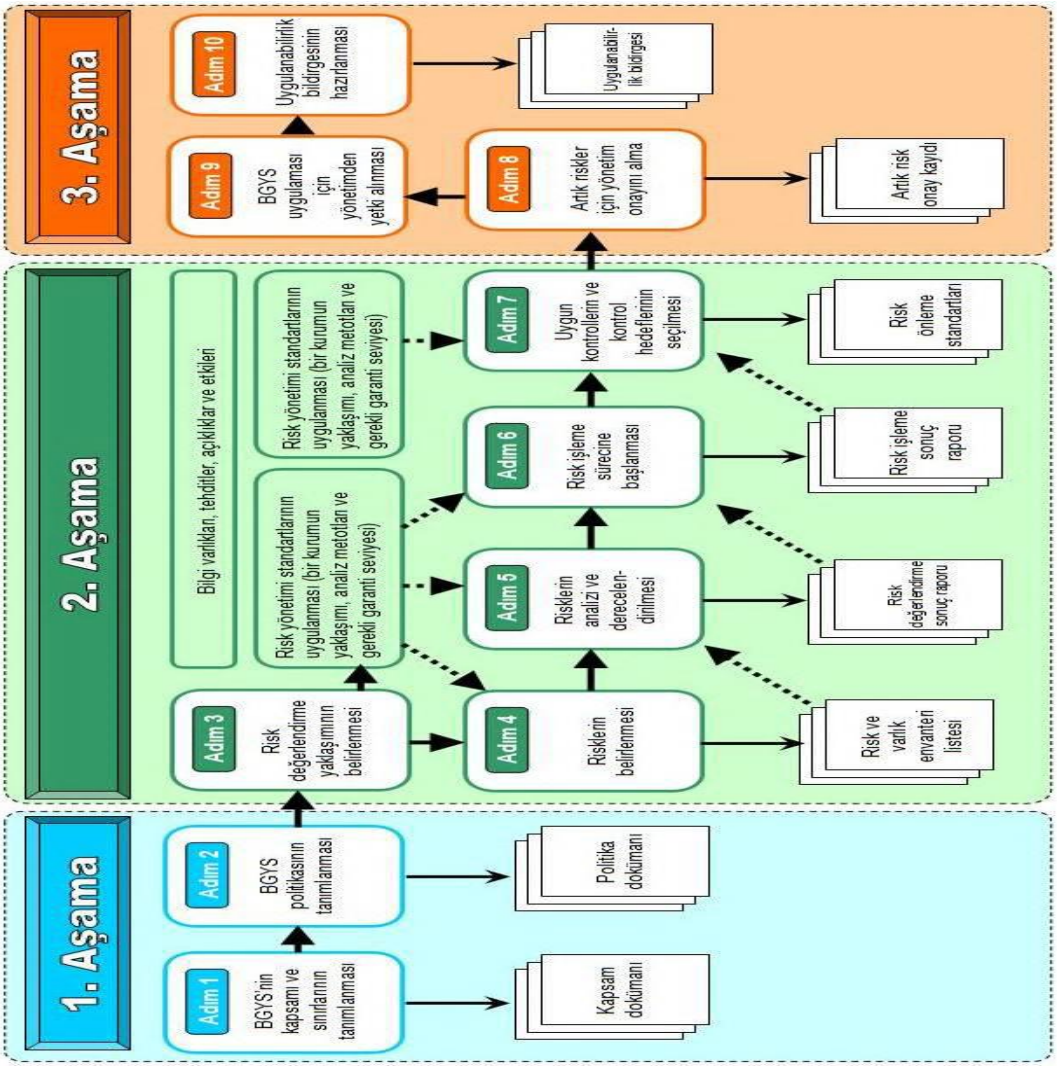
Kaynak: ISO 27999 Standardı.

4.1. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ OLUŞTURMA

Öncelikle BGYS kurulumunu bir plan dâhilinde süreci yönetmek gerekir. Kurulum sürecine nereden, hangi aşamalarla sürdürmemiz gerektiğini daha iyi anlayabilmek için UEKAE tarafından hazırlanan BGYS kurulumu kitapçığından yararlanmak faydalı olacaktır. Bu kitapçığın içerisinde yer alan bilgileri değerlendirdiğimizde; ISO27001 standardının gereksinim olarak bize sunduğu zorunlulukların nasıl yerine getirilebileceğini açıklar. Bunun yanında TS ISO/IEC 27001'i esas alan bilgi güvenliği yönetim sistemi (BGYS) kontrollerinin gerçekleştirilmesi ve denetlenmesi kılavuzu ve ISO 31000 risk yönetimi prensipler ve kılavuzlar yayınları da BGYS kurulumunda faydalı olacaktır.

BGYS kurulum aşaması şu adımlara göre devam etmektedir. İlk olarak BGYS'nin sınırlarının belirlenmesi ve kapsamının tanımlanması gerekir. Ardından sırasıyla BGYS politikasının tanımlanması, risk değerlendirme yaklaşımının tanımlanması, risk belirleme, risk analizi ve risk değerlendirmesi, risk işleme yaklaşımlarının değerlendirilmesi, kontrol hedeflerinin seçimi, artık riskin yönetim onayı, BGYS uygulamasının yönetim onayı, uygunluk bildirisinin hazırlanması

aşamaları gelir. Bazı aşamalar birbirini izleyen ve tamamlayıcı nitelikteki süreçlerdir. Bu aşamaları da kendi içerisinde ayırarak gruplandırabilmemiz mümkündür.



Şekil 14: Bilgi Güvenliği Yönetim Sistemi Kurulum Aşamaları

Kaynak: UEKAE Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzu

4.1.1. BGYS'nin Sınırlarının Belirlenmesi ve Kapsamının Tanımlanması

Bir kuruluş; kendi bünyesinde bilgi güvenliği sistemi kurarken ilk dikkat etmesi gereken, kurulacak sistemin neleri içine alacağı ve kapsamında nelerin yer alacağını bilmesidir. İlk etapta tüm sistemin ve tüm tarafların içine dâhil edilerek oluşturulan BGYS kurum için gerekli ve kolay bir süreç gibi gözükebilir. Her ne kadar BGYS kurulumu en kapsamlı şekilde hazırlanmış olsa dahi, uygulama ve kontrol aşamalarında ortaya çıkacak olan sorunlar bize farklı yaptırımlarla geri dönebilir. Bir sistemin

kurulmasından çok, o sistemin idame ettirilebilmesi önemlidir. UEKAE tarafından hazırlanan BGYS kapsam belirleme kitapçığı verdiği örneklerle de yardımcı bir kaynaktır.

İş (aktiviteler), organizasyon (yönetimsel birimler), işin mekânı, varlıklar ve teknoloji karakteristikleri belirtilerek ve kapsam dışında kalacak olan her ayrıntının sebepleri açıklanarak BGYS'nin sınırları ve kapsamı tanımlanır. Hangi yönetimsel birimlerin ve aktivitelerin bilgi güvenliği yönetim kapsamı içerisinde yer alacağı belirtilmelidir (Saliba,1998:12 –14).

Kapsam dokümanı çok sık değişime uğraması gerekmese de yaşayan bir dokümandır. Gerektiğinde kapsamın içeriği değiştirilebilir. Fakat kapsamın ilk aşamada belirlenirken yönetilebilir boyutta tutulması önemlidir. Bu yüzden organizasyonun fiziksel yapısı ve süreçleri göz önüne alınmalıdır. Örneğin; az görülmesine rağmen yönetilebilirlik adına çok büyük bazı organizasyonlarda Finans bölümü ve Yazılım geliştirme bölümü için iki ayrı BGYS oluşturulduğu gibi örnekler mevcuttur (Humphreys, [?]:32-35).

Yapmış olduğumuz mülakatlarda bir kurum kapsam olarak tüm kuruluşu kapsayacak şekilde BGYS kurarken, diğer bir kurum ise sadece bilgi işlem birimini kapsayacak şekilde BGYS kurmayı tercih etmiştir. Bunun sebeplerini sorduğumuzda bütün kurumu içine BGYS kurmanın maddi anlamda çok bir etkisi olmadığını fakat kapsamın genişlemesiyle doğacak yeni sorumlulukların bu kararı vermelerinde etkili olduğunu görmekteyiz. BGYS kurulduktan sonra taahhüt edilen şartlar sağlanamazsa öncelikle kazanılan sertifika geri alınır ve ardından cezai yaptırımlar uygulanır. Bunu ilk başta hesaba katarak sistem kurma çalışmalarımıza yön vermemiz gerekir. Daha sonradan sistemin kapsamıyla ilgili yapılacak olan küçük değişiklikler sonlara doğru ilerleyen aşamalarda çok büyük değişikliklere sebep olabilir.

Alınan bilgi güvenliği sertifikasının üzerinde BGYS'nin kapsamı da yazmaktadır. Bizim mülakat yaptığımız kurumların kazanmış oldukları sertifikaları göz önüne alıp incelediğimizde ilk etapta arasındaki farkları ve ne anlatılmak istediğini anlamakta zorluk çektik. Kurum yetkilileri bize ayrıntılı bir şekilde kurumlarının BGYS kapsamının sınırlarını belirtmesi üzerine iki sertifika arasındaki kapsam farkını daha iyi anlayabildik. BGYS sertifikasına sahip kuruluşlarla çalışmak isteyen diğer kuruluşlar

da, öncelikle sertifika üzerinde yer alan kapsamı iyi bir şekilde incelemeleri gerekir. Bu farkı sizlerin de daha iyi anlayabilmeniz için her iki kurumdan da aldığımız BGYS sertifikalarını ekler bölümünde yayınladık.

BGYS kapsamı kuruluşun adını ve unvanını belirtmelidir. Kurumun hepsini mi yoksa belirli bölümlerini mi kapsayacağını açıklamalıdır. Kuruluşun hangi alanda faaliyet gösterdiğini, kuruluşun mekânını, kuruluşun varlıklarını ve teknolojilerini belirten sınırlar çizilmelidir. Kuruluşun özel yapısından dolayı içermesi gereken farklı bağlayıcılıklar varsa o hususlar da kapsamın içinde yer almalıdır. BGYS içerisinde yer alıp ta her hangi bir politika ile korunma altına alınmayan varlıkların ve durumların neden her hangi bir işlem yapılmadığı açıklanmalıdır.

4.1.2. BGYS Politikasının Tanımlanması

Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür(Tuğlular, 2003). BGYS politikası, hedefleri ortaya koyan, yönetime yön veren ve harekete geçiren, hangi riskin değerlendirmeye alınacağına ilişkin risk yönetim kapsamı ve kriterini belirleyen bir çerçeve sunmalıdır. BGYS politikasının amacını bulması için yönetim politika içeriğindeki maddelerin uygulamaya geçirileceğine ilişkin kararlılığını çalışanlara hissettirmelidir (Önel ve Dinçkan, 2007:13).

Kurumun her kademesinde ve özellik gösteren her konuda politikalar oluşturulmalıdır. Fakat bu politikalar öncelikle genel bir bilgi güvenliği politikası hazırlandıktan sonra, ona bağlı olarak şekillendirilmelidir. Alt bölümler ve yan konular için hazırlanan politikalar daha ayrıntılı ve teknik konuları barındıracak nitelikte olmalıdır.

Bilgi Güvenliği Politikası ile ilgili ISO/IEC 27001 standardı A.5.1 maddesi için, BGYS Kontrolleri Gerçekleştirilmesi ve Denetlenmesi Kılavuzu'na göre bir Bilgi Güvenliği Politikasında en azından aşağıdaki hususlar yer almalıdır (Humphreys ve Plate, 2005).

- Bilgi güvenliğinin tanımı, genel kapsamı ve hedefi,

- Bilgi güvenliğinin kurum için neden önemli olduğu, bilgi güvenliği sağlanmasının amacı ve bilgi güvenliği ilkeleri, bu amaç ve ilkeler için yönetim desteği,
- Kontrol hedefleri ve kontrollerin seçimi için risk değerlendirmesi ve risk yönetimini de içeren bir çerçevenin ortaya konulması,
- Güvenlik politikaları, ilkeleri, standartları ve uyum gereksinimlerinin özet bir açıklaması,
- Bilgi güvenliği ile ilgili tüm görev ve sorumlulukların tanımı,
- Diğer ayrıntılı politikalar ve belirli bilgi sistemleri için prosedürler veya kullanıcıların uyması gereken kurallar gibi politikayı destekleyen dokümanlara atıflar

Bilgi Güvenliği Politikası kurumda bilgi güvenliğine yön veren temel dokümandır. Bu doküman, kurumun tüm paydaşları tarafından erişilebilen ve bilinen bir doküman olacaktır. Bu nedenle, politikayı yazarken, dikkat edilmesi gereken ilk konu, politikanın kısa ve anlaşılabilir olmasıdır. Politika çok uzun olursa, kurum kullanıcıları tarafından okunmayacaktır. Bunu göz önüne alarak, bilgi güvenliği politikasına ek olarak, tamamen kurum kullanıcıları hedeflenerek, bilgi güvenliği politikasının özetlenmiş bir sürümü hazırlanabilir. Böylece, kullanıcıların tüm dokümanı okumaları ve kendilerinden beklenenleri daha iyi anlamaları mümkün olabilir. Bu hazırlanan sürüm, Bilgi Güvenliği Politikasının ekinde veya ayrı bir doküman olarak yayınlanabilir ve paydaşlar ve kurum arasında bir sözleşme olarak kullanılabilir (Öztürk, 2008:12).

4.1.3. Risk Değerlendirme Yaklaşımı

Bilgi güvenliği politikası temel alınarak sistematik bir risk değerlendirme yaklaşımı belirlenmelidir. Kurum kendine uygun bir metodoloji seçmekte serbesttir. Seçilen risk değerlendirme metodolojisi kıyaslanabilir ve tekrarlanabilir sonuçlar üretmeyi garanti etmelidir. Bu adımda kabul edilebilecek risk seviyeleri belirlenmeli ve bunlar için ölçütler geliştirilmelidir (Önel ve Dinçkan, 2007:17).

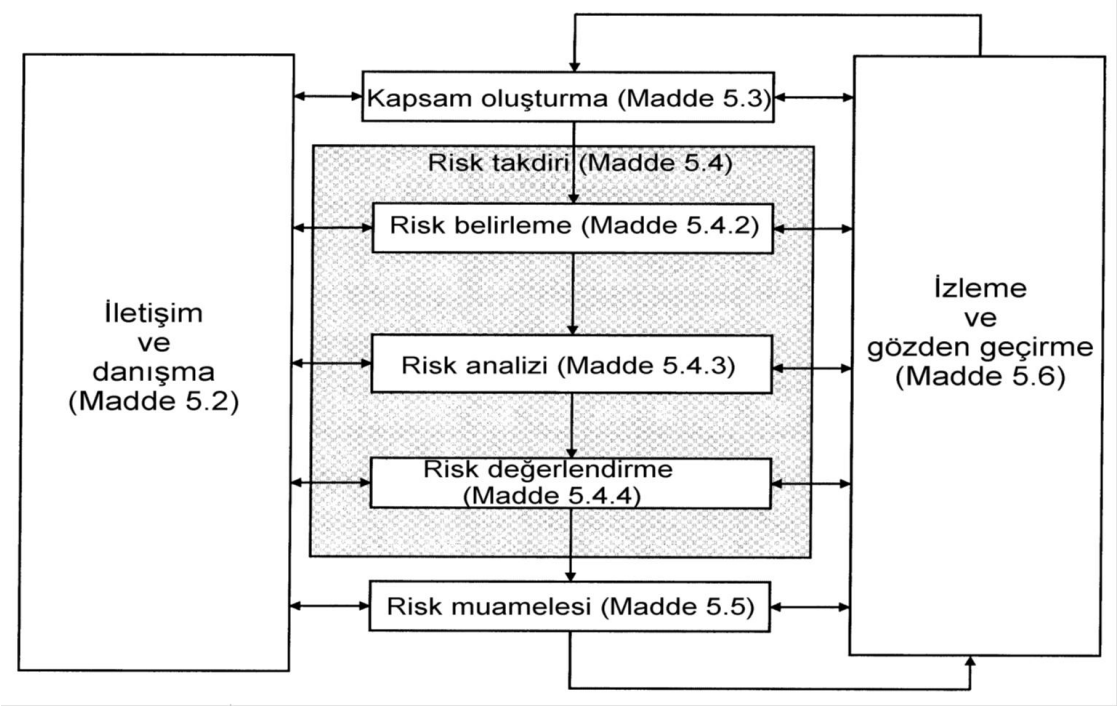
Belirlenen sistemin sağlıklı sonuçlar vermesi, ardından gelen aşamaların daha başarılı olmasını sağlayacaktır. Risk değerlendirme konusunda daha fazla bilgi

edinebilmek için ISO 31010 Risk değerlendirme teknikleri ve UEKAE tarafından hazırlanan Risk yönetim süreci kılavuzundan da yararlanılabilir. Risk tabanlı kurulan bu ISO27001 standardı yeni versiyonuyla beraber risk yönetimi konularında yaptığı değişikliklerle de ön plana çıkmaktadır. Varlık sahibi kavramı yerine kullanılmaya başlanan risk sahibi terimi bundan sonra risk yönetimi konularının daha ayrıntılı olacağının bir işaretidir. Risk ve varlık envanteri tabloları bu bölümde hazırlanmalıdır.

4.1.4. Risk Belirleme

Korunması gereken varlıkları tehdit eden riskler, risk değerlendirme yöntemi kullanılarak tespit edilmelidir. BGYS içerisindeki tüm varlıkların tanımlanması, yani varlık envanterinin çıkarılması risk değerlendirme işinin esasını oluşturur. Kurum BGYS kapsamına dahil edeceği tüm varlıkların sahiplerini, türünü ve önem derecesini bir envanter listesi şeklinde belgelemelidir. Bir varlığın önem derecesini belirlemek için bu varlığın gizliliğine, bütünlüğüne ve kullanılabilirliğine gelecek zararın kuruma yapacağı etkinin derecesini baştan ortaya koymak gerekmektedir. Varlıkların bu üç temel güvenlik özelliğine gelecek zararlar farklı etki derecelerine sahip olabilirler. Örneğin çok gizli seviyede bir bilginin açığa çıkması kuruma büyük zararlar verebilecekken aynı gizli bilginin kullanılamaz hale gelmesi o kadar büyük zarar yaratmayabilir (Önel ve Dinçkan, 2007:12).

Her bir varlığın gizlilik, bütünlük ve erişilebilirlik üzerine dayalı riskleri belirlenmesi gerekir. Bir varlığın bu ilkelerden herhangi birini veya aynı anda birkaç niteliğini birden kaybetmesi sonucunda ortaya çıkabilecek durumlar belirlenmelidir. Sistemin ve diğer üçüncü tarafların üzerinde yaratacağı etkiler belirlenmelidir. Bunun sonucunda hangi varlığın hangi niteliğini ne kadar süre ile kaybettiğinde, oluşabilecek olumsuz etkileri hesaplanmalıdır. Risk belirleme esnasında daima gerçekçi ve en kötü sonuca göre değerlendirmelerde bulunmakta fayda vardır. İleride oluşabilecek riskli bir ortamda kayıpların fazla olması ve önceden öngörüde bulunulmaması tüm sistemi tehlikeye atacaktır. Unutulmaması gereken husus her kurumun sahip olduğu varlığı kaybetmesi sonucu oluşacak olumsuz etkilerin aynı olmayacağıdır. Risk ve varlık envanteri tabloları bu bölümde hazırlanmalıdır.



Şekil 15: Risk Yönetimi Süreci

Kaynak: ISO31000 Risk Yönetimi -Prensipler Ve Kılavuzlar

4.1.5. Risk Analizi Ve Risk Değerlendirmesi

Risklerin tespit edilmesi ve değerlendirilmesi çalışmaları içerisinde geniş bir alanı tutan risk analizi; sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreç olarak tanımlandığı gibi, fayda-maliyet analizi, seçim, önceliklendirme, gerçekleştirim, sınama, önlemlerin güvenlik değerlendirmesi gibi komple güvenlik gözden geçirmesini de içerebilir (Kumaş, 2007:174-180).

Risk analizi, risk değerlendirmesine ve risklerin azaltılma ihtiyacı olup olmadığına dair kararlara ve en uygun risk iyileştirme stratejileri ve yöntemlerine bir girdi sağlar. Risk analizi ayrıca, seçimlerin yapılacağı kararların alınmasına ve farklı türlerde ve seviyelerde risk gerektiren seçeneklere de bir girdi sağlar. Risk analizi, riskin sebepleri ve kaynaklarının, onların olumlu ve olumsuz sonuçlarının ve bu sonuçların oluşabilme ihtimalinin dikkate alınmasını gerektirir. Analiz, durumlara bağlı olarak nitel, yarı nicel veya nitel veya bunların bir birleşimi şeklinde olabilir. Sonuçlar somut veya soyut etkiler cinsinden ifade edilebilir. Bazı durumlarda, farklı zamanlar, yerler,

gruplar veya durumlar için sonuçları ve bunların ihtimalini belirlemek için birden fazla sayısal değer veya açıklayıcı gerekir (ISO31000, 2011:38).

Bağımsız kuruluşlar tarafından yapılan ve kurum çalışanları tarafından yapılan denetim faaliyetleri risk analizinin amaçlarına göre yapılmalıdır. Risk analizi hazırlanırken kurum içi ve kurum dışı saldırıların olabileceği unutulmamalı ve felaket yönetimi senaryolarıyla beraber hepsi hesaba katılmalıdır.

Tablo 10: Risk Analiz Örnekleri

Tehdit Kaynağı	Açıklık	Oluşabilecek Risk
Ekipman arızası nedeniyle bağlantının kesilmesi	*Ekipmanların yedekli çalışması sürekli olarak test edilmemektedir.*	*İnternet bağlantısının kesilmesi*
Doğal afetler nedeniyle bağlantının kesilmesi	*Telekom altyapısının doğal afetlere karşı korumasız olması*	*İnternet bağlantısının kesilmesi*
Yerel ağda yayılan bir solucanın ağı satüre etmesi nedeniyle bağlantının kesilmesi	*Anti-virüs yazılımlarının tanımadığı yeni virüslere karşı uçsistem koruması bulunmaması*	*Kurum Bağlantılarının kesilmesi*
Sistemin yada programın hatalı güncelleştirme nedeniyle kullanılamaz duruma gelmesi	*Güncelleştirmelerin öncesinde test yapılmaması*	*E-posta Sunucusu'nun tehlikeye girmesi*

Kaynak: Kumaş, 2009:36.

E. Kumaş tarafından hazırlanan bir araştırmada E-devlet sistemiyle ilgili risk analizi çalışmalarına örnek verilmiştir. Risk analizi çalışmalarına örnek oluşturması için bizde bu çalışmada yer alan risk analizi tablosunu aşağıda sunuyoruz (Kumaş, 2009:37). Yapılan risk analizinden sonra ortaya çıkan sonuçlar risk değerlendirilmesine alınır ve rapor hazırlanır. Raporun içeriği iş etkileri ve risk analizinde belirtilen hususların olabilirliği hakkında olmalıdır.

4.1.6. Risk İşleme Yaklaşımlarının Değerlendirilmesi

Bu adımda risk değerlendirme sonuç raporundan yola çıkılarak uygun risk işleme (risk treatment) yöntemleri belirlenmelidir. Belli bir risk karşısında dört farklı tavır alınabilir (Önel ve Dinçkan, 2007:14):

- Uygun kontroller uygulanarak riskin ortadan kaldırılması veya kabul edilebilir seviyeye düşürülmesi
- Riskin oluşmasına neden olan faktörleri ortadan kaldırarak riskten kaçınılması
- Riskin sigorta şirketleri veya tedarikçiler gibi kurum dışındaki taraflara aktarılması
- Kurum politikalarına ve risk kabul ölçütlerine uyması şartıyla riskin objektif bir biçimde ve bilerek kabul edilmesi

Uygun kontrol tedbirleri uygulanarak riskin ortadan kaldırılması her kurum için birinci önceliktir. Uygun kontroller yapılmasıyla, riskin derecesinin düşürülmesi de olumlu bir sonuç olmasına rağmen riskin kabul edilebilirlik durumuna göre tercih edilmeyebilir. Riski ortaya çıkaracak faktörleri ortadan kaldırarak riskten kaçınırken hesap edemediğimiz birçok kaynağı da iptal etmiş olabiliriz. Yasaklamalar yapılırken sonucunun bize ne gibi eksiklikler doğuracağını önceden iyi hesaplamak gerekir.

Riskin üçüncü taraflara aktarılması tercih edilmesi durumunda fayda maliyet analizi yapılmalıdır. Riskin olumsuz bir sonuç ortaya koyması ile oluşabilecek zarara karşın, sigorta masraflarının oluşturacağı maliyet hesaplanarak karar verilmelidir. Kurumun yapmış olduğu iş dalına göre ve müşterilerine taahhüt ettiği iş kalitesine göre bazı risklerin sonuçları göz ardı edilebilir.

Örneğin bir haber ajansının internet sitesine erişimin bir saat sağlanamaması, o kurum için kabul edilemez bir risktir. Bu riskin çözümü için ilave tedbirler alınması ve gerekli masraflara girilmesi gerekir. aynı varlık üzerinden değerlendirme yaparsak bir bankanın bu riski kabul etme ihtimali çok daha düşüktür. Daha kısa süreli bir erişim sıkıntısını daha büyük bir risk olarak kabul edebilir. Diğer bir yandan bir üniversitenin internet sitesine erişimin aksaması daha fazla süre için bile kabul edilebilir bir risktir. Kaybedecek olduğumuz değerler, bize elinde bulundurduğumuz varlığın gerçek kıymetini belirler. ISO27001 standardının yeni versiyonuyla beraber risk işleme

yönteminin yazılı halde olması zorunluluğu kaldırılıyor ve risk işleme sürecinin tanımlanması gerektiği anlatılıyor.

4.1.7. Kontrollerin Ve Kontrol Hedeflerinin Seçimi

ISO 27001standardının ekler kısmında yer alan kontrol maddeleri bize temel oluşturacak nitelikte hazırlanmışlardır. Bu kontrol maddelerinin hepsini veya bir kaçını BGYS için uygulamak tavsiye niteliğindedir. Bu kontrol maddelerinin yanında yeni maddelerde eklemek yine tercihe dayalıdır. Sistemin başarısını objektif olarak görebilmemiz için en uygun kontrol maddelerinin seçilmesi gerekir.

Yenilenen ISO27001 standardı ile ek-a kısmında yer alan kontrol maddelerinde de değişiklikler olmuştur. Mevcut sürümdeki kontrol hedefleri on birken, yeni sürümdeki kontrol bölümü on dörde yükselmiştir. Bunun yanında kontrol maddeleri sayısı da yüz otuz üçten, yüz on dörde düşmüştür. Yenilen versiyondaki kontrol amaçları ve yeni eklenen kontrol maddeleri aşağıda ayrıntılı olarak verilmiştir.

- A.5 Bilgi Güvenlik Politikası
- A.6 Bilgi Güvenliği Organizasyonu
    - A.6.1.5 Proje Yönetiminde Bilgi Güvenliği
- A.7 İnsan Kaynakları Güvenliği
- A.8 Varlık Yönetimi
- A.9 Erişim Kontrolleri
- A.10 Kriptografi
- A.11 Fiziksel ve Çevresel Güvenlik
- A.12 İşletim Güvenliği
    - A.12.6.2 Yazılım Yükleme Kısıtları
- A.13 İletişim Güvenliği
- A.14 Sistem Edinimi, Geliştirilmesi ve Bakımı
    - A.14.2.1 Güvenli Yazılım Geliştirme Politikası
    - A.14.2.5 Güvenli Sistem Mühendisliği Prensipleri
    - A.14.2.6 Güvenli Yazılım Geliştirme Ortamı
    - A.14.2.8 Sistem Güvenliği Testi

- A.15 Tedarikçi İlişkileri
    - A.15.1.1 Tedarikçi İlişkileri İçin Bilgi Güvenlik Politikası
    - A.15.1.3 Bilgi Ve İletişim Teknolojisi Tedarik Zinciri
- A.16 Bilgi Güvenliği İhlal Yönetimi
    - A.16.1.4 Bilgi Güvenliği Olaylarını Değerlendirme Ve Karar Verme
    - A.16.1.5 Bilgi Güvenliği Olaylarının Cevaplanması
- A.17 İş Sürekliliği Yönetiminin Bilgi Güvenlik Alanları
    - A.17.2.1 Bilgi İşleme Olanaklarının Erişilebilirliği
- A.18 Uyum

Bilgi güvenliği politikası; öncelikle yönetimin onayı ile doküman haline getirilmeli ve yayınlanarak kurum içi çalışanlar ve ilgili dış tarafların bilgisine sunulmalıdır. Belirli aralıklarla ve önemli değişiklikler yaşandığında gözden geçirilmeli ve güncellenmelidir.

Bilgi güvenliği organizasyonu iki bölümle karşımıza çıkmaktadır. İlk bölüm iç organizasyonun bilgi güvenliğindeki görevlerini ve sorumluluklarını açıklar. Yeni bilgi işlem tesisleri için yetki proseslerini tanımlama, gizlilik anlaşmaları ve bilgi güvenliğinin bağımsız gözden geçirilmesi konularını içerir. İkinci bölüm önceden dış taraflarla olan ilişkileri, riskleri ve üçüncü taraf anlaşmalarını açıklarken, yenilenen versiyonda mobil cihazlar ve uzaktan çalışma konuları yer almaktadır. Mevcut durumda bu bölümün benzeri erişim kontrolü bölümünde yer almaktaydı.

İnsan kaynakları güvenliği; mevcut standartta sekizinci bölümde yer alır. İlk olarak işe alım öncesi durum açıklanır. Adaylarla ilgili geçmiş bilgilerinin kontrol edilmesi, kanunlar ve etik değerlere ışığında işe olan yeterliliği irdelenir. İş yaşantısı sürecinde yönetimin sorumlulukları, bilgi güvenliği farkındalığı, bilgi güvenliği eğitimleri ve bilgi güvenliği kırılmasına sebep olanlar için hazırlanması gereken disiplin prosesi açıklanır. Son olarak ta işe son verme durumunda yapılması gerekenler açıklanır.

Varlık yönetimi; mevcut durumda yedinci bölümde yer alır. İlk bölümde varlık envanteri oluşturulması gerektiği, varlıkların hepsinin sahiplenilmesi gerektiği ve kullanıcılar için kabul edilebilir yetkilerinin verilmesini açıklar. Yeni standartta bu bölüme varlığın geri verilmesi durumları eklenmiştir. İkinci bölümde bilgi

sınıflandırılması, bilgi etiketlemesi ve bilgi işleme konuları anlatılmaktadır. Yeni sürümde üçüncü bölüm olarak ortam işleme konusu eklenmiştir. Daha önce bu konu haberleşme ve işletim yönetimi konularının altında yer almaktaydı.

Erişim kontrolleri; mevcut sürümde on birinci bölümde yer almaktadır. İlk olarak bilgiye erişimin kontrollü bir şekilde bir politikaya bağlanarak yapılması gerektiği açıklanır. Ağa erişim ve ağ hizmetleri konuları da bu bölüm altına gelmiştir. İkinci bölümde kullanıcı erişimi açıklanmaktadır. Kullanıcıların kayıt olmaları, kayıt dışına çıkmaları, erişim hakları, yöneticilerin ayrıcalıklı erişim hakları ve erişim haklarının iptal edilmesi veya tekrar değerlendirilmesi konularını kapsar. Kullanıcı sorumluluğu altında kullanıcıların gizli bilgilerine erişimin korunması konularında sorumlu oldukları açıklanır. İşletim sistemi ve uygulama erişim kontrolleri içerisinde bilgi erişim bölgeleri, güvenli oturum açma ve kapama prosedürleri, parola yönetim sistemleri, ayrıcalıklı programların kullanılması ve program kodlarına erişim kontrolleri açıklanmaktadır.

Kriptografi kontrollerinde, gerekli politikalar ve anahtar yönetimi konuları ele alınmaktadır. Mevcut sürümde bilgi sistemleri edinim, geliştirme ve bakımı bölümlerinin altında yer almaktadır. Şifreleme ve şifre oluşturma konularının temel bilgi güvenliği farkındalığı konularının içerisinde de yer alması gerekmektedir.

Fiziksel ve çevresel güvenlik konuları da şuan ki sürümde dokuzuncu bölümde yer almaktadır. İlk bölümde bilgi ve bilgi işlem alanlarının nasıl bir sistemle güvence altına alındığı açıklanır. yetkili kişilerin girebileceği alanlar açıklanır, ofisler ve odalar için alınması gereken fiziki tedbirler açıklanır. Doğal yâda insan kaynaklı felaketlere karşı alınması gereken tedbirler açıklanır. dağıtım ve yükleme alanlarının erişiminin nasıl sağlanması gerektiği ile ilgili hususlar açıklanır. İkinci bölümde ise teçhizatın yerleştirilmesindeki hususlar, elektrik kesintileri, destek hizmetlerinin aksamasından doğacak arızalar için koruma tedbirleri, kablolama güvenliği, teçhizatın bakım ihtiyaçları, ekipmanın, bilgi veya yazılımın bulunduğu yerden çıkarılabilmesi, teçhizatın güvenli olarak elden çıkarılması ve tekrar kullanımı konuları açıklanır. ayrıca yeni sürümde bu bölüme temiz masa, temiz ekran politikası eklenmiş ve bu konu içinde kontrol esaslarını anlatılmıştır.

İşletim güvenliği; daha önce onuncu bölümde haberleşme ve işletim yönetimi bölümünün altında gördüğümüz konuları açıklamaktadır. İşletim prosedürlerinin yazılı hale edilmesi gerektiği ve tüm ihtiyacı olan kullanıcıların erişebilmesi imkanı olması gerektiğini, değişim yönetimi konularını, yönetim kapasitesi konularını ve geliştirme, test ve işletim olanaklarının ayrımını anlatır. Kötü amaçlı kodlara karşı korunmayı, bilgilerin yedeğinin alınmasını, saat senkronizasyonu, olay kayıtlarının tutulması, kayıt bilgilerinin güvenliği, işletim yazılımlarının kontrolleri ve teknik alanlardaki açıklıkların yönetilmesi gibi konular açıklanmaktadır. Ayrıca yeni sürümle beraber yazılım yükleme kısıtlamaları konusu da bu bölüm içine eklenmiştir.

İletişim güvenliği; ağ güvenliği yönetimi ile ilgili hususlar, ağ hizmetleri güvenliği, ağların kullanıcılara ve gruplara göre ayrılması, hizmet sağlayıcıların kurum içinden ve dışından olması konuları açıklanmaktadır. İkinci bölümde de bilgi değişimi politika ve prosedürleri konuları, bilgi değişimi anlaşmaları ve elektronik mesajlaşma konularını ele alır.

Sistem edinme, geliştirme ve bakımı; bu bölüme yeni sürümle beraber eklenen yeni maddeler vardır. İlk olarak bilgi sistemlerinin güvenlik gereksinimleri, yapılması gereken analizleri, halka açık ağlarda uygulama hizmetlerinin güvenliği konularına değinir. İkinci bölümde geliştirme ve destek proseslerini, sistem değiştirme kontrolü prosedürlerini, yazılım paketlerindeki değişikliklerin kısıtlanması, geliştirme çevresinin güvenliği, dış kaynak geliştirme ve test bilgilerinin korunması konularını açıklar.

Destekçilerle olan ilişkiler; tedarikçilerle olan ilişkilerde bilgi güvenliği prosedürleri, anlaşmalar, tedarik zinciri bilgi ve iletişim prosedürleri açıklanmaktadır.

Bilgi güvenliği ihlal olayı yönetimi; mevcut sürümde on üçüncü bölümde yer alan bu konu eklenen yeni bölümlerle on altıncı bölümde karşımıza çıkmaktadır. Sorumluluklar ve prosedürler, bilgi güvenliği olaylarının raporlanması, bilgi güvenliği zayıflıklarının raporlanması, bilgi güvenliği ihlal olaylarından öğrenme ve delil toplama konularını açıklar. Bilgi güvenliği ihlal olaylarının yazılı prosedürlerle cevaplandırılması konularına da değinilir.

İş sürekliliği yönetiminin bilgi güvenliği alanları; bilgi güvenliliğinin sürekliliğinin planlanması, iş sürekliliğini yerine getirme için gerekli dokümanlar,

politikalar ve bunların bakımı ile ilgili prosedürler, bilgi işleme olanaklarının erişilebilirliği açıklanmaktadır.

Uyum bölümünde; yasal mevzuata ve sözleşmelerden doğan gereksinimlere uyumu, fikri mülkiyet haklarını, kayıtların korunmasını, kişisel bilgilerin gizliliği ve korunması, kriptografik kontrollerin kullanılmasını açıklar. İkinci bölümde de bilgi güvenliğinin yeniden bağımsız değerlendirilmesi, güvenlik politika ve standartlarıyla uyum ve teknik uyumun tekrar değerlendirilmesi konularını içermektedir.

4.1.8. Artık Risk Onayı

Risk iyileştirmesinden sonra geriye kalan riske artık risk denir. Artık risk belirlenemeyen riski içerir. Artık risk "muhafaza edilen risk" olarak da bilinir. Karar alıcılar ve diğer paydaşlar risk iyileştirmeden sonra artık riskin doğası ve uzantısından haberdar olmalıdır. Artık risk belgelendirilmeli ve izlenmeli, gözden geçirilmeli ve uygun olduğunda bir daha muamele edilmelidir (ISO31000, 2011: 48).

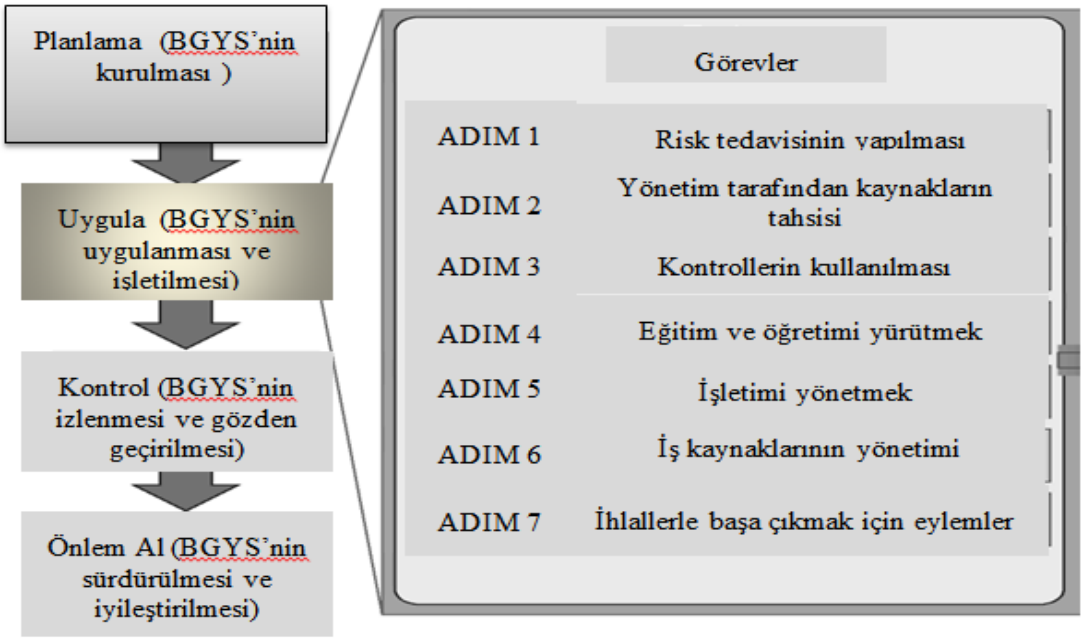
Yönetim kademesi tarafından belirlenen artık risklerin onaylanması ve doküman haline getirilmesi gerekir. Kayıt altına alınarak onaylanan artık riskler zaman içinde şartlar olgunlaştıkça yeniden gözden geçirilmeli ve iyileştirmeler yapılmalıdır. Yönetim tarafından onaylanması o riskin artık hiçbir işlem görmeyeceği anlamına gelmez. Standardın yeni versiyonuyla beraber artık riskin onay makamı üst yönetim kademesi yerine, risk sahipleri olarak değiştirilmiştir.

4.1.9. Uygunluk Bildirgesinin Hazırlanması

Bu sürece kadar olan aşamaların neticesinde bir bilgi güvenliği sistemi ortaya çıkmış olur. Bu sistemin uygulanabilmesi için gereken tek adım yönetim tarafından onaylanmasıdır. Yönetimin yetkiyi vermesi sonucunda kabul edilen sistem tüm çalışanlara duyurularak uygulanmaya başlanır. Uygulamaya başlarken tüm personeli bilgilendirmek amacıyla bir toplantı yapılması ve kurulan sistemin önemi bir kez daha vurgulanabilir. Uygulamaya geçilen sistemde uygunluk bildirgesi hazırlanmasıyla kurulum işlemi sona ermiş olur.

Uygulanabilirlik Bildirgesi; seçilen kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğini anlatmalıdır. ISO/IEC 27001 Ek-A'dan seçilmeyen kontrollerin neler olduğu ile bunların seçilmeme gerekçeleri de Uygulanabilirlik Bildirgesinde verilmelidir. Ayrıca mevcut durumda uygulanmakta olan kontroller de yine bu belge içinde yer bulmalıdır (Önel ve Dinçkan, 2007:18).

Yeni çıkan versiyonda da bu zorunluluk devam etmektedir. 6.1.3 içinde ne yapılması gerektiği ve ilgili maddenin (d) fıkrasında ek-a bölümünde yer alan kontrol maddelerinden hangisinin kullanılıp, hangisinin neden kullanılmadığı ile ilgili uygunluk bildirgesi hazırlanması istenmektedir.



Şekil 16: BGYS Kurulumunda Yapılması Gereken Görevler (Uygulama Aşaması)

Kaynak: ISO 27999 Standardı.

4.2. YAZILI HALE GETİRİLMİŞ BİLGİ

Mevcut sürümde dördüncü maddenin üçüncü fıkrasında yer alan dokümantasyon gereksinimleri ortadan kalkmıştır. Onun yerine eklenen bu madde belge ve kayıt ifadelerin ayrı ayrı kullanmak yerine hepsini yazılı hale getirilmiş bilgi olarak nitelemektedir. Mevcut sürümde BGYS dokümantasyonunun neleri kapsaması gerektiği ve standardın hangi maddesine dayanılarak hazırlanması gerektiği

belirtilmekteydi. Yeni sürümle beraber hangi dokümanları tutmamız gerektiği ile ilgili bölüm kalkmıştır. Fakat kayıtların tutulması zorunluluğu devam etmektedir.

Bir organizasyon için kabul edilen yazılı bilgi diğer bir organizasyon için geçerli olmayabilir. Kuruluşun büyüklüğüne, faaliyetlerinin türüne, ürünlerine ve sağladıkları hizmete göre değişiklikler gösterebilir. Çalışan kişilerin becerilerine göre ve iş süreçlerinin karmaşıklığına göre de değişiklikler gösterebilir. Yazılı bilginin oluşturulması ve güncellenmesi ile ilgili alt madde eklenmiştir. Yazılı bilgi uygun tanımlama ve açıklamayı yapması gerekir. Hangi koşullarda saklanacağını, hangi dilde ve sürümle hazırlandığı ve güncellendiği kayıt altına alınmalı, onaylanmalı ve sonraki dönemlerde bu hususlar dikkate alınmalıdır.

Yazılı bilgi kontrol edilirken; gerekli yer ve zamanda, ihtiyaç duyulan miktarda erişim sağlamaya imkân verip vermediği kontrol edilmelidir. Yazılı bilginin nasıl muhafaza edildiği, nasıl korunduğu, yapılan değişikliklerin kontrollü bir şekilde nasıl gerçekleştirildiğini açıklar. Yazılı bir ifade kuruluş için ihtiyaç olmaktan çıkmışsa, nasıl kontrol altında tutulması gerektiği ve nasıl tespit edilmesi gerektiği anlatılır.

Yeni sürümle beraber birebir doküman zorunluluğunu belirten madde ortadan kalkmıştır. Hangi kayıtların tutulmasını gerektiğini anlamak içinde standardın ana maddeleri ve ek kısmını inceleyip gerekli olan kayıtları tespit etmemiz gerekir. Yazılı haldeki tutulması gereken bilgi kayıtları ve doküman ihtiyaçlarının hangi maddelere göre oluşturulması gerektiği aşağıda sıralanmıştır.

Standardın ana maddelerinde geçen yazılı bilgi ihtiyaçları:

- BGYS kapsamı (madde 4.3.)
- Bilgi güvenliği politikası (madde 5.2.)
- Risk analizi ve risk değerlendirme (madde 6.1.2.)
- Risk tedavi prosesi ve Uygulanabilirlik beyanı (madde 6.1.3.)
- Eğitimler ve yeterlilik belgeleri (madde 7.2.)
- Risk değerlendirme sonuç raporları (madde 8.2.)
- Risk değerlendirme sonuç raporları (madde 8.3.)
- Ölçme, izleme ve analiz sonuçları (madde 9.1.)
- İç denetim planı ve İç denetim raporu (madde 9.2.)

- Yönetimin gözden geçirme raporu (madde 9.3.)
- Uygunsuzluk ve düzeltici faaliyetlerin kayıtları ve sonuçları (madde 10.1.)

Standardın ek bölümde yer alan kontrol maddelerinin gereksinim duyduğu yazılı bilgi gereksinimleri:

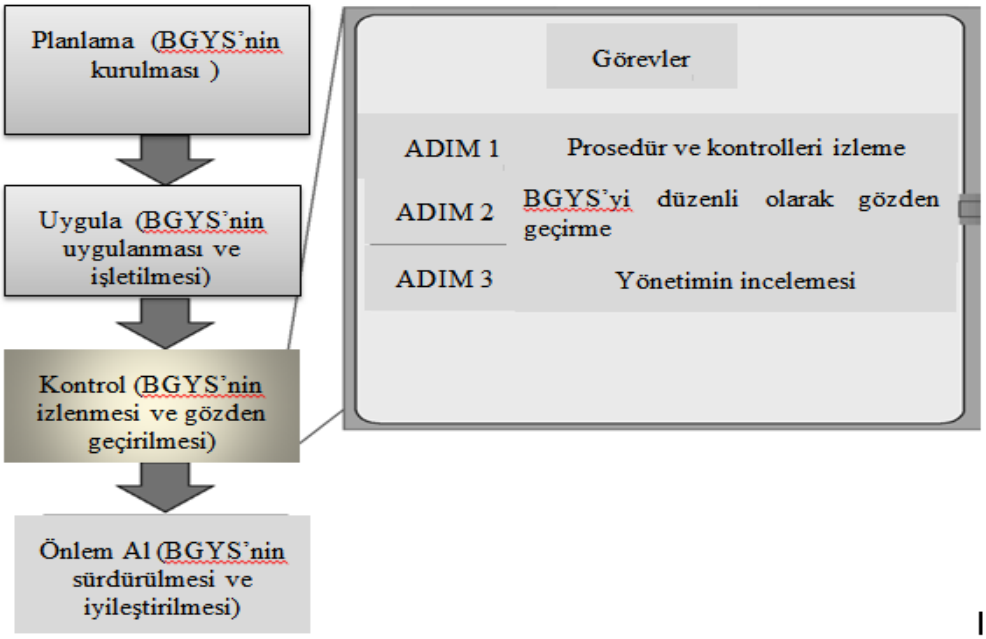
- Varlık envanteri (A.8.1.)
- Erişim kontrolü politikası (A.9.1.1.)
- İşletim prosedürleri (A.12.1.1.)
- Kullanıcı sisteme girişi, sistemi terk etmesi, kullanıcının yaptığı hataların kayıtları ve bilgi güvenliği olayları (A.12.4.1.)
- BGYS konuları ile ilgili gizlilik ve açıklamama anlaşmaları(A.13.2.4.)
- Güvenli sistem mühendisliği prensipleri (A.14.2.5.)
- Tedarik zinciri bilgi güvenliği politikası (A.15.1.1.)
- Bilgi güvenliği ihlali tepki prosedürü (A.16.1.5.)
- İş sürekliliği prosedürü (A.17.1.2.)
- Yasalardan, düzenlemelerden ve anlaşmalardan doğan gereksinimler (A.18.1.1.)

Bir BGYS kurulurken en az yukarıda belirtilen yazılı belgelerin olması gerekir. Kuruluşun ihtiyaçlarına ve özelliklerine göre daha fazla yazılı belgede bulundurulabilir. Eklerde yer alan kontrol maddelerinin bulundurulma zorunluluğu organizasyonun yapısına göre değişebilir.

4.3. BGYS KURULUMU SONRASI İŞLEMLER

Bu zamana kadar gerçekleşen adımlar BGYS kurulum sürecini açıklayan adımlardır. Bu aşamaya geldikten sonra, kurulum sürecinde yapılan çalışmaların sonuçlarını görmeye başlarız. İlk olarak yönetim tarafından kabul edilen bilgi güvenliği sisteminin uygulanması gerekir. Bu uygulama en az bir aylık bir süreyi kapsamalıdır. Bu esnada oluşacak hatalar ve eksiklikler gözlemlenir ve rapor tutularak, iyileştirmeye gidilir. Bu adımdan sonra atılacak gözden geçirme, iyileştirme ve sürekliliğin sağlanması adımları her zaman devamlı surette, herhangi bir uyarı beklemeden icra edeceğimiz faaliyetlerdir. Bilgi güvenliği sistemleri, teknolojik gelişmelere ayak

uydurabilmeli ve dinamik yapısını her daim canlı tutmalıdır. Kurulan Bgys etkili olabilmesinin tek yolu kendini sürekli gözden geçirerek, yenileyebilmesinden geçer.



Şekil 17: BGYS Kurulumunda Yapılması Gereken Görevler (Kontrol Aşamaları)

Kaynak: ISO 27999 Standardı.

4.3.1. Yönetimin Sorumluluğu

Mevcut sürümde bu işlemleri yapması gereken kişi ve kademe belirtilmemiş onun yerine "kuruluş" ifadesi kullanılmış ve "kuruluş bunları yapmalıdır" ifadeleri yer almıştır. Yönetimin sorumluluğu bölümünde yönetimin yapması gerekenler vurgulanmaktadır. Yeni sürümle beraber liderlik kavramı da karşımıza çıkmaktadır. Üst yönetimin bilgi güvenliği yönetim sistemleri konusunda önderlik etmesi gerektiğinden bahsetmektedir. Üst yönetimin bilgi güvenliği politikası hazırlaması gerektiği ve politikanın hangi konuları içereceğini anlatmaktadır.

Kuruluş içindeki roller, sorumluluklar ve yetkilerin üst yönetim tarafından dağıtılması ve raporlanması konularını açıklamaktadır. Roller ve sorumluluklarla ilgili dokümanları hazırlama zorunluluğu da vardır. Liderlik konusu diğer bütün maddelerin gerçekleştirilmesi sürecinde faaliyet gösteren bir kavram niteliği kazanmıştır. Bgys

kurulumuna karar verilmesi aşamasından, en son gerçekleştirilen adıma kadar liderlik konusunun etkin bir rolü vardır.

4.3.2. Kaynakların Yönetimi

Kaynakların yönetimi mevcut sürümde yönetim sorumluluğunun altında yer alan bir konu iken, yeni sürümde yedinci bölümde yer alan destek başlığının altında toplanmıştır. Kaynak yönetiminde BGYS'nin işlemesi, sürdürülmesi, izlenmesi için kaynak ayırmayı, yasal mevzuat hükümlerini ve yapılan anlaşmalara uyulması için gerekli kaynakların ayrıldığı konularını anlatır. Bunun yanında eğitim, farkındalık ve yeterlilik konularına da değinilir. Yeni sürümde daha önce kaynaklar bölümünün altında gördüğümüz yetkinlik ve farkındalık konuları ayrı ayrı ele alınmaktadır.

4.3.3. Farkındalık Yaratma

Farkındalık yaratma, BGYS kurulundaki temel amaçlardan bir tanesidir. Bilgi güvenliği çalışmalarına öncelikle bireylerde bilgi güvenliği algısı yaratarak başlanası gerekir. Çünkü sistemi kuracak ve onun idamesini sağlayacak olanlar sistem içinde rol alan bireylerdir. Ne yapıldığının farkında olmayan personel, sistemin kurulmasına ve işletilmesine yüzde yüz verimle katkıda bulunamaz.

Yapılan işlemler politikalar ve prosedürlerde yazılı olarak kalır daha da ileriye gidemez. BGYS kurmadan da kurumlar personeli üzerinde farkındalık yaratmayı tercih edebilirler. Bunun için kurumların seminer, eğitim ve konferans gibi faaliyetleri desteklemeleri gerekmektedir. Ülkemizde Bilgem tarafından yürütülen farkındalık eğitimleri ve bilgiguvenliği.gov.tr internet ağı üzerinden de bireysel kullanıcıların hizmetine sunulmuştur. E-devlet projelerinin temelinde de devlet desteği ile bilgi güvenliği farkındalığı yaratma amacı güdülmektedir.

E-Devlet Kapısı Projesi özelinde Bilgi Güvenliği Yönetimi çalışmaları gereği belirli bir farkındalık ve bilinçlilik düzeyi sağlanması sonrasında projenin çerçevesini genişleterek kurumsal düzeyde yürütmek uygun olacaktır. Türkiye'nin kamu yapılanması içerisinde yapılandırılması hedeflenen "Bilgi Güvenliği Kurumu" na çok is düşmektedir. Öncelikle orta seviye yöneticiler düzeyinde bir tanıtım toplantısı, sonrasında ise her kurumdan bir "temsilci" görevlendirilecek şekilde bilgi güvenliği ile

ilgilenecek bir uzman atanması faydalı olacaktır. Bu konuda e-Devlet Kapısı Projesi teknik şartnamesinde bulunan "Güvenlik Komisyonu/Grubu" nun yönlendirilmesinde kurumlara öncelikle bir farkındalık eğitimi, projenin güvenlik konusunda gidişatı ile ilgili bir bilgilendirme sağlandıktan sonra kurum temsilcilerini sinerji yaratarak hedefe yöneltebilecek bir strateji ortaya konulması hedeflenmektedir. Bu strateji çerçevesinde kurumların yönlendirilmesi ile ilgili olarak aşağıdaki şekilde verilmiştir (Kumaş, 2009).

Şekil 18: Kamu Kurumlarında Bilgi Güvenliği Farkındalığı

Kaynak: Kumaş, 2009.

Ankara'daki on dört üniversite kütüphanesi üzerinde yapılan bilgi merkezlerinde bilgi güvenliği farkındalığı araştırmasında şu sonuçlara varılmıştır. Araştırma bulguları doğrultusunda, kütüphanelerin büyük bir kısmında bilgi güvenliğinin sağlanması gerekli ve önemli bulunurken, bilgi güvenliğinin ne olduğu ve ne tür uygulamaları içerdiği hususunda yeterince bilgi sahibi olunmadığı, hali hazırda yürütülen güvenlik uygulamalarının bilgi işlem daire başkanlıkları tarafından gerçekleştirildiği sonucuna ulaşılmıştır. Bilgi güvenliğinin sağlanması çoğu kütüphanede bilgi işleme mal edilmiş olup, yöneticilere göre personel olası tehditlere karşı alması gereken önlemlerin yeterince farkında değildir. Bununla birlikte kütüphanelerde bilgi güvenliği farkındalığı

yaratmayı amaçlayan herhangi bir uygulama bulunmamakta ve konuya ilişkin bir eğitim verilmemektedir(Öztemiz ve Yılmaz, 2013:87-98).

> *Bir meslek yüksekokulunda yapılan; bilgi iletişim teknolojilerinin öğrenciler üzerindeki farkındalığı araştırmasında şu sonuçlar karşımıza çıkmaktadır. Öğrencilerin yaklaşık %80' i notebook, netbook & tablet pc, masaüstü bilgisayar ve akıllı telefon cihazlarından en az birine sahiptir. Öğrencilerin yaklaşık olarak %60'ı her gün bilgisayar kullanırken %92'si ise haftada en az birkaç kez bilgisayar kullanmaktadırlar. Öğrencilerinin %85'i bir sosyal ağa üyedir ve %63'ü interneti daha çok sosyal ağlara erişmek için kullanmaktadır. Bilgi güvenliği konusunda ise her dört öğrenciden biri anti-virüs programı kullanmaya özen göstermemektedir. Konu güvenlik olduğunda bu oranların çok da düşük olmadığı söylenebilir. Sosyal ağların suç işlemeye elverişli olduğunun farkında olanlar ise sadece %70. Bu ağların hukuk ihlallerine açık olduğunu bilmeyenlerin oranı ise %60 civarındadır. Bu amaçla zararlı yazılımlar ve bunlardan korunma yolları, bilişim suçları, telif hakları gibi konular temel bilgisayar derslerinin içeriğine eklenebilir (Karpuz vd.,2013:142).*

4.3.4. Eğitim Ve Yeterlilik

Eğitim faaliyetleri bilgi güvenliği sistemi kurmak isteyen kuruluşlar için en önemli öğedir. Sistem kurmaya karar veren bir kuruluş öncelikle bu çalışmayı kendi imkânlarıyla mı yoksa dış kaynak kullanarak mı gerçekleştireceğine karar vermelidir. Eğer bu çalışmayı kendi personeliyle yapmayı düşünürse, personeline yeni eğitimler aldırmak zorundadır.

Ülkemizde birçok danışmanlık firması ISO27001 baş tetkikçi eğitimleri vermektedir. Bu eğitimlerde önemli olan husus uluslararası geçerliliğe sahip kuruluşlar tarafından sertifikalandırılan eğitim faaliyetlerini tercih etmektir. Certified Information Systems Security Professional (CISSP) bilgi sistemleri güvenlik uzmanlığı sertifikası, sektöründe en çok geçerliliği olan bir eğitim belgesidir. Bu belgenin alınabilmesi için gerekli eğitim düzeyi şartları aranmaktadır. Ardından uluslararası bir sınava girilerek başarılı olma şartı aranmaktadır.

Certified Information Systems Auditor (CISA) bilgi güvenliği denetçi sertifikası ISACA tarafından yapılan sınavlarla verilmektedir. Ayrıca ISACA bünyesinde Sertifikalı Bilgi Güvenliği Yöneticisi (CISM), Sertifikalı Kurumsal BT Yönetişim Uzmanı (CGEIT) ve Risk ve Bilgi Sistemleri Kontrolü Onayı (CRISC) belgeleri de verilmektedir. Bu konuda daha geniş bilgi almak için ISACA'nın resmi internet sayfasında, ülkemizdeki BT uzmanlar aracılığıyla hazırlattığı Türkçe bölümleri takip edebilirsiniz.

Bunun yanında üniversitelerin sürekli eğitim merkezlerinde yürütülen temel bilgi güvenliği eğitimleri sürdürülmektedir. BGYS kuracak bir kuruluş öncelikle tüm personeli ilgilendiren konularda temel bilgi güvenliği eğitimlerini alanında uzman kişiler aracılığıyla sağlamalıdırlar. Bu eğitim faaliyetleri belirli periyotlarla tekrarlanmalıdır. İşe yeni alım sürecinde de temel eğitim konularını kapsayan eğitimler verilmelidir.

Bilgi işlem personeline kendi alanlarıyla ilgili önem arz eden konularda özel ve teknik eğitimler verilmelidir. Kuruluş bünyesine entegre olacak yeni bir faaliyette veya yeni gelişen ve farkına yeni varılan bir konu hakkında gerekli eksikliklerin giderilmesi için eğitim faaliyetleri düzenlenmelidir. Teknik personelin istekleri doğrultusunda eğitim faaliyetinin kapsamı genişletilmeli ve sıklık süresi düzenlenmelidir. Yukarıda belirttiğimiz bilinirliği yüksek olan sertifikaların alımı konusunda personele destek olunmalıdır. Yönetim kademesinde rol alan personelin eğitim faaliyetleri de bilgi işlem personelininki gibi ayrıcalıklar içermelidir. Yönetim kademesinin sahip olacağı bilgi güvenliği eğitim konuları tüm personelin aldığı eğitimden farklı olmalıdır.

Son zamanlarda ülkemizde birkaç üniversitede açılan, bilgi güvenliği konusunu temel alan yüksek lisan bölümleri vardır. Bunun yanında sürekli eğitim merkezleri ve kısıtlı kapsamda verilen bilgi güvenliği eğitimleri haricinde müfredatta işlenen bir eğitim konusu mevcut değildir. Bilgi güvenliği alanında verilen eğitimlerin temel eğitim müfredatının içine dâhil edilmesi gereklidir. Lisans düzeyindeki eğitimlerde ise, tüm öğrencileri kapsayacak bir program hazırlanmalıdır.

Bilgi güvenliği denildiğinde, teknik konulardan çok farkındalık yaratıcı eğitimler planlanmalıdır. Özellikle geleceğin yönetici ve liderlerinin yetiştirildiği beşeri bilimler alanında bu konulara özen gösterilmelidir. Bilgi güvenliği kurulumunda üst yönetimin önemini ve liderlik konularının ön plana çıktığını görmüştük. Geleceğin yöneticileri olacak bu öğrencilerin, lisans düzeyindeki eğitimleri esnasında bilgi güvenliği eğitimi almaları gelecekte daha güçlü ve daha etkili sistemlerin kurulmasını sağlayacaktır.

DPT tarafından 2005 yılında "Bilgi Toplumu Stratejisi" başlıklı bir çalışma başlatılmış ve çalışmada bilgi toplumu olma yolunda yapılması gereken somut adımlar belirlenmiştir. "Bilgi Toplumu Stratejisi" nin 88. maddesini "Ulusal Bilgi Sistemleri

Güvenlik Programı" oluşturmaktadır. Sorumluluğu TÜBİTAK-UEKAE' ya verilmiştir. Programın en önemli hedefi başta kamu kurum ve kuruluşları olmak üzere ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamaktır. Pilot olarak seçilen kurumlara ISO 27001'e uygun bilgi güvenliği yönetim sistemi oluşturma konusunda danışmanlık verilmektedir. Çalışmaların hedefi, kurumların ISO 27001 sertifikası alabilecek seviyeye gelmesini sağlamaktır. TÜBİTAK-UEKAE bünyesinde (BOME) Bilgisayar Olaylarına Müdahale Koordinasyon Merkezi kurulmuştur. Bu merkez hem bilgisayar olay müdahale ekibi kurma konusunda kamu kurumlarına danışmanlık vermekte, hem de güvenlik olayları ile ilgili koordinasyon görevini yürütmektedir (Bahşi ve Karabacak, [Tarih yok]:146).

Bilgisayar Olaylarına Müdahale Ekibi Koordinasyon Merkezi (BOME-KM), sorumluluk alanında birden çok kurum veya kuruluş olan ve bu kurum ve kuruluşlar arasında olay müdahale koordinasyonu yapan ekiptir. BOME KM, olay müdahale servisini olay müdahale koordinasyon şeklinde vermektedir. TR-BOME, ülkemizde kurum ve kuruluşlarda BOME'lerin kurulması veya bilgisayar olaylarına müdahale yeteneğinin kazanılması amacıyla eğitimler vermektedir. Bu konuda iki farklı eğitimimiz bulunmaktadır. Bu eğitimler BOME Kurulum ve Yönetim ve Bilgi Sistemleri Olay Müdahale ve Adli Analizdir. BOME Kurulum ve Yönetim eğitiminde güvenlik olayları müdahale konusunun yönetim ve organizasyon tarafı anlatılmaktadır. Eğitimin içeriğinde BOME politikaları, kalite ve servis çerçevesi, olay müdahale süreci ve BOME operasyonel ihtiyaçlar anlatılmaktadır. Internet'te gerçekleşen güvenlik olaylarına müdahale koordinasyonunu sağlamak için CERT Coordination Center (Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi) kurulur (www.bilgiguvenligi.gov.tr (09.04.2014)).

Ülkemizde internet kullanımının hızla yaygınlaşması ile e-devlet ve elektronik bankacılık gibi uygulamaların sayısındaki artış, ulusal ve kişisel bilgi kaynaklarının güvenliğinin sağlanmasını çok daha önemli hale getirmiştir. Siber saldırılar ve siber terörizm olaylarındaki artış da özellikle ulusal bilgi kaynaklarının güvenliğini tehdit eder durumdadır. Bu şartlar bilgisayar olaylarına müdahale ekiplerinin ülke içinde hızla kurulmasını ve işler hale getirilmesini zorunlu kılmaktadır. Bu ihtiyaçtan hareketle, Ulusal Akademik Ağ (UlakNet) bünyesinde güvenlik konularında çalışacak UlakNet Bilgisayar Olaylarına Müdahale Birimi, Ulak-CSIRT kurulmuştur. UlakNet bünyesinde

bilgi güvenliği konusundaki bilincin artırılması, yaşanan bilgisayar güvenlik olayları sayısının azaltılması ve ağın kurulduğu tarihten beri sürdürülen çalışmaların daha koordineli bir hale getirilmesi için UlakNet Bilgisayar Olaylarına Müdahale Birimin kurulmasına karar verilmiştir(Ulak-CSIRT). Ulak-CSIRT' ün ilk aşamadaki sorumlulukları aşağıdaki şekilde tanımlanmıştır:(Soysal vd., [?])

- Ağ genelinde bilgi güvenliği bilincini artırmak,
- Akademik ağa yapılan bilgisayar güvenliğini tehdit edici saldırı sayısını azaltmak,
- Güvenlik ihlali sorumlularını tespit etme aşamasının koordinasyonunu sağlamak,
- Güncel açıkları ve çözümleri hakkında ağa bağlı uçların yöneticilerini bilgilendirmek,
- Bağlı uç yöneticilerine bilgi güvenliği hakkında eğitim vermek,
- Bilgi güvenliğini sağlamak için kullanılacak yöntemler hakkında Türkçe belgeleri sağlamak.

4.3.5. İletişim

Yeni sürümle beraber yedinci bölümün altında karşımıza çıkan bu konun mevcut sürümde bir karşılığı yoktur. Görülen lüzum üzerine bu sürüme eklenen yeni konuların bir tanesidir. Bu bölümde kuruluşun, bilgi güvenliği yönetim sistemleri ile alakalı organizasyon içinden ve dışından iletişime geçme ihtiyaçlarını belirlemesi gerektiğini anlatır. Kimin iletişime geçeceği, kimlerle iletişim kuracağı, ne zaman görüşeceği, neleri görüşmesi gerektiği ve iletişimin zarar görmesi durumunda neler yapılması gerektiği ile ilgili hususların açıklığa kavuşturulmasını anlatır. Mevcut sürümde bu konuların hepsi belirsiz bir şekilde, sahipsiz kalmaktadır.

4.3.6. Performans Değerlendirmesi

Mevcut sürümde de dördüncü maddenin alt kısımlarında yer alan Bgys' nin izlenmesi ve gözden geçirilmesi konusu, yeni sürümde de dokuzuncu bölümde karşımıza çıkmaktadır. Neyin izlenmesi ve ölçülmesi gerektiğini ve bu ölçüm ve

analizde kullanılacak metotları belirlemelidir. İzleme ve ölçme işlemlerinin kim tarafından ne zaman yapılacağını ve ortaya çıkan sonuçların ne zaman analiz edilip, değerlendirileceğini açıklar. Mevcut sürümde bu ifadelerin eksikliği göze çarpmaktadır.

İç denetim mevcut sürümde altıncı madde olarak yer alan bu konu, yeni sürümde dokuzuncu bölümün alt maddesi olarak karşımıza çıkmaktadır. Kuruluşun kendi ihtiyaçlarına ve bilgi güvenliği standardının gereksinimlerine uyup uymadığını kontrol etmek ilk öncelikli denetlenecek konudur. Denetimler yapılırken risk analizleri ve önceki denetimlerin sonuçları dikkate alınmalıdır. Kurum denetçi olarak seçeceği personeli seçerken tarafsız kararlar verebilecek kişiler arasından seçmelidir. Denetim kriterleri ve kapsamı önceden yazılı olarak belirlenmelidir. Denetim sonrasında raporlama yapılarak tespit edilen aksaklıklar ilgililerine bildirilmeli ve raporlar muhafaza altına alınmalıdır. Sorumluluklar, standarda gereksinimlerine, yasal mevzuata uyum ve güvenlik gerekliliklerine uyum kontrol edilmelidir.

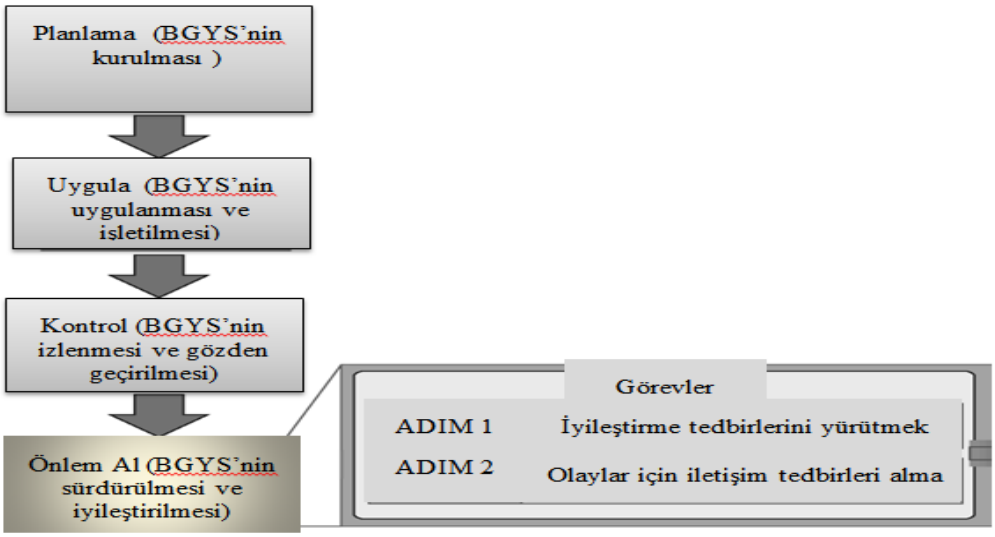
Sistemin iç denetimi kurum çalışanı tarafından yapılması durumunda olması gereken durum, ilgili çalışanın iç denetim eğitimi alması ve bu konuya eğitim sonrasında sistematik olarak yaklaşabilme yeteneğinin kazandırılmış olması gerekmektedir. İç denetim eğitimi ülkemizde verilmekte, bu eğitimi alma imkânı olmayan kurumlarda ise daha önce bilgi güvenliği konusunda uzman olan birinin görevlendirilmesi gerekmektedir. Kuruluş her iki seçenekte de bir İç Denetim Prosedürü oluşturulmalı ve genel manada yapılacaklar sıralanmalıdır (Mete, 2010:99).

Kurumlar kendi içlerinde belli birimleri ve bu konuda yetkin personelini görevlendirip, belli zamanlarda iç güvenlik denetimleri yaptırmalı ve bunun yanı sıra yılda en az iki kez de kurum dışı güvenlik danışmanlık firmalarından dış denetim hizmeti almalıdır (Eminağaoğlu ve Gökşen, 2009:8). Tetkik konusunda daha fazla bilgiye sahip olmak isteyenler için ISO 27001 BGYS İç tetkik eğitimi faaliyetlerine katılmalarının yararlı olacağı değerlendirilmektedir. Ayrıca TSE GUIDE13268-4 BGYS kontrol ve denetimleri için faydalı bir kaynaktır.

Yönetimin gözden geçirmesi mevcut sürümde yedinci maddenin tamamını kapsayan bu konu, yeni sürümde dokuzuncu bölümün alt kısmında yer almaktadır. Üst yönetim planlanan zaman aralıklarında bilgi güvenliği sisteminin devamlılığını,

yeterliliğini ve etkinliğini gözden geçirmelidir. BGYS de oluşacak iç ve dış konulardaki değişiklikleri, önceki yönetimin gözden geçirdiği konuların sonuçları değerlendirilir.

İzleme ve ölçmenin sonuçları, uygunsuzluk ve düzeltici faaliyetler, denetimlerin sonuçları bilgi güvenliği performansının geri beslemelerinde yer alması gereken eğilimlerdir. Yönetimin gözden geçirmesi, iş sürekliliğindeki fırsatları ve her türlü değişen ihtiyacın karşılanması amacıyla yürütülmelidir. Gözden geçirme faaliyeti yürütülürken ilgili taraflardan gelen geri beslemeler ve risk değerlendirme ve risk tedavi planının sonuçları da değerlendirmeye alınmalıdır. Gözden geçirme sonucunda kayıtlar tutularak, iyileştirme önerileri sunulacaktır.



Şekil 19: BGYS Kurulumunda Yapılması Gereken Görevler (Önlem Al Aşamaları**)**

Kaynak: ISO 27999 Standardı.

4.3.7. İyileştirme

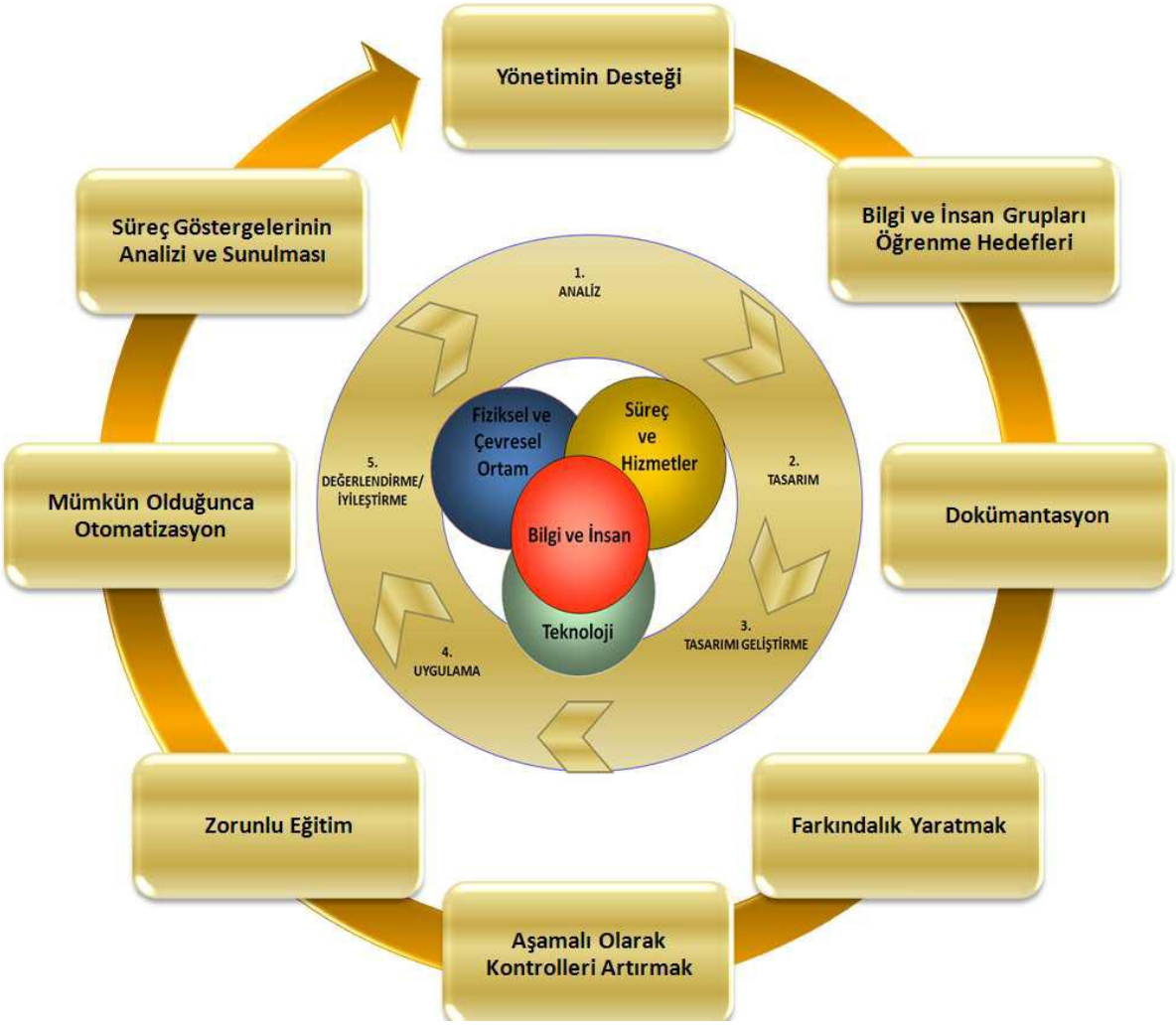
Mevcut sürümde sekizinci madde de yer alan iyileştirme faaliyetleri, yeni sürümde de en son bölüm olan onuncu madde de yer almaktadır. Herhangi bir uygunsuzluk ortaya çıktığında ilk olarak tepki verilmelidir ve düzeltmeye gidilmelidir. Oluşacak sonuçlar dikkate alınmalıdır. Uygunsuzluğun yeniden doğmaması ve başka bir yerde yeni bir uygunsuzluk oluşmaması için uygunsuzluklar gözden geçirilmeli, uygunsuzluğun sebepleri bilinmeli, mevcut ve potansiyel uygunsuzluklar belirlenmelidir.

BGYS'nin iyileştirilmesi için kurum tarafından önleyici ve düzeltici tedbirler alınması gereklidir. Olumsuzlukların yaşanmaması için, risk değerlendirme sonuçlarına bağlı olarak değişen riskler bazında önleyici tedbirler alınmalıdır. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. BGYS gereksinimleriyle olumsuzlukları gidermek üzere düzeltici önlemler alınmalıdır. Önleyici tedbirler için gerçekleştirilen faaliyetler çoğunlukla düzenleyici tedbirler için gerçekleştirilen faaliyetlerden daha az maliyetlidir (Vural ve Sağıroğlu, 2008:515).

Bilgi güvenliği yönetim sisteminde gerekli değişiklikler yapılmalı ve düzeltici faaliyetler için yapılacak faaliyetlere başlanmalıdır. Uygunsuzluğun ve yapılan işlemlerin içeriği organizasyon tarafından doküman halde bulundurulmalıdır. Bilgi güvenliği sisteminin uygunluğunun, yeterliliğinin ve etkinliğinin devamlı sürdürülebilmesi için kuruluş gerekli tedbirleri almalıdır. Unutmamalıdır ki bir sistemi kurmak kadar o sistemin devamlılığını sağlamakta önemlidir. Yapmış olduğumuz mülakatlar esnasında, bilgi işlem personelinden aldığımız düzeltici ve önleyici faaliyetler raporlarını sizlere ekler bölümünde sunduk. Sertifika almaya hak kazanmış BGYS sahibi kurumlardan alınan bu örneklerin sizler için daha etkili olacağını düşünmekteyiz.

İşletmeler, önleyici faaliyetlerde yazılı hale getirilmiş prosedür için, olası uyumsuzlukları ve bunların nedenlerini belirlemek, ihtiyaç duyulan önleyici faaliyetleri belirlemek ve gerçekleştirmek, gerçekleştirilen faaliyetlerin sonuçlarını kaydetmek, gerçekleştirilen önleyici faaliyetleri gözden geçirmek, değişen riskleri tanımlamak ve dikkatin önemli derecede değişen riskler üzerinde yoğunlaştıracak önleyici faaliyet gereksinimlerini kapsamalıdır (TS-ISO/IEC 27001, 2006:2-10).

Necla Vardal üniversiteler üzerinde yaptığı doktora çalışmasında; bilgi güvenliği konusunda insan ve eğitimin rolünü vurgulayarak örnek bir BGYS modeli hazırlamıştır. Bu modelde en dışta yer alan kısım, modelin etkili olarak uygulanmasında sürekli iyileştirme ilkesi ile tekrarlayan süreç adımları için kritik noktaları ve başarı için ipuçlarını belirtmektedir. Aşağıdaki şekilde örnek BGYS modeli sunulmuştur (Vardal, 2009:148).



Şekil 20: ÖBGYS Modeli Bileşenleri, Süreç Adımları ve İpuçları

Kaynak: Vardal, 2009:126.

BEŞİNCİ BÖLÜM

ARAŞTIRMA METODOLİJİSİ VE ISO27001 BGYS SERTİFİKASI HAKKINDA YAPILAN MÜLAKATLAR

5.1. ARAŞTIRMANIN KONUSU

Ülkemizdeki kurum ve kuruluşların bilgi güvenliği yönetim sistemleri konusundaki farkındalıkları ve bilgi güvenliği yönetim sistemleri ile ilgili yapılan çalışmaların hangi düzeyde olduğunu saptamaktır.

Bilgi güvenliği yönetim sistemleri ile ilgili uluslararası kabul görmüş standartların bilinilirliği ve bu standartların kuruluşlarda uygulanması ile ilgili süreç çalışmaları incelenmiştir.

Standartların kuruluşlar tarafından doğru bir şekilde uygulandığının ispatı olarak, alınan bilgi güvenliği yönetim sistemleri sertifikalarının gereklilikleri ve yapılması gerekenler incelenmiştir.

5.2. ARAŞTIRMANIN AMACI

Bilgi güvenliği konusunda ülkemizdeki kurum ve kuruluşların uluslararası standartlarla tescil ettikleri çalışmalarını irdeleyerek, bu alanda yapılmış olan karşımıza çıkan az sayıdaki akademik çalışma verilerine reel örnekler vererek daha anlaşılabilir bir perspektif kazandırmaktır. Kuruluşlara ve araştırmacılara bilgi güvenliği kurulumu hakkında yardımcı olabilecek yöntem ve teknikleri yalın bir dille, yaşanmış tecrübelere dayalı olarak sunup, bu konuda araştırma yapacak olan kişi ve kurumları cesaretlendirerek rehber olma amacı güdülmüştür.

Bu araştırmada güdülen asıl amaç; BGYS kurmak isteyen kurum ve firmalara akademik anlamda yapılan bir çalışmayla, yaşanmış örnekler vererek anlaşılması kolay, cesaret verici bir yol haritası çizmektir. Bilgi güvenliği konusunun bireyden başladığını hatırlatarak, eğitim sistemimizin içinde bilgi güvenliğine olan ihtiyaç vurgulanmıştır.

5.3. ARAŞTIRMANIN KAPSAMI

Araştırmanın evreni, ülkemizdeki ISO27001 bilgi güvenliği yönetim sistemi sertifikasına sahip 132 kuruluştur. Araştırmamız esnasında sertifika sahibi kuruluşların isimlerine ulaşmak için çaba harcadık. Sertifika sahibi kuruluşlardan otuz civarındakilerinin isimlerine basın yayın organlarında çıkan sertifika haberleri vasıtasıyla ulaştık. Bu kuruluşlara elektronik posta yoluyla mülakat yapma isteklerimizi sunduk. Çoğu kuruluştan cevap gelmedi. Cevap veren kuruluşlarda bilgi güvenliği yönetim sistemleri konusunun kurumları için gizli bilgiler içerdiğini ve görüşme yapamayacaklarını bildirdiler. Sadece sertifika sahibi iki kuruluş bize olumlu cevap verdi. Bizde araştırmamızı bu iki kuruluşla gerçekleştirdik.

5.4. ARAŞTIRMANIN SINIRLILIKLARI

Bilgi güvenliği konusu başlı başına gizlilik gerektiren bir temel üzerine kurulduğu için araştırma yapılırken mülakat yapılabilecek kuruluş bulunamaması bizleri araştırmamız esnasında bizi kısıtlayan en büyük husus olmuştur.

Bilgi güvenliği konusunda yapılan çalışmaların çoğunluğu piyasada yer alan danışmanlık ve eğitim firmaları aracılığıyla yapılıyor olması, sertifika sahibi birçok kuruluşun konu hakkında çok fazla bilgi sahibi olmamasına ve bizlerin mülakat taleplerini olumsuz yönde karşılamalarına sebep olmuştur.

Bilgi güvenliği konusunda sertifika sahibi birçok kuruluşun büyük ölçekli organizasyon yapılarına sahip olmaları, mülakat için bizlere zaman ayıramama sorununu da beraberinde getirmiştir.

Yapılacak olan araştırmanın belirli bir zaman dilimi içerisinde yapılıyor olması da bizi zor duruma sokmuştur.

Sertifika sahibi kuruluşların sayısının ülkemizde çok az olması bizi zor durumda bırakmıştır.

Bu konuda yapılan akademik alandaki çalışmaların yetersizliği de bizleri zor durumda bırakmıştır.

5.5. ARAŞTIRMANIN YÖNTEMİ

Araştırmamız esnasında toplanan veriler yüz yüze kişisel görüşme ile sağlanmıştır. Araştırmamız esnasında az sayıda var olan araştırmalarında belirli sorular ve anketler üzerinde döndüğünü gördük. BGYS kurulumu ile verilen örneklerin hayali bir kurum yaratılarak araştırmacılar tarafından ortaya konulduğunu ve bu durumunda insanların çok fazla dikkatini çekmediğini ve cesaretlendirmediğini görülmüştür.

Biz de araştırmamızda bu eksikliği fark ederek sertifika sahibi, süreci yaşamış kurumlar üzerinde çalışarak, bu süreci daha anlaşılabilir hale getirmek istedik. Belge sahibi birçok firma ile yazışmalar yapıldıysa da birçoğundan olumsuz cevap vermek için dahi geri dönüş olmadı. İlk olarak Pendik Belediyesi, ardından Keçiören Belediyesi bizimle mülakat yapmayı kabul etti. Yapılan mülakatlar neticesinde her iki kurumunda BGYS sürecinde danışman firmaların büyük rol oynadıkları ortaya çıktı.

Pendik Belediyesi ile yapılan görüşme sonucunda bizim BGYS hakkındaki düşüncelerimiz daha da zenginleşti. İnternet ortamından ve kısıtlı sayıdaki akademik çalışmadan öğrendiğimiz BGYS konularına farklı bir bakış açısıyla bakmamızı sağladı. Yapılan mülakatta öğrendiklerimiz bizi daha fazla öğrenme daha farklı renkleri keşfetmeye itti. Yeni mülakat yapma ihtiyaçları doğdu. En az iki kuruluşla mülakat yapılması sonucunda daha objektif bir sonuç ortaya koyabileceğimizi düşündük ve yeni bir mülakat yapabilmek için başvurulara başladık. Keçiören Belediyesi bizim mülakat talebimizi kabul etti ve görüşmeler tamamlandı. İki görüşme esnasında da dikkatimizi çeken konu danışmanlık ve eğitim firmalarının BGYS sürecindeki rolleri oldu.

Belediyelerle yarı biçimsel mülakat tekniğini uygulayarak; önceden hazırlamış olduğumuz soruları bilgi işlem personeline sorarak ve mülakat esnasında gelişen yeni konulara da cevaplar bularak araştırmada bulunduk.

Yapılan bu mülakatlarla araştırmamızı, bu zamana kadar yapılan çalışmalardan çok farklı bakış açılarıyla şekillendirerek sonlandırmış olduk. Yapılan mülakatlara yorum katmadan sizlere sunmayı daha doğru bulduk.

5.6. ARAŞTIRMANIN KISITLARI VE GELECEK ARAŞTIRMALAR İÇİN ÖNERİLEN KONULAR

Araştırmamızda, mülakat yaptığımız kuruluşların her ikisinde de bilgi işlem personeli görüşmeler yapılmıştır. Yapılan çalışma bilgi işlem personeli tarafından nasıl algılanmakta ve bilgi işlem biriminin süreç içindeki rolleri ağırlıkla ele alınmıştır.

Bilgi güvenliği yönetim sistemleri kurulumu kararı, bir organizasyonda stratejik kararlar neticesinde ortaya çıkmalıdır. Bu karar alt kademeden gelen teklifler neticesinde, üst yönetim kurulu tarafından verilmelidir. Mülakat esnasında üst yönetim personelinin görüşlerinin alınması daha verimli bir çalışma doğurabilecektir.

Alt kademede yer alan personelin bu süreci nasıl algıladığı, kabul süreci ve almış olduğu bilgi güvenliği eğitimlerine adaptasyonları daha ayrıntılı bir şekilde incelenebilir.

Mülakat yapılan her iki kuruluşunda Belediye olması, yapılan mülakatın diğer kuruluşlara göre farklılıklar göstermesine sebep olabilir.

Sertifika sahibi kuruluşların sertifika süresi boyunca akredite kuruluşlara karşı sorumlu olmaları ve denetimlere açık olmaları sebebiyle, bazı konularda yapılan yanlışların bize mülakat esnasında aksettirilmemesine sebep olabilir.

Araştırmanın sonucunda, gelecek araştırmalara konu olabilecek bazı ilgi çekici alanlara ulaşılmıştır. Bunlardan bazıları:

- Bilgi güvenliği yönetim sistemi kurulum sürecinin çalışanlar üzerindeki etkileri
- Bilgi güvenliği yönetim sistemi kurulum sürecinde üst yönetim kademesinin sorumluluk ve yetkileri
- Bilgi güvenliği yönetim sisteminin organizasyon içindeki kabul süreci
- Bilgi güvenliği eğitimleri
- Bilgi güvenliğinin teknik personeli ilgilendiren hususları
- Bilgi güvenliği sertifika alım süreci
- Bilgi güvenliği denetimleri
- Bilgi güvenliği sertifikalarının yenilenmesi
- Farklı alanda faaliyet gösteren iki kuruluşun BGYS süreçlerinin incelenmesi

- Çalışan sayısının BGYS kurulumu üzerine etkileri incelenebilir.

5.7. PENDİK BELEDİYESİ İLE BGYS SÜRECİ HAKKINDA YAPILAN MÜLAKAT

Ülkemizde tespit ettiğimiz belge sahibi kuruluşlara, elektronik posta yolluyla iletişime geçmeye çalıştık. Yüksek lisans tez çalışması hazırladığımızı ve kurumla bilgi güvenliği sertifikası alma süreçleri ile ilgili mülakat yapmak istediğimizi belirttik. Çoğu kuruluştan bize herhangi bir geri dönüş olmadı. Bazı kuruluşlarda elektronik posta yoluyla bilgi güvenliği ile ilgili konuların gizli bilgiler içerdiği için, bizimle herhangi bir şey paylaşmalarının uygun olmayacağından bahsettiler. Pendik belediyesi Bilgi İşlem Müdürü Necip ARSLAN bizi telefonla arayarak aynı hususları belirterek, bilgi güvenliği ile ilgili hususları paylaşamayacaklarını anlattı. Telefon görüşmemiz esnasında bizim ilgilendiğimiz konuların; BGYS kurulum sürecinde yaşanan zorluklar ve alınması gereken dersler olduğunu belirttik ve o da bize telefon numarasını vererek, bizi görüşmek için Pendik Belediyesine davet etti. Mülakat yapmak için Pendik Belediyesi ek binası Bilgi İşlem Müdürlüğü'ne gidildi ve burada görüşmeler yapıldı. Yapılan görüşme sonunda bize elektronik ortamda ve basılı olarak bilgi güvenliği ile ilgili materyaller verdiler. Bize bu akademik çalışmamızda destek oldukları için tüm bilgi işlem personeline teşekkür ederek ayrıldık.

Yapılan mülakat esnasında geçen kurum veya kuruluş kelimeleri Pendik Belediyesini, birim kelimesi Bilgi işlem Müdürlüğünü kapsar. Bu kuruluş ile yaptığımız görüşmeler, yarı biçimsel mülakat tekniği kullanılarak gerçekleştirilmiştir. Görüşmeden önce hazırlamış olduğumuz bir soru grubu mevcuttur. Görüşmecini cevaplarına göre o anda yeni sorular aklımızda canlandı ve sorulara da yanıt arama ihtiyacı duyduk. Sadece hazırlamış olduğumuz soru kalıplarına bağlı kalınmamıştır. Yapılan bu çalışmayı diğer araştırmalardan farklı kılan en önemli özellik, birebir yüz yüze mülakat tekniği ile açık uçlu sorularla daha ayrıntılı ve farklı soruların cevaplarını, süreci birebir yaşamış kişilerle görüşülerek oluşturulmuş olmasıdır. Mülakat yapacağımız esnada Bilgi işlem müdürü Necip Bey'in farklı bir görüşmesi olduğu için, onu beklerken süreci yakından takip eden tecrübeli bilgi işlem personelleriyle bir ön görüşme yapma imkânımız oldu. Yapılan bu ön görüşme, asıl mülakat öncesinde yapılması bizim için çok faydalı oldu.

Bilgi işlem müdürü diğer görüşmelerini bitirdiği zaman kendisiyle mülakat yapma fırsatı bulduk. Kısa süre önce kurum personelinden öğrendiğimiz konuların üzerinden bir kez daha geçerek ve ön görüşme esnasında vurgulanan konular üzerine yoğunlaşarak mülakatın daha verimli hale geldiği gözlemlenmiştir. Mülakat sonunda, alınan ISO27001 BGYS sertifikası(dijital ortamda), DÖF formları(3 adet dijital ortamda), TS ISO/IEC27001 BGYS gereksinimleri standartları (basılı olarak, üzerinde çok fazla notlar mevcut çalışma yapılmış) ve uygunsuzluk alıştırmaları örneği(basılı halde üzerinde yapılan çalışmalar mevcut) bilgi işlem müdürü tarafından çalışmalarımıza yardımcı olması için bize verilmiştir. Bu kaynaklardan bazılarını ekler kısmında bulabilirsiniz.

- **İyi günler Necip Bey, öncelikle bize BGYS kurma kararınızı nasıl aldığınızı anlatır mısınız?**
- Bilgi işlem birimi olarak birinci önceliğimiz kurumun bilgi güvenliğini sağlamaktır. Bizler zaten bu sertifikayı almadan öncede bilgi güvenliği konusunda gerekli tedbirleri alarak kurumumuzun her zaman tehditlere karşı korunmasını sağlıyorduk. Bu sertifikayı alarak bunu geliştirmiş ve belgelendirmiş olduk.
- **ISO27001 BGYS sertifikası alma kararı nasıl ortaya çıktı?**
- Biz birim olarak yeni projelerle ve teknolojik yeniliklerle her zaman ilgileniriz. Bu sertifikada takip ettiğimiz bir hususdu. Bu konuda araştırmalar yapmıştık. Belediyemiz imar süreçlerini iyileştirme için bir proje yürütmeye başladı. Bu süreçte Dünya Bankası kredilerinden faydalanıyorduk. Bizimde böyle bir sertifika almaya ihtiyacımız olduğunu belirttik ve Belediyemiz tarafından uygun görüldü ve bu kredilerle ISO27001 sertifikası alma süreci başlamış oldu.
- **Bu sürece ilk olarak nasıl başladınız?**
- İlk olarak bu sertifikanın nasıl alındığını araştırdık ve bir danışman firma olmadan bu sürecin işlemesinin çok zor olacağı kanısına vardık. Bir piyasa araştırma sürecimiz başladı, ardından danışmanlık ve eğitim hizmeti verecek firmayı belirledik. Natek iletişim danışmanlık ve eğitim firması ile bu sürece başlamış olduk. Bizimle beraber aynı firma danışmanlığında Bağcılar Belediyesi de böyle bir proje yürütmeye başladı.
- **BGYS kurulumuna ilk hangi konulardan nasıl başladınız?**

- İlk olarak tüm kurumu kapsayacak şekilde, üst yönetim kademesiyle beraber bu sürecin başlaması gerektiğinin kararını aldık ve danışman firmayı kurumumuza davet ettik. Firma yetkilileri ile bizim birimdeki arkadaşlar beraber kurumun varlık envanterini çıkardılar. Kurumun sahip olduğu değerleri en küçük ayrıntısına kadar hesaplayıp, yazılı halde kayıt altına aldık.
- **Bize hazırladığınız varlık envanterinden bir örnek nüsha verebilir misiniz?**
- Hayır. Bu kesinlikle yapılamaması gerekir. Varlık envanteriyle kurumda bulunan her şeyi kayıt altına almış oluyoruz. Bu belgenin başka birinin eline geçmesi demek bizim bütün sahip olduğumuz değerleri bilmesi ve bunları hesaba katarak bize rahatlıkla bir saldırıda bulunmasını sağlar. Bu envanterin gizlilik içerisinde saklanması ve açığa çıkmaması gerekir.
- **Süreç ne kadar sürdü?**
- Yaklaşık olarak bir yıl sürdü. 2009 yılının eylül ayında başladık. 2010 yılının ekim ayında sertifikamızı aldık.
- **BGYS kurulum süreci nasıl ilerledi?**
- Varlık envanterini oluşturduk, ardından BGYS'nin evreleri sırasıyla uygulanmaya başlanmıştır. Planlama, uygulama, kontrol etme ve önlem alma. PUKÖ döngüsü dediğimiz işleyiş şekli budur. Genel olarak tüm evrelerde bu metot kullanılır. Bizde ilk olarak planlamayla başladık. Bu safhada öncelikle bilgi güvenliği komitesi ve bilgi güvenliği sorumlusu personelleri belirledik. BGYS kapsamını belirledik, risk değerlendirmelerini yapmaya başladık. Tehditler açıklılar ve etkinliklerin listesini çıkarttık. Bunların iş üzerine etkilerini çıkartıp, rapor haline getirdik. Kontrol listelerini seçtik, oluşan artık riskleri gözden geçirdik ve bilgi güvenliği sistemini onaylayarak uygulanmasına karar verdik. BGYS'ni uygulamaya başladıktan sonra çıkan hataları da görerek düzeltmelere de giderek gelişimini sağladık. Aylık raporlarda hazırlayarak kontrollerimiz devam ettirdik. Bağımsız kurum dışından da testler yapıldı, farklı senaryolar ortaya konarak farklı zamanlarda ne gibi tepkiler verdiğimizi kontrol ettiler. Bu gelişmelerden sonra kendimizi hazır hissettiğimiz zaman belgelendirme kuruluşunu davet ettik ve onlar denetimlerini yaptılar. Sonunda belge almaya hazır olduğumuz görüldü ve belgelendirme kuruluşu tarafından adımıza ISO27001 belgesi hazırlandı.

- **Siz süreci birebir yaşayarak öğrendiğiniz için bir yıllık süreyi biraz hızlı geçtik. İsterseniz daha önce bu süreci hiç yaşamış kişi ve kuruluşlara örnek olması adına bir yıl süren bu projeyi daha ayrıntılı ve daha anlaşılır hale getirelim. Kısa sorularla aşamaları ayrıntılı bir şekilde açıklayalım. Kurumunuz danışmanlık ve eğitim firması ile ilgili ortak yürüttüğü çalışmalara nasıl başladığınızı anlatarak baştan alalım mı?**
- Biz kurum içinde BGYS kurma aldıktan sonra danışmanlık firmasını davet ettik ve onlarda Belediye binasına gelerek faaliyetlerimize başladık. Aramızda alacağımız hizmetlerle ilgili bir anlaşma imzaladık. Yapılan anlaşmada verilecek eğitimlerin süresi kapsamları, denetimler, ayrıntılı olarak yer alıyordu.
- **Eğitim faaliyetlerinden de bize biraz bahsedebilir misiniz? Katılımlar nasıldı?**
- Öncelikle danışmanlık firması ile eğitim takvimi oluşturduk. Bizim ve onların uygun olduğu günler hesap edilerek esnek bir eğitim takvimi oluşturduk. Eğitim konuları, yer ve zaman kararlaştırıldı. Eğitimlerdeki temel amaç tüm personel için bilgi güvenliği farkındalığı yaratmaktır. Biz tüm personele verdiğimiz temel bilgi güvenliği eğitimlerini her yıl tekrarlayarak devam etmekteyiz. Sertifika aldıktan sonra bile yıllık eğitim faaliyetlerine devam etmeniz gereklidir. Çünkü bilgi güvenliğini korumak için eğitimle oluşturduğumuz farkındalığı korumak gerekir. Danışman firma yetkilileri tarafından yapılan temel eğitimlere katılımlar yüksek düzeydeydi. Bunun yanında bilgi işlem personeli için farklı alanlarda teknik eğitimler verildi ve herhangi bir ihtiyaç duyduğumuzda bilgi işlem personeli için eğitim vermeye devam ediyoruz. Danışmanlık firması ile beraber ortak yaptığımız anketlerle personelin bilgi ve ilgi düzeyini ölçmekteyiz. Bütün çalışanları kapsayan ve sadece bilgi işlem personelini kapsayan anket çalışmalarımız olmaktadır.
- **Bilgi işlem personeline ISO27001 bilgi güvenliği yönetim sistemleri kapsamında ne gibi eğitimler veriyorsunuz?**
- Bu kapsamda bizim bilgi güvenliği personelimize eğitim verme durumumuz söz konusu değildir. Biz personelimize profesyonel anlamda eğitim veren kurumlarda eğitim imkânı sağlıyoruz. Bilgi işlem birimi içinden seçtiğimiz personelimizden bazılarını ISO27001 Bilgi güvenliği yönetim sistemi iç tetkik eğitimi almasını

sağlıyoruz. Bu personelimizin de iç tetkik sertifikasını almasını sağlıyoruz. Bu eğitimleri ilerleyen günlerde de desteklemeye devam edeceğiz. Size personelimizin aldığı ISO27001 BGYS iç tetkikçi eğitiminin kitapçıklarından da verelim. Yararlanacağınız bir kaynak olur hem de eğitimlerle ilgili size farklı bir bakış kazandırır.

- **Aldığınız danışmanlık, eğitim ve denetim hizmetleri için ne kadar bir ücret ödediniz?**
- Tam olarak bir bilgimiz yok. Zaten dünya bankası fonlarından bir kaynak sağladığımız için bize her hangi ek bir masraf oluşturmadı.
- **Hangi danışmanlık firması ile beraber çalıştınız?**
- Ankara merkezli bir firmaydı. Adı Natek iletişimdi.
- **BGYS kurulumunda yararlandığınız kaynaklar nelerdir?**
- Genellikle destekçi firmanın kaynaklarından yararlandık. Bununla beraber TSE tarafından hazırlanan standartlar dokümanlarından faydalandık.
- **BGYS kurum çalışanları dışında kimlerle etkileşim içindedir?**
- Bizim kurumumuz bir belediye olduğu için öncelikle bizim hizmet sunduğumuz vatandaşlarımızı etkilemektedir. BGYS güvenilirliği, ulaşılabilirliği ve bütünlüğü verdiğimiz hizmetin kalitesini gösterir. Bunun yanında biz ISO27001 standartlarına göre bir BGYS kurmak istediğimizde işin içine bizim hizmet aldığımız kuruluşlarda giriyor. Bir firmadan yazılım alıyoruz, diğer firmadan yazıcı alıyoruz başka cihazlar alıyoruz. Bunların hepsi bizim BGYS' ni etkileyen faktörlerdir. Herhangi birinde oluşacak bir hata bizim BGYS etkiler. Bunun için biz kurum dışından da iletişim halinde olduğumuz, bilgi ve bilgi teknolojileri satı aldığımız kişi ve kuruluşlarla da mevcut yazılı politikalar oluşturup, çalışmalarımızı gizlilik içinde yürütürüz.
- **BGYS sadece bilgi işlem personeli ile mi yürütülmektedir?**
- Bilgi güvenliğinin sadece bilgi işlemcilerin yapacağı teknik bir sistem olduğunu düşünmek yanlış olur. Ama şu da bir gerçek bilgi işlem personelinin asıl sorumluluğu budur. BGYS takımını bilgi işlem personeli oluşturur. BGYS denildiği zaman üst yönetim kademesinin de onayı alınarak tüm çalışanların farkındalık yaratılarak sürece dâhil edildiği bir oluşum vardır. Bireysel her kullanıcı öncelikle kendi bilgi güvenliğini korumak zorundadır. Bununla ilgili

belirlenen politikalar yazılı olarak tüm çalışanlara tebliğ edilir. Bunun yanında her birimden kendi ihtiyaçlarını belirleyen ve bilgi işlem personeliyle ortak çalışmaları yürüten birer personel belirlenir ve bilgi güvenliği komitesine dâhil edilir. Bu personel bilgi işlemden gelen gelişmeleri kendi birimine aktarır. Aynı şekilde kendi biriminin ihtiyacı olan yetki, sorumluluk, yazılım, erişim hakkı gibi istekleri bize iletir. Örneğin tapuda çalışan arkadaşların bir yazılıma ihtiyacı olabilir. Bunu bize bildirdikleri durumda bizde inceleyip, ihtiyaçlara göre yeni yazılım yükleyebilip, kullanıcılara yetki verebiliriz.

- **BGYS içinde yer alan roller ve sorumluluklar bunumu içerir?**
- Roller ve sorumluluklar daha ayrıntılı bir bölümdür. Tüm kullanıcıları rolleri ve sorumlulukları vardır. Bilgi işlem personelini ilgilendiren hususlar daha çok olduğu için BGYS içindeki sorumlulukları da daha fazladır. Sahip olunan her varlık için bakım, işletme ve kullanım gibi hususlarda kime ne gibi roller ve sorumluluklar düştüğü belirtilir. Yazılı halde birim sorumlusu tarafından onaylandıktan sonra tüm personele tebliğ edilir. Bu aşamadan sonra her personel BGYS içinde ne yapıp, ne yapmaması gerektiğini bilir. Sorumlulukların başında da ilk olarak bilgi işlem yöneticisi seçilir. Bu yöneticide bilgi işlem ile ilgili tüm faaliyetleri yürütmekten sorumludur. Tabi bunları yapmadan önce kurumun sahip olduğu tüm varlıklarını belirlemeniz ve sınıflandırmanız gerekir.
- **Varlıklar belirlenirken dikkat edilmesi gereken hususlar nelerdir?**
- Varlık, kurumunuz için değeri olan her şeydir. İlk başta varlıkları belirlerken önem derecelerine göre hareket etmek gerekir. Oluşturduğumuz varlık envanterinde sınıflandırma da yapmamız gerekir. Kurum için önem dereceleri belirlenip, etiketleme yaparak varlıkları belirlememiz gerekir. Bu envanteri titizlikle oluşturma sebebimiz, diğer aşamaların hepsine etki edeceği içindir. Varlık envanteri doğru bir şekilde hazırlanmazsa; prosedürler, politikalar, roller ve sorumluluklar hepsi yanlış hazırlanır ve bütün BGYS'nin yeniden hazırlanmasını gerektirebilir. İşe etki yapan analizleri de hazırlarken yine varlık envanterinin önemi ortaya çıkar.
- **İş etkisi analizi dediğimiz hususlar neyi içerir, neye göre yapılır? Örnek verebilir misiniz?**

- İş etki analizi dediğimizde envanterdeki varlıkların, işlevini yerine getirememesi sonucunda oluşacak kayıpları, etki ettiği birimleri, kapsamlarını ve bizim bu aksaklığı ne kadar süre için olağan gördüğümüzü anlatan tablodur. Örneğin varlık olarak kurumun web sayfası çalışmazsa kim etkilenir, kurum çalışanları ve kurumun web sayfasını kullanan herkes, ne kadar süre çalışmasa kabul edilebilir iki-üç saat denilebilir. En fazla ne kadar süre çalışmaması kabul edilir, en fazla iki gün içinde yeniden kullanıma geçmesi gerekir. Bu şekilde kurum varlıklarının işe olan etkisi hesaplanır ve yazılı hale getirilir. Sorumlu olan kişiler ona göre tedbirini alır ve iş yaşantısının sürekliliği sağlanır.
- **Kurum personeli BGYS kurulmasına nasıl bakıyor, herhangi bir tepkileri oluyor mu?**
- Kurum çalışanları ilk etapta tam olarak BGYS kurmanın kurum için faydalarını anlayamamıştı. Sonuçta yeni bir sistem, sorumluluklar, oluşturulan yazılı politikalar bunların hepsi her kurumda çalışanlar için gereksiz, fazladan ayrıntı olarak görülebilir. Eğitimlere katılmak kişilere zorda gelebilir. Fakat bilgi güvenliği farkındalığı eğitimlerden sonra katılan personel BGYS kurulumunun önemini daha iyi anlıyor. Sadece kurum içinde değil özel hayatlarında da bilgi güvenliği konusunun önemli olduğunun farkına varıyorlar.
- **Risk yönetimi tabanlı bir standart için risk değerlendirme, risk işleme gibi konular galiba biraz daha ayrıntılı anlatılması gerekir. Bize standarttın risk konularını içeren bölümlerini anlatır mısınız?**
- Aslında bu standart baştan sona risk konularını kapsıyor. Varlık envanteri çıkarıldıktan sonra her varlık için açıklıklar, tehditler ve etkinlikler belirlenir. Sonra bu tehditlerin olabilme ihtimalleri, tehditlerin gerçekleşmesi sonucu oluşacak etkiler ve bunların değerlendirmesi sonucunda riskin ne olduğu ve riskin önem derecesi ortaya çıkar. Risk için ne gibi tedbirler alındığı ve uygulanabilir mi değil mi belirtilmesini kapsar. Siz bu riskleri ne zaman içinde değerlendirip, risk olmaktan çıkaracaksınız. Yâda bu riski kabul edip herhangi bir işlem yapmayacağınızı belirtirsiniz. Bu çalışmanın hepsini yazılı hale getirirsiniz ve risk analizi oluşturulmuş olur.
- **Politikalar ve prosedürler neleri kapsıyordu nasıl bir sistemle bunları hazırladınız?**

- Öncelikle bilgi güvenliği politikası hazırlanır. İçerisinde bilgi güvenliğinin tanımı, kapsamı, amacından başlayarak, varlıklardan, rollerden, sorumluluklardan, fiziki güvenlik tedbirlerinden, personel güvenliğinden, üçüncü şahısların sistemle olan ilişkilerinden, erişimle ilgili yetkiler ve ayrıntılardan oluşur. Bu saydığımız alt maddeler içinse ayrıntılı prosedürler hazırlanır. Bilgi güvenliği politikası hazırlanıp, kurum amiri tarafından sonra onaylandıktan sonra çalışanlara duyurulur ve uygulanmaya başlanır.
- **ISO27001 standartlarının hepsini birebir uygulamamız gerekir mi?**
- ISO27001 standardının kontrol maddelerinden bazıları uygulanmayabilir. Uygulanabilirlik bölümünde bunların kullanılmayacağı da belirtilmesi gerekir.
- **Kontroller nasıl yapıldı ve kontroller bittikten sonra ne olur?**
- Öncelikle kurum içinde kendimizin yaptığı iç denetimler oldu. Ardından danışmanlık firması çalışanları ve bağımsız firma denetleyicileri ile denetlemeler yapıldı. Standarttın ekinde yer alan kontrol maddeleri vardı. Bu maddeler yazılı hale getirilerek kontrollerin yapıldığı kayıt altına alınmalıdır. Sonra belgelendirme kuruluşunun çalışanları geliyor ve onlarda kontrollerini yapıyorlar. Eğer eksikler görürlerse bununla ilgili belgeler düzenleniyor ve bize düzeltmek için zaman tanılıyor. Bu eksikler için DÖF belgeleri düzenliyoruz.
- **Sizde belgelendirme kuruluşunun kontrollerinde her hangi bir eksiklikle karşılaştınız mı? Bize DÖF belgeleriyle ilgili örnekler verebilir misiniz?**
- Kontroller esnasında bizimde yanlış yaptığımız birkaç husus olduğu ortaya çıktı. Bunlarla ilgili bizde DÖF belgeleri düzenledik. Majör olan kusurlar yeniden değerlendirilerek, tekrar kontrolden geçirildi. Hatalar giderilirse belge almaya hak kazanırız. Eğer DÖF belgelerinde tespit edilen hatalar minör hatalar ise zaten bir daha kontrollere gerek yoktur. Belge almamıza engel oluşturan her hangi bir husus yoktur. Sadece bizim eksiklerimizin farkında olmamız için ortaya konulur. Size örnek oluşturması için birkaç bilgiyi eksilterek birkaç DÖF belgesi verelim.(Ekler bölümünde bu belgeleri bulabilirsiniz. Bize verilen bütün DÖF örnekleri minör kusurları içermektedir.)
- **Danışmanlık ve eğitim firmasıyla çalışmak bir zorunluluk mu yoksa size kalmış bir tercih midir? Sizin belge almak isteyen kurumlar için tavsiyeniz ne yöndedir?**

- Mevzuatta böyle bir zorunluluk yok. Ama destekçi bir firma olmadan bu sertifikayı almak çok zordur. Danışmanlık firmalarının yoğunlaştıkları bir konu, bu süreci daha önceden yaşamış tecrübeli personelleri var. Bunun yanında verdikleri eğitim hizmetleri var. Tüm personeli kapsayan, her seviyedeki çalışan için ayrı eğitim destekleri var. Yapılan sızma testleri, bağımsız kurum dışından birinin gözüyle yapılan denetimler var. Sertifika aldıktan sonraki dönem içinde de devam eden yıllık eğitim ve denetim programları var. Bunların hepsini hesaba kattığımızda bizim kurum içinde kendi imkânlarımızla yapacağımızdan daha hızlı ve daha kaliteli olacağını düşündük. Bizim böyle bir süreç için personel ayırmamız ve yalnız bu işte görevlendirmemiz daha maliyetli olacaktır. Yapılan ön denetimlerde başarısız olma ve tekrar en baştan sürece başlama riskini de düşünürsek bizim danışmanlık firmasıyla çalışmamız gerektiğine karar verdik. Bana göre belge sahibi almak isteyen her kuruluşun profesyonel anlamda bir danışmanlık ve eğitim firmasıyla ortak çalışma yürütmesi gerekir.
- **Sertifikayı aldıktan sonra herhangi bir kurumdan size danışmanlık anlamında başvurular oldu mu?**
- Danışmanlık anlamında değil ama tecrübe aktarımı olarak Tuzla Belediyesinden başvuran arkadaşlar oldu. Bizde onlara geçen zorlu süreci anlattık ve destekçi bir firma ile çalışmadan bu işin çok zor olacağından bahsettik. Arkadaşlar kendi imkânlarıyla bu süreci başarmayı düşündüklerini söylediler ve danışman firma olmadan kendileri hazırlanıyorlar. Arada bizim arkadaşları ziyaret edip takıldıkları yerlerle ilgili sorular soruyorlar. Ben kendi başlarına bu süreci başarabileceklerine pek inanmıyorum. (NOT: Şubat 2014 itibariyle Tuzla Belediyesi henüz bu belgeye sahip değildir.)
- Yapmış olduğumuz bu mülakatı yüksek lisans tezimizde yayınlayacağız.
- **Kurumunuz isminin geçmesinde bir sakınca var mı? Uygun değil ise isim belirtmeden yayınlayabiliriz?**
- Biz Pendik belediyesi olarak Türkiye'de sayılı kuruluşun alabildiği ISO27001 belgesine sahip ilk belediye olma özelliğine sahibiz. Her yerde de bu özelliğimizi belirtiyor ve bundan gurur duyuyoruz. Bu çalışmada da ismimizin geçmesinden mutlu oluruz.

- **Bize zaman ayırdığınız için çok teşekkür ederiz. İş yaşantınızda başarılar dileriz.**

Pendik belediyesinde yaptığımız bu mülakat bizim çalışmalarımız için büyük önem oluşturdu. Yaptığımız akademik araştırmalarda bazı sorulara cevap bulamıyorduk. Yaptığımız görüşme ile ISO27001sertifikayı almak isteyen kuruluşlara ve bu yönde çalışmalar yapan kişilere örnek olmayı hedefledik. Önceden bize örnek oluşturacak, sertifika sahibi bir kuruluşla birebir görüşülerek hazırlanmış bir çalışma olmadığı için sorularımızı kendimiz araştırmalarımız sonucunda oluşturduk. Sorulan sorularda öncelik bizim akademik çalışmalarda tam olarak cevap bulamadığımız konuları içeriyordu. İkinci öncelikte ise; bizim hazırlıklarımız esnasında önemli görüp, kurum tarafından da önemsendiğini test etmek amacıyla eklediğimiz sorular vardı. Bazı sorular ise mülakat esnasında görüşmecinin cevapları doğrultusunda o anda ortaya çıktı.

Yapılan bu çalışma sonrasında bazı konuların eksik kaldığını ve tek bir kuruluşa göre araştırmanın sonlandırılmasının belki de yanlış yönlendirme yapabileceğini düşünülerek ikinci bir kuruluşla daha mülakat yapmaya karar verilmiştir. İki kuruluşun daha objektif sonuçlar doğurabileceğini ve bu çalışma ile karşılıklı kıyaslama imkânı sağlanarak daha sonraki çalışmalar için farklı bir bakış amacı kazandırma hedeflenmektedir. Bu mülakat sonrasında yapılan çalışmalar sonucunda, yeni mülakat için hazırlıklar yapılmıştır. Kendimizi bir öz eleştiriye tutarak, çalışmanın kritiğini yaptık. Bizim yüzeysel geçtiğimiz bazı konulara daha ayrıntılı değinmemiz gerektiği savına vardık.

Yeni sorular hazırlayarak bu çalışmada eksik kaldığını düşündüğümüz alanları ISO27001 BGYS sertifikasına sahip diğer bir belediye ile yapmaya karar verdik. Özel sektör firmaları genellikle isimlerinin duyulmasını pek istememektedirler. Ayrıca akademik çalışmalara zaman ayırmak istememektedirler. İlk mülakattan edindiğimiz tecrübelerle; belediyelerin akademik çalışmalara daha fazla yardım ettiği ve belediyelerin yaptıkları çalışmaların duyulması, çalışmalarda isimlerinin geçmesi konularında daha olumlu oldukları gözlemlenmiştir. Bizde ikinci çalışmamızın Keçiören Belediyesi ile yapmaya karar verdik. Düşündüğümüz gibi de oldu. Görüşme talebimize olumlu cevap geldi.

5.8. KEÇİÖREN BELEDİYESİ İLE YAPILAN BGYS MÜLAKATI

Pendik belediyesi ile yaptığımız mülakattan sonra BGYS kurulumu ile ilgili bazı konular daha anlaşılabilir hale geldi. Sürecin işleyiş şeması, nerelere dikkat edilmesi gerektiği, yaşanılan zorluklar, kurum içi beklenti ve tepkiler bize yazılı kaynaklarda bulamayacağımız tecrübeler kazandırdı. Okuyarak anlayamayacağız birçok yeri önem derecelerine göre belirterek bize anlaşılır hale getirdi. Yapmış olduğumuz mülakattan sonra cesaretimizi toplayarak, kamu kurumlarıyla bir mülakat daha yapmanın bize faydalı olacağını değerlendirdik. Keçiören Belediyesi'nin de bu sertifikayı aldığını basın aracılığıyla öğrendik. Bilgi İşlem Müdürü İsmail KÖSE Bey ile elektronik posta yoluyla iletişime geçtik, bizi görüşme için Belediye Bilgi İşlem Müdürlüğü'ne davet ettiler.

İlk etapta başka bir kurumla da görüşme yaparsak, en iyi olanına tezimizde yer vermeyi düşünmüştük. Ancak ikinci mülakatımızı da yaptıktan sonra her ikisinin de tez içinde yer alması gerektiğine karar verdik. Öncelikle bize verilen değer, akademik bir çalışma için verdiği emek bizi karara götürdü. Ardından son birkaç yılda yapılan tezlerde işlenen değişik bilgi güvenliği yaklaşımları bizi bu karara sevk etti. Yapılan bilgi güvenliği çalışmalarında diğer kalite yönetim sistemleriyle olan ilişkiler, kurum çalışanlarının yaklaşımı gibi konuları da ele alınmıştır. Bu çalışmalar bize daha fazla kurum üzerinde çalışma yaparak, daha objektif bilgiler verebileceğimiz fikrini doğurdu. Yani bir kurumda yapılan yanlışlar, verilen farklı tepkiler olabilir. Bu süreci iki kurumla tartışarak, gözlemlemek daha fazla ayrıntıya girmek ve iki mülakatı birbiriyle kıyaslamak adına da bizim için daha faydalı olacağı kanısına vardık.

Görüşme öncesinde diğer kurumla yaptığımız mülakat bir kez daha gözden geçirildi. Yeni sorularda eklenerek hazırlıklar tamamlandı. Yarı biçimsel mülakat tekniği kullanılarak bu görüşme tamamlandı. Görüşme öncesinde hazırlanan soru kalıplarına bağlı kalınmadan, görüşme yapılan kişilerin cevapları ve yönlendirmesiyle önceden hazırlanmayan sorulara da cevaplar arandı ve ortaya çıkan yeni konular hakkında da görüşler toplandı. Planlanan zamanda Keçiören Belediyesi Bilgi İşlem Müdürlüğü'ne giderek bilgi işlem personeli ve proje koordinatörü Funda SEVİMLİ hanımla görüşmemiz tamamlandı. Görüşmemiz esnasında bize Bilgi İşlem personeli Ali Bey de katıldı.

- **Kurumunuzun BGYS kurulumu süreci ile ilgili bilgi verebilir misiniz? İlk olarak bu kararı nasıl aldığınızı sorabilir miyiz?**
- Belediye binasında tamamıyla yeniden kablolama ihtiyacımız vardı. Bundan önce de Bilgi İşlem Birimi olarak, bizde BGYS sertifikası ile ilgileniyorduk. Kablolama ihalesi esnasında bu ihtiyacımızı belirterek ihale içinde BGYS sertifikası danışmanlık ve eğitimi ile ilgili bölümü de ekledik. Kablolama ihalesini alan firma tarafından danışmanlık ve eğitim firması ayarlandı ve süreç böylece başladı.
- **BGYS sertifikası için önceden bilgi sahibi olan ve teklifi yapan personelleriniz mi vardı yoksa danışman firmalar tarafından mı size teklifler geldi?**
- Danışman firmalar tarafından bir teklif gelmedi. Zaten biz danışman firma seçmedik, 22-D kapsamında yapılan kamu ihalesiyle kablolama ihalesi yapıldı. Kablolama ihalesini alan firma danışmanlık ve eğitim firmasını ayarladı. Bizim bu ihalede sistem odasının yenilenmesine ve felaket kurtarma merkezi projelerimizde vardı. Onlarda ihaleye dâhil edildi. Sertifika ile bilgisi olan ve ısrarcı olan kişide eski Bilgi İşlem Müdürümüz Tekin Beydir. Bilgi Güvenliği sertifikası ihtiyacını da ihalenin içinde yer almasını o sağlamıştır.
- **Hangi destekçi firma ile çalışmalarınıza başladınız?**
- ICT Sert Danışmanlık ve eğitim firmasıyla.
- **İlk olarak nereden başladınız?**
- Biz ilk olarak bilgi güvenli sisteminin kapsamını belirleyerek işe başladık. İstenilen şartları araştırdık. Kendi kurumumuzda bu şartları nasıl sağlayacağımızı düşündük ve standarttın içeriğini incelemeye başladık. Tüm belediye için hesaplamalar yaptık. Baktık ki işin içinden çıkamıyoruz, kapsamı daraltmaya başladık. Sadece Bilgi İşlem Müdürlüğünü kapsayacak şekilde sertifika almaya karar verdik. BGYS kapsamı bilgi işlem müdürlüğü olarak belirlendi.
- **Tüm belediye için sertifika almak ne gibi zorluklar doğuruyordu?**
- En başta oluşturulan varlıklardan tutunda, elinizde ne varsa bunların kayıt altına alınması, bunların korunması, ayrıca artan personel miktarı, onlara verilen eğitimler, büyüdükçe artan risk oranları bizi bu kararı almamıza itti. Bu sertifikayı alabilmek için belli kriterleri sağlamanız ve sonrasında bunların korunduğunu

taahhüt etmeniz gerekiyor. Hem sertifikayı almak zorlaşıyor hem de sertifika aldıktan sonrada şartları sağlamak daha da zorlaşıyor. Sertifika alındıktan sonrada yapılan kontroller var. Bunun yanında taahhüt ettiğiniz şartları sağlayamazsanız kuruma karşı çok farklı yaptırımları var. Sertifikanın üzerine dikkatlice bakarsanız görebilirsiniz belediye adına değil belediyemizin bilgi işlem müdürlüğü adına alınmış bir belgedir.

- **Kapsamı belirledikten sonra ne ile devam ettiniz?**
- Varlık envanterini çıkartmaya başladık, nelerin envantere dâhil edilip edilmeyeceğine karar verdik. Bu envanter listesini dokümante etmeye başladık. Bu arada destekçi firmada kurumumuza gelerek bir toplantı yaptık. Bize envanter çıkarma konusunda çok yardımcı oldular. Danışman firma olmadan bunları bizim envanteri hazırlamamız çok zor olurdu. Varlıkların korunması, açıklıkların giderilmesi için çalışmalar başlatıldı. Bir kaç test firmasıyla görüştük ve bizim sistemimizi denemelerini istedik. Kontroller için geldiler ve testler yaptılar, açıkları tespit ettiler.
- **Kontro**l **için gelen bu firmalar nasıl belirlendi?**
- Bulduğumuz firma İstanbul'dan bir firmaydı. Tabi firma ararken danışmanlık firması da yardımcı oldu.
- **Danışmanlık firmasıyla süreç nasıl başladı?**
- Biz kapsamı belirledikten sonra, danışmalık firmasından arkadaşlar geldiler. Bizim yaptığımız kapsamı da incelediler ve envanter çalışmasına yardımcı oldular. Bir toplantı düzenledik ve sürecin nasıl ilerleyeceğini konuştuk. Öncelikle kararlar alındı ve danışmanlık ve eğitim firması tarafından bir bilgi güvenliği eğitimi verildi. Bir yol haritası hazırlandı bizim müsait olduğumuz zamanlara göre eğitimler planlandı. Aramızda görev dağılımı yaparak sorumlular kendileri ile ilgili bölümler üzerinde çalışmaya başladı.
- **Verilen bu eğitimlere kaç kişi katıldı?**
- Eğitimlere 50–60 civarında personel katıldı.
- **Eğitim yalnız belli çalışanlar, için miydi?**
- Hayır, temel bilgi güvenliği konularını kapsıyordu tüm personel için yapmıştık.
- **Peki, tüm çalışanlarınızın sayısını öğrenebilir miyiz?**
- Tüm belediye çalışanlarımızın sayısı yaklaşık 2000 ile 3000 arasında bir sayı.

- **Sizce katılım az değil mi, bunun bir sebebi var mıdır?**
- Katılım çok az oldu. Personel bu konu hakkında pek istekli davranmıyor. Bilgi güvenliği denince bilgi işlem biriminin yapması gerektiği bir iş olarak görüyorlar. Kendi üzerlerine bir sorumluluk almak istemiyorlar. Zaten bizde bu yaklaşımı da değerlendirerek tüm kurum için bu sertifika almanın çok zor olacağını değerlendirmiştik. Düşündüğümüz gibi de oldu.
- **Peki destekçi firma şart mı en başından itibaren sizde tek başınıza bu işi yürütebilir miydiniz?**
- Destekçi firma şöyle gerekli; en başından itibaren elinizdeki mevcut her şeyi dokümante etmeniz gerekiyor. Dışarıdan bir firma yardımıyla bunu yapmak çok daha kolay hale geliyor. BGYS kurarken bazı zorunluluklar oluşuyor. Belgeyi aldıktan sonrada bu zorunluluklar, sorumluluğa dönüşüyor. Bu sorumlulukları kuruma entegre etmek için en iyi seçenek dışarıdan bir firma olmasıdır. Hem personeli de bazı hükümlülüklerden korumuş oluyoruz hem de bağımsız bir gözle bakmış oluyorlar. Bize normal gözüken bir durumu onlar bağımsız davranarak daha ayrıntılı ve başka bakış açılarıyla yorumlayabiliyorlar. Sorumluluklarda biraz olsun kendi personelimizin üzerinden kalkıyor. Bu tür firmalar aynı zamanda denetleme faaliyeti de yaptıkları için daha fazla ayrıntıyı biliyorlar. Bizim geçireceğimiz denetimlerde nelerle karşılaşacağımızı önceden görüyorlar Ona göre işlerini sağlam yapıyorlar. Sizde tek başınıza yapabilirsiniz ama çok uğraşırsınız. Tek tek dokümanları çıkartacaksınız, denetlemeler gireceksiniz, yeniden gözden geçireceksiniz, en baştan alacaksınız. Bu çalışanlar için aşırı bir yük olur ve diğer işlerinin aksamasına sebep olur. Ama danışmanların hazırlamış oldukları dokümantasyonlar var. Onları sizin kurumunuza entegre ettikleri zaman hem zamandan kazanılmış oluyor hem de gözden kaçan noktalar varsa bir kez daha incelenmiş oluyor.
- **Şu anda destekçi firma ile çalışıyor musunuz?**
- Hayır, firmayla görüşmüyoruz sadece yılda bir denetlemeler var o zamanlarda bir araya gelip çalışmalarımız devam edecek. O zaman destek alabiliriz.
- **Peki, eğitimler devam ediyor mu?**
- Eğitim olarak zaten bir defa bir faaliyet gerçekleştirdik. Onda da BGYS ile ilgili genel bilgiler verildi. BGYS nedir, kapsamı, amaçları anlatıldı. BGYS geldikten

sonra kurum içindeki karakter, hareketler, planlar neye göre şekillenecek bunlarla ilgili eğitim verildi. BGYS geldikten sonra kurum personeli nasıl bir hareket sergileyecek bununla ilgili eğitimler verildi. Eğitimlerdeki temel amaçlardan bir tanesi de farkındalık yaratmak. Yani elinizde bilgi var, kaynaklar var fakat bunun sizin için önemi nedir, bunu anlamak gerekli bunun farkına varmak gerekli eğitimlerde ilk öğretilende bunlardır.

- **Bu sertifikanın bir yıl geçerliliği olduğu ve sonrasında yine denetlemeler olduğunu biliyoruz. Siz kurum olarak bu denetlemeleri geçtiniz mi?**
- Sertifikanın geçerlilik süreci üç yıldır. Yılda bir ara denetlemeler vardır. Biz daha sertifika alalı bir yıl geçmedi. Önümüzdeki aylarda bu denetlememiz olacak bizde hazırlanıyoruz.
- **Ayrıca BGYS ile ilgili kurumunuzun yürüttüğü başka eğitim çalışmaları var mı? Personel eğitimi konusunda farklı çalışmalar yapılıyor mu? (Baş Denetçi, tetkikçi eğitimleri vb.)**
- Kurumumuzda ayrıca BGYS hakkında personel eğitim programları yürütülmüyor.
- **Kurumunuzun oluşturduğu BGYS organizasyonunda kimler görevlidir?**
- Bilgi güvenliği koordinasyon grubumuz vardır. Bu grupta BGYS koordinatörü bulunur. Genellikle bilgi işlem personelinden seçilir. Danışman firma ile beraber ortak işleyişi takip eder. Sürecin tamamında rol alır. Eğitim çalışmalarını ve kurum personelinin BGYS içindeki rol ve sorumluluklarını takip eder. Kurumda bu işi ben yürütmekteyim. Her birimden de en az birer kişi birim sorumlusudur. Kendi birimlerinin bilgi işlem ile ilgili sorumluluklarını, eğitimlerini ve ihtiyaçlarını takip ederler ve eğitim faaliyetlerine katılırlar. Birde BGYS asıl sorumlusu vardır. O da kurum amiridir. Kurum adına yapılan çalışmaları ve hazırlanan politikaları onaylayan ve imza ile taahhüt eden kişidir.ISO27001 zorunlu tuttuğu maddeler var. Biz onlar üzerinden yola çıktığımızda önce kapsamı belirledik. Kapsamda tüm belediyeyi alınca işin zorlaştığını ve bizim bunu başaramayacağımızı gördük. Kapsamı daraltmaya karar verdik.
- **Kapsamı daraltma sebebiniz BGYS kurulum maliyetlerini azaltmak için midir?**
- Hayır, kapsamı daraltmanın BGYS kurulumu maliyetleriyle bir alakası yok. Fakat kapsam arttıkça içinde yer alan ayrıntılar artmakta bunlarda dolaylı olarak size

ayrı bir yük getirmektedir. BGYS size diyor ki ilk bina giriş kapısında ne gibi önlemler alıyorsunuz? Gelen vatandaşa içeri girerken giriş kartı veriliyor mu? Orada görevli güvenlik personelinin kullandıkları silahları ayrıca kilitli bir dolapta muhafaza altına alınıyor mu? Gelen kişilerin sadece gitmesi gerektiği yere gidebilmesini sağlayabiliyor musun? Buna benzer şeyler var. Örnekleri arttırabilirsiniz. Bu önlemler arttıkça çalışanlarda, maliyetlerde artmaktadır. Bunun içinde ister istemez baştan sona yeni bir eğitim süreci gerekir.

- **BGYS kurulumu çalışmalarında sizce dikkat edilmesi gereken en önemli hususlar nelerdir?**
- BGYS çalışmalarında öncelikle elinizde neler olduğunun farkında olmak gerekir. BGYS size soruyor elinde arşivin mi var, elinde personelinin özlük dosyalarının olduğu dolaplar mı var, evrak dolapları mı var, elinde otomasyon sisteminin veri tabanı mı var diyor, elinde kağıt notların olduğu bir şeyler mi var diyor her neyse. Senin bilgi olarak kullandığın ne varsa bunların bana bir envanterini çıkart diyor. Sonra bunlara erişen kullanıcıları çıkart bana diyor. Envanter dediğimiz şey işte budur. Sonra diyor sen BGYS kapsamını belirle. Biz sadece bilgi işlem birimine bu sertifikayı aldığımız için dolayısıyla belediyenin geri kalanı bizim aldığımız sertifikadan sorumlu değil. Bu sertifika Sadece bizi bağlıyor, bir cezai yaptırım olacaksa da sadece bizim birime oluyor. Sonra diyor ki sen bunların hepsini bir yazıya dök. Excel olur başka bir şey olur, bunu bir tabloda göster diyor. Ne kadar bilgisayarın var, hangi özelliklere sahip belirt diyor. Bunları belirttikten sonra bunları etkinlik değerlendirmesini, bütünlük değerlendirmesini ve erişilebilirlik değerlendirmesini yapmanız gerekir. Örneğin diyoruz ki benim dolabım çok gizli, bunu şundan başkası kullanamaz. Bilgisayarlara erişim hakkı sadece şu kişilerde vardır diyoruz ve onları yazıyoruz. Sonra bu kuralı koymuş oluyoruz ve kuralları uygulamaya başlıyoruz. Bu aşamaları sağladıktan sonra biz diğer aşamalara geçebiliriz. Bu saydıklarım temel aşamalardır. Bunları sağlamadan diğer adımlara geçiş olmaz. Bu koşulları sağladıktan sonra BGYS adına kendiniz diğer ihtiyaçlarınızı belirleyebilirsiniz. Örneğin benim sistemimde güçlü bir firewall yok, yâda benim bir felaket kurtarma sistemim yok, yâda ben yedekleme yapmıyorum diyebilirsiniz. BGYS size sen bu eksikliklerinin farkında mısın diye soruyor. Bu eksikliklerini ne zaman gidereceksin zaman belirt diyor veya bu

eksiklikleri gidermeyeceksen sebebini yazılı olarak imza atarak belirt diyor. Siz diyorsunuz ki benim felaket kurtarma sistemim yok. Şuan ki mevcut durumda maliyeti çok yüksek ben bu sistemi 5 yıl içinde kurmayı planlıyorum ve imza ile tahakkuk ediyorum. Benim için bu kabul edilebilir risk diyebilirsiniz.

- **Felaket kurtarma sistemini kurmadan, ilerleyen bir zamanda bunu kuracağınızı belirtmeniz yeterli oluyor mu? Yine de sertifika alabiliyor musunuz?**
- Tabi ki yeterli oluyor. Belge almanıza engel bir durum söz konusu değil. Siz BGYS kurarken kendi eksikliklerinizin de farkına varıyorsunuz. İşin güzel yanı BGYS kurulumu esnasında zaten kurumunuzu daha iyi tanıyorsunuz.
- **Aldığınız sertifikanın belediyenin bilgi işlem birimini kapsadığını söylediniz. İnternet üzerinden e-belediye hizmetinin kullanılması da bu sertifikanın kapsamında mıdır?**
- Evet, bu hizmetlerde bizim bilgi işlem birimi tarafından sağlandığı için, sertifikanın kapsamı içinde güvenliği sağlanmaktadır. Bütün e-belediyecilik hizmetinin alt yapısı şu anda bulunduğumuz birimin içinde yer alıyor. Biz bilgi işlem birimi için yüz tanıma sistemi kurduk. Yabancı bir personel giremez. Bu güvenlik önlemlerini aldığımızı BGYS içinde beyan ettik. Sunucularımızın yedeklemesi alınıyor bunları beyan ettik. Bir durum ortaya çıktığında iki personelimiz müdahale ediyor, beyan ettik. Bir arıza oluştuğunda bunların kaydının tutulduğunu, arızanın giderildiğini, beyan ettik. Aldığımız bütün tedbirleri BGYS yazılı belgelerinde tahakkuk ettik ve yapıyoruz.
- **Daha basit şekilde soruyu sorarsak belediyenin internet sitesinden girip, su faturamızı yatırdığımız zaman bizim bilgilerimizi diğer kişilerden koruyabiliyor musunuz? Aldığınız bu sertifika bize bu güvenceyi veriyor mu?**
- Kesinlikle biz bu türde bir işlem yapan vatandaşın bilgi güvenliğini en üst seviyede koruyoruz. Biz bu sertifikayı alırken zaten bunların hepsini yazılı olarak beyan ettik bunun aksini yaparsak bize farklı yaptırımlar uygulanır. BGYS denetçileri zaten sık sık gelip bu türde denetlemelerini yapıyorlar. Bende firewall var diye beyan etmişim gelip kontrol ediyor, nerede diye soruyor? Gösteriyorsun

tamam deyip, diğer beyanları kontrol ediyor. Loglama yapıyorum diyorsun, göstermeni istiyor. Gördüğü anda tamam diyor.

- **Siz bu sertifikaya şuan için sahipsiniz. Hazırlamış olduğunuz envanterde yer almayan yeni bir malzeme veya değeri olan bir varlık aldınız. Bunun mevcut kabul edilmiş BGYS ne entegresi nasıl oluyor?**
- BGYS ile ilgili tüm kayıtlarımız hem beyan ettiğimiz kuruluşta hem de bizde de mevcuttur. Bizde yer alan ilgili bölümlere kendimiz ekleme yaparak bu işlemi gerçekleştiriyoruz. Her hangi bir denetleme esnasında da durumu belirtiyoruz. Sorun oluşturacak bir durum değil. Kurumda yer alan BGYS koordinatörünün imzası yeterli oluyor.
- **BGYS içinde kimlerin görevleri var?**
- BGYS oluşturulurken roller ve sorumluluklar belirlenir. O aşamada kimin neden sorumlu yetkileri ne kadar, sistem içinde ne yapması gerekir, hepsi orada tek tek belirtilir. Yazılımdan sorumlu personel, ağ güvenliğinden sorumlu personel asıl ve yedek sorumlular kapsamın içinde yer alan herkese dağıtılır.
- **Sizce BGYS kurulumunu ISO27001 standartlarına göre yapabilmek için danışmanlık firmasına ihtiyaç var mıdır? Yoksa kuruluş kendi personeliyle de bu süreci yöneterek BGYS sertifikasını alabilir mi?**
- Bence danışmanlık firması olmadan da başarılı olunabilir. Ama bir personelin yalnız bu işe ayrılması gerekir. Mevzuatları iyi okuyup anlaması gerekli ve kendi kuruluşuna göre biçimlendirmesi gerekir. Standarttın içinde ne yapması gerektiği madde madde yazıyor. Yapılması gereken sadece envanter çıkartmak, kapsam alanını belirlemek, çıkardığı envanterlerle ilgili gerekli soruları yanıtlamak, başvuru yapmak ve ardından gelen denetçiyle tek tek hepsini gözden geçirip sistemi anlatmak gerekiyor. Kuruluşlar neden destekçi firmalarla çalışmak istiyorlar? Çünkü sistemi kurmaya yardım edenlerde bu firmalar, denetlemeleri yapanlarda yine bu firmalar. Neyin eksik olup olmadıklarını kendileri çok iyi bir şekilde biliyorlar.
- **Bilgi işlem personeli olarak sizce ISO27001 sertifikası almanız gerekli midir, yoksa almasanız da olur mu? Sizin bu sisteme bakışını nasıl olmuştur?**
- Biz bilgi işlem personeli olarak her zaman için bu süreci destekledik. Çünkü en çok bizim işimize yarayacaktı. Biz bunun bir ihtiyaç olduğunu müdürlerimize

başından itibaren söyledik. BGYS sayesinde bizimde işlerimiz rahatlamış oluyor. BGYS yazılı politikalarıyla kurum amirinin imzasıyla bize emir niteliği taşıyor. Örneğin biz personelin nerelere ulaşabileceğini, hangi sistemleri, hangi bilgisayarları kullanabileceğini BGYS'nin içinde belirtiyoruz. BGYS kimin ne kadar yetkisi olduğunu en başta belirliyor. İleride bir personel, ben niye bu bölgeyi kullanamıyorum, ben niye diğer bilgisayarlarda da işlem yapamıyorum dediğinde; bizim ona cevabımız kurum amiri tarafından onaylanan Bgys ile olacaktır. Böylelikle keyfi uygulamalarında önüne geçilmiş olacaktır. Bizim sertifika almamız bize ayrıca prestij kazandırmıştır.

- **Siz sertifika aldıktan sonra sizinle iletişime geçip, sizden tecrübe paylaşımı isteyen kurumlar oldu mu?**
- Şuan için herhangi bir ardım talebi olmadı.
- **Yazılı veya digital ortamda bize kaynak olarak verebileceğiniz her hangi bir şey var mıdır?**
- Danışmanlık ve eğitim firmasıyla beraber ortak yürüttüğümüz eğitimlerle ilgili temel eğitim notlarının olduğu bir kitapçığı size verebiliriz. Sertifikanın digital ortamda görüntüsünü verebiliriz. Bunun dışında kullandığımız bir cihazın markasını dahi size söylememiz uygun değildir.
- **Bilgi işlem müdürlüğü olarak sertifikanın kapsamında sizler varsınız? Sizin bilgi güvenliğini korumayı taahhüt ettiğiniz kişi sayısı ortalama olarak ne kadardır?**
- Bilgi işlem birimi olarak yalnızca kendi birimimizin bilgi güvenliğini taahhüt ediyoruz. Fakat bilgi işlem müdürlüğü içinde yer alan sunucular bizim varlık envanterimizde yer almaktadır. Bu sebeple bu sunuculardan hizmet alan herkesin bilgi güvenliğini korumakla hükümlüğüz. Bu kişi isterse yurtdışında oturan ve Keçiören e-belediye hizmetlerinden yararlanmak isteyen bir vatandaşımız olsun. Mekânın ve zamanın bizimle bir ilgisi yoktur. Bizim hizmetlerimizi alan herkes bilgi güvenliği kapsamının içine girer. Yaptığımız her işten sorumluyuz.
- **Bize zaman ayırdığınız ve sorularımıza vermiş olduğunuz içten cevaplar için teşekkür eder iş yaşantınızda başarılar dileriz.**

SONUÇ

Yapılan araştırmalar sonucunda; öncelikle kendimizin bilgi güvenliği konusunda daha iyi eğitilmesini sağlamış olduk. Araştırmaya başlamadan önce yaptığımız literatür taraması sonucunda bu konuda hazırlanan az sayıdaki akademik çalışma bizim çalışmalarımızı bir noktaya kadar getirip orada belli bir sonuca varamadan eksik bırakıyordu. Bu sebepten dolayı bizi nihai sonuca götürebilecek her türlü kaynağı ve her türlü araştırma metodunu kullanarak farklı görüşleri de içine alan bir çalışma ortaya çıkarmaya çalıştık. Araştırmalarımız esnasında şunu fark etmiş olduk. Bugün öğrendiğimiz bir bilgi, iyi bir şekilde işlenip kullanıcıya sunulamazsa yarın kaliteli bir bilgi olma niteliğini kaybedebilir. Bu araştırmaya başlarken en kapsamlı ve kullanışlı olan bilgi güvenliği standardı tespit edilerek o konu üzerine yoğunlaşmıştık. Fakat çalışmalarımız sürerken bu standardın ve diğer standartların yeni versiyonlarının çıktığını gözlemledik. Ülkemizde daha henüz yayınlanmamış olan bu standardı yurt dışı kaynaklardan edinerek, kendi dilimize çeviriler yaparak ve yabancı yayınlardan yararlanarak sizlere tanıtmayı hedefledik.

Yeni versiyonun tanıtılması hususunda ülkemizde internet sayfaları aracılığıyla yapılan yayınları da takip ederek, yabancı dilde yayınlanmış ana metin üzerinden kontrollerini sağladıktan sonra sizlere sunumunu gerçekleştirdik. Bu esnada bir konu daha dikkatimizi çekti. Yapılan birçok araştırma blog sayfalarında internet aracılığıyla sunulmaktadır. Bu çalışmaların sunum olarak bu şekilde yapılması çok daha fazla kitleye ulaşmasını sağlayabilir. Yapılan bu araştırmalarda kullanılan dilin günlük yaşantımızda kullandığımız yapıda olması anlaşıla bilirliğini daha da arttırmaktadır. Fakat yapılan bu tetkiklerin akademik çalışmalarla da güvence altına alınması gereklidir. Yazılan bir ifadenin doğruluğu genel kabul görmüş denetimlerden geçirilerek, gerçekliği doğrulandıktan sonrada akademik çevrelerce de araştırılarak yayınlanmalıdır. Yapılan bir araştırmanın kaynak niteliği kazanabilmesi için bu gereklidir. Yapılan birçok araştırma kendi dilimizde hazırlanan kaynakların yetersizliğinden dem vurmaktadır. Bu konuda devlet teşvikleriyle de yeni çeviriler, yeni yayınlar ve yeni standart geliştirme çalışmaları sürdürülmelidir. BGYS kurulumu için TÜBİTAK-UEKAE tarafından hazırlanan yardımcı kılavuz yayınlar çalışmamız esnasında bizim içinde çok faydalı birer kaynaktı. Fakat bu kaynaklarında yenilenen

sürümlere göre kendini yenileyebilen ve toplumu bilgilendirici nitelikte yayınlar hazırlamaya hız kesmeden devam etmesi gereklidir. Üniversitelerimizin bu konuda yayınlar ortaya koyması gereklidir. Bilgi güvenliği konusunda; istenilen yer ve zamanda kendi dilimizde, herkesin anlayabileceği şekilde kaynaklar oluşturulmalı ve bu kaynakları oluşturacak teşvikler yapılmalıdır.

Bilgi güvenliği konusunda insanların düştüğü en büyük yanlış, bu konunun teknik bir konu olduğuna inanmalarıdır. Belki de bu konunun böyle anlaşılmasının sebeplerinden bir tanesi de, mevcut araştırmaların birçoğunun fen bilimleri bölümünden, bilgisayar alanlarıyla ilgili kişiler tarafından hazırlanmış olmasıdır. Doğal olarak bu kişilerin araştırmaları da kendi alanlarını kapsayan teknik konuların ele alındığı ve toplumun belli bir kesimine hitap edecek şekilde hazırlanmış olmasından kaynaklanmaktadır. Bilgi güvenliği konusu toplumun her kesiminde yer alan bütün bireyleri ilgilendiren temel bir konudur. Aynı şekilde bilgi güvenliğinin sağlanması da sadece teknik ekipmanla ve teknik personelin bilgisi ile yürütülecek bir faaliyet değildir. Her birey öncelikle kendi bilgi güvenliğini sağlamaktan kendisi sorumludur. Günlük yaşantısında kullandığı cep telefonundan, sosyal ağlardaki hesaplarına kadar, internet üzerinde yaptığı işlemlerden günlük hayatta sahip olduğu varlıklara kadar hepsinin güvenliğinden öncelikle her birey kendisi sorumludur.

Son yıllarda sosyal mühendislik olarak tanımladığımız modern dolandırıcılık metotları yedi den yetmişe toplumun her kesimini hedef almakta ve çok büyük kayıplar yaşatmaktadır. Sosyal mühendisler kişisel ikna kabiliyetleriyle, insanlara güven telkin ederek dünyanın herhangi bir yerinden sizlere ulaşabilmekte ve sizleri rahatlıkla avlayabilmektedirler. Ülkemizde son yıllarda basın yayın organlarında çok fazla gündeme gelmesine rağmen, hala devam etmekte olan, toplumun her kesiminden kişiler (profesör unvanına sahip kişiler dâhil) kolaylıkla cep telefonundan aranarak; kendini güvenlik güçleri personeli olarak tanıtması sonucunda para talep etmesi ve bu talebin karşılanması olayı sosyal mühendislik alanının en basit ve en bilinilir örneklerindendir. Bu duruma düşen birçok kişi yaptığı yanlışın farkına varsa dahi kendisinin ayıplanacağını düşünerek, bu konuyu hiç kimseyle paylaşmamaktadırlar. Bu yöntemle dolandırılan birçok kişinin aynı metotla farklı zamanla tekrar mağduriyete uğradıkları bilinmektedir. Kullanılan bu yöntemin çok basit olması ve defalarca ifşa olması sonucu

çok da fazla değiştirmemektedir. Çünkü toplum olarak bilgi güvenliği konusunda genel bir bilgisizlik hâkimdir.

Ülke olarak öncelikle bilgi güvenliği konusunda bir bilgi güvenliği politikasına sahip olmamız gereklidir. Yapılacak çalışmalar uzun vadeli ve kısa vadeli olarak sıralanmalıdır. Bu konuda eğitimcilerimize düşen roller belirlenmeli ve uzmanlar eşliğinde, eğitim politikalarımızın içine bu konu dâhil edilmelidir. Öncelikle eğitim faaliyetlerine her alanda faaliyet gösteren eğitimcilerimizi dâhil etmeliyiz. Bilgi güvenliği konusunda farkındalık oluşturduğumuz eğitimcilerimiz yetiştirdikleri bireylere aldıkları eğitimlerin ışığında bir süreç gelecek sunacaklardır. Eğitim politikalarının gerçekleştirilebilmesi için üniversitelerimizde birçok görevler düşmektedir. Lisans seviyesinde eğitim alan her öğrenciye kendi bölümlerine paralellik gösteren, bilgi güvenliği eğitimleri müfredata dâhil edilmelidir. Bu eğitim konuları devamlı olarak güncellenmeli ve zamana karşı dinamik durabilmelidir. Toplumun her kesimine hitap edebilecek akademik yayınlar, bildiriler ve konferanslar düzenlenmelidir. Danışmanlık ve eğitim faaliyetleri konusunda sertifika almak isteyen kuruluşlara hizmet verebilecek düzeyde bölümler oluşturulmalıdır. Personelin bilgi güvenliği konusunda yeterliliğe ulaşabilmesi ve geçerliliği olan eğitici ve denetçi sertifikaları alma konusunda teşvik edilmelidir. Üniversitelerimizin de BGYS alanında uluslararası geçerliliğe sahip standartların gerekliliğini sağladıklarını göstererek BGYS sertifikaları almaları ve topluma bu alanda da örnek olmaları gerektiğini düşünmekteyiz.

Araştırmamızda bilgi güvenliği konularını içeren, dünyada kabul görmüş ve en fazla kullanılmakta olan standartlar ve rehber niteliğindeki kılavuz yayınlar irdelenmiştir. En çok bilimsel araştırmaya konu olan standart ve kılavuzları açıklamaya çalışırken, en güncel versiyonları baz alarak araştırmamızı gerçekleştirdik. Her konuda yeterli miktarda bilgi vererek, bir konu hakkında derinlemesine araştırma yapmayı düşünenler içinde yerli ve yabancı hangi kaynaklardan yararlanabileceklerini açıkladık. Araştırmamız derinleştikçe kendi eksiklerimizin de daha rahat farkına varmaya başladık. BGYS hakkında yorumlamalar yapabilmeye başladık. Bilgi güvenliği konusunda standartların en önemli özelliği teknik konuları içermeyen prosedürleri açıklayıcı yapıda olmasıdır. En doğru standardın her kurum için farklı olabileceğini daha iyi anladık. Bir standardın diğer bir standartta olmayan özelliklere sahip olabileceğini gözlemledik. Her kuruluş kendi ihtiyaçlarına cevap verebilecek standartlar

ve kontrol hedeflerini seçmeli ve bu seçimini üst yönetim kurulu kararıyla belirlemelidir. Aynı anda birkaç kaynak baz alınarak sistem kurulumu gerçekleştirilebilir.

Bütün standartları bir arada inceleyince en başta kusursuz gibi görünen ISO27001:2005 standardının da eksiklerinin olduğunu görmeye başladık. Yurtdışı kaynaklarda yayınlanan ISO27001 standardının yeni versiyonunu incelediğimizde, yapılan değişikliklerin ne denli haklı olduğunu anladık. bu araştırma esnasında öncelikle mevcut ISO27001 sürümü baz alınarak araştırmamız yürütülürken, yeni versiyonun yurtdışında yayınlanmasının ardından her iki sürümü de kıyaslayarak kapsamı genişletmeye karar verdik. Yeni versiyonla beraber diğer yönetim sistemlerinde de daha önceden uygulanmaya başlanan annex sl yapısını inceleyerek, açıklamalarda bulunduk. Bu yapı sayesinde yönetim sistemlerinin birbirleriyle olan uyumu sağlanmış oldu. Böylelikle genel yapıda açıklanan bir kavram, tüm yönetim sistemlerinde aynı anlamı ifade etmekte ve böylece anlam kargaşasını ortadan kaldırmış olmaktadır. Bu yapı sayesinde bir yönetim sistemi hazırlamış olan bir kuruluş, diğer yönetim sistemlerini kurmak istediğinde genel yapıdaki hazırlıkları kullanabilecek, zamandan ve iş gücünden tasarruf etmiş olabilecektir. Bu yapının öğrenilmesi yönetim sistemleri konusunda çalışma yapacak kişiler için çok büyük önem arz ettiği düşünülmektedir. Bundan sonra, bütün yönetim sistemlerindeki revizyonlar ve yeni oluşturulacak yönetim sistemi standartları bu yapıda oluşturulması kararı alınmıştır. IRCA tarafından hazırlanmış olan "annex sl" broşürü tüm araştırmacılar için faydalı olacaktır.

ISO27001 BGYS standardı sonucunda bir sertifika sahibi olmak iş yaşantısında belge sahibi kuruluşlara ayrıcalıklar kazandırmaktadır. Her kuruluş iş yaşantısında; gizliliğe, bütünlüğe, erişilebilirliğe ve güvenliğe önem veren kurumlarla çalışmak ister. Bu saydığımız niteliklerin ve daha birçok özelliğin uluslararası geçerliliğe sahip, bağımsız kuruluşlar tarafından belgelendirilmesi de ayrı bir önem arz eder. Bir kuruluş bilgi güvenliğinin bütün gereksinimlerini yerine getirdiğini ifade edebilir. Fakat bağımsız denetimlerle ve farklı zamanlarda yapılan kontrollerle bu yeterliliğin; bağımsız kuruluşlarca, sürekliliğini ve güvenilirliğini ispatlaması gereklidir. BGYS standartlarını yerine getiren bir kuruluş öncelikle kendisinin belli bir politika çerçevesinde disiplin içerisinde yürütüldüğünü gösterir. Üçüncü taraflarla olan ilişkiler belli bir prosedür içerisinde yürütüldüğü için ortaklaşa yapılacak işinde garantisi

sağlanmış olur. Özellikle teknoloji, e-faturalandırma, gümrükleme, haberleşme ve iletişim gibi sektörlerde bazı kanun ve ihale metinlerine konulan maddelerle bu standardın şartlarının sağlandığının ispatı olarak sertifika sahibi olmayı şart koşmaktadırlar. Ayrıca bu belgenin alınması çalışanları, özelliklede bilgi işlem birimi çalışanlarını çok fazla rahatlatacaktır. Bu standardın gereksinimlerini yerine getiren bir kuruluşta her şey belli politikalar ışığında, önceden belirlenmiş ve üst yönetimin onayı ile ortaya konulmuştur. Herhangi bir ihlal olayında da kimin ne yapması gerektiği önceden belirlenmiştir. Roller ve sorumlulukların dağıtılmasıyla ve her işlemin kaydının belli prosedürlere uygun olarak belli bir zaman dilimine kadar saklanması sonucundan her eylemin sorumlu kolay tespit edilebilmektedir. Yapılan iş sözleşmelerinde her personele önceden tebliğ edilen bilgi güvenliği hususları, sonradan doğabilecek herhangi bir sorunda organizasyonun elini kuvvetlendirecek belge niteliği taşımaktadır. Yasal mevzuatlardan doğabilecek sorun ve sorumluluklara karşı BGYS bizleri koruma altına alır. ISO27001 BGYS sertifikası almak bir kuruluşun ilgili olduğu her alanda fayda sağlamaktadır. Yönetim kademesinden, en alt kademeye kadar, bilgi işlem personelinden, müşteri olan taraflara kadar her kesim bu sertifikanın güvencesi altındadır.

Araştırmamızda ISO27000'dan başlayan bilgi güvenliği standartları ailesine yer verdik. İlk olarak tanımlardan ve sözlük kısmından oluşan standarttan başlayarak, belge ve denetimcilerin gereksinimleri içeren standartlardan sonra, her sektör için ayrı ayrı yazılmış olan standartlar hakkında bilgiler verdik. Her sektör için özellik arz eden standartların asıl amacı ISO27001 standardının gereksinimlerini sağlamaktır. Kuruluşlar kendilerini ilgilendiren konuların daha iyi açıklanması ve daha ayrıntılı bir çalışma yapmak için bu yardımcı kılavuz standartları kullanmaktadır. ISO27001 ve ISO27006 standartları dışında gereksinimler içeren ve yapılması zorunlu olan standartlar yoktur. Diğer standartları sağlamanın sonucunda, her hangi bir belgeye sahip olamazsınız.

ISO27001 sertifikası almak için öncelikle standardı elimize alıp, standardın gereksinimlerini tartışmamız gerekir. Standartlar bize neleri yerine getirmemizi anlatmakta fakat nasıl yapıldığını açıklamamaktadır. Biz bu araştırmamızda bilgi güvenliği yönetim sistemleri hakkında bilgi edinmek, kendi imkânlarıyla BGYS kurmak isteyenlere, BGYS kurulumu ile ilgili ayrıntılı bilgiler vermeğe ve bu sürece katkısı olacağına inandığımız kaynakları belirtmeye çalıştık. Öncelikle belirli aşamalara

bölerek süreci tanıtmayı hedefledik. Ardından da ISO27001 standardının maddelerinin sırasına göre mevcut ve yeni sürüme göre, süreci bir kez daha hiçbir eksik kalmamasına dikkat ederek açıkladık. Standardın ek kısmında yer alan kontrol maddelerini de yeni sürümde yapılan değişikliklere göre ele aldık. BGYS denetimleri ve kontrollerinin ardından sürekli iyileştirme isteyen bir sistem olduğunu vurguladıktan sonra sertifika alabilmek için hangi kuruluşlara başvurmamız gerektiğini ve o kuruluşun ne gibi özellikler taşıması gerektiğini açıkladık. ISO27001 standardının diğer yönetim sistemi standartlarıyla ilişkilerini karşılaştırarak, ülkemizdeki ve dünyadaki dağılımı yıllara göre sayısal verilerle sunduk. Yönetim sistemleri içerisinde daha yeni fark edilmeye başlanan bilgi güvenliği yönetim sistemlerinin, yeni versiyonla beraber daha fazla kuruluş tarafından, diğer kurulu yönetim sistemlerine entegre edilerek daha kolay kabul göreceği düşünülmektedir.

Araştırmalarımız esnasında ne kadar fazla kaynak taraması yapsak ta, yapılan çalışmalardaki örnekleri incelesek te sonuç olarak bir yerde tıkanıklık yaşadık. Kendi anlattığımız gereksinimlerin doğruluğunu da test etmek amacıyla ve sürecin daha iyi anlaşılabilmesi adına ISO27001 sertifikasına sahip kuruluşlarla BGYS kurulumu ve işletilmesi süreci ile ilgili mülakat yapmaya karar verdik. Daha öneki çalışmalar bakıldığında örnek bir X firması kurularak hayali bir kuruluşu kendi araştırmalarımıza göre şekillendirildiğini gördük. Biz ise bilgi güvenliği sertifikası alarak kendini ispatlamış ve adının açıklanmasından rahatsızlık duymayacak kuruluşlarla araştırmamızı tamamlamayı düşündük. Bu sayede diğer BGYS kurulumu yapmayı hedefleyen kuruluşların ve bu konuda çalışma yapmak isteyen araştırmacıların cesaretleneceğini düşündük. Yaptığımız araştırmalar neticesinde elde edilen teorik bilgilere dayanarak, mülakat için önceden sorular hazırladık. İlk yaptığımız mülakatta sorulara cevap buldukça farklı konularda daha önce hiç duymadığımız ayrıntılar su yüzüne çıkmaya başladı. Mülakat esnasında görüşme yaptığımız kişilerin rahat davranışları ve konuya olan hâkimiyetleri bizleri önceden belirlediğimiz soru kalıplarının dışına çıkmamıza sevk etti. Teori ile işleyiş arasındaki farkları gördükçe görüşmede ele alınan konuların kapsamı daha da zenginleşti.

İkinci mülakatımızda daha tecrübeli ve ilk kuruluşla kıyaslama imkânı bularak görüşmemizi gerçekleştirdik. Burada da çalışanlar tarafından bize samimiyetle belirtilen hususlar farklı bir bakış açısı kazandırdı. İkinci mülakat yaptığımız kuruluşun sertifika

kapsamı sadece bilgi işlem birimini kapsamaktaydı. Biz her iki kurumun sertifikalarını defalarca incelememize rağmen bunun farkına varamamıştık. Mülakat esnasında bilgi işlem personelinin bize sertifikalarının kapsamını ayrıntılı bir şekilde açıklaması sonucunda sertifikayı tekrar inceleyip aradaki farkı anlayabildik. Yapmış olduğumuz mülakatlar bakmak ile görmek arasındaki farkı bize gayet iyi açıklamış oldu.

Yapılan mülakatlar neticesinde bilgi güvenliği konularının teoride ve pratikte aynı anda yürütülmezse aksak kalacağını bir kez daha anlamış olduk. Mülakatlar sonrasında yapılacak çalışmanın kapsamı genişleyerek, çalışmalarımız yeniden değerlendirmeye alındı. Sonuç olarak ilk defa gerçek belge sahibi kuruluşlarla yaşanan sürecin içeriği ve çıkarılan dersleri kapsayacak şekilde pratik çözümlerle ülkemizdeki reel tabloyu ortaya koymaya çalıştık. ISO27001 standardının yeni oluşturulan sürümünü yakın bir zamanda ülkemize göreceğiz. Biz araştırmamızda bu sürüm ile ilgi bilgileri genellikle çeviri yaparak sunmaya çalıştık. İlerleyen günlerde yeni sürümle ilgili açıklamalarımızın birebir olmasa da, yakın anlamlarla tercüme edilerek kamuoyuna sunulacağını değerlendirmekteyiz. Ortaya çıkan bu araştırmanın her bölümü başlı başına araştırma yapılabilecek konuları içermektedir. Bu sebepten dolayı araştırmacıların bu tezi irdelerken bu hususu da değerlendirmeleri faydalı olacaktır. Her bölümde yapılan açıklamaların yanı sıra konunun ayrıntıları için hangi kaynaklara başvurulması gerektiğini açıklayıcı bilgilerde bu maksatla verilmiştir.

KAYNAKLAR

Akyol, F. (2013), *COBIT (Bilgi ve İlgili Teknolojiler İçin KONTROL Hedefleri) Uygulayan Şirketlerdeki Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçlere Etkileri*, Beykent Üniversitesi, Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Alasulu, N.(2012), *Bilgi Güvenliği ve Kalite Yönetim Sistemleri Arasındaki İlişkinin İncelenmesi ve Bir Uygulama*, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Elazığ.

Annex sl, IRCA Briefing Note Annex SL, www.irca.org (17.03.2014).

Aslandağ, K. (2010), *Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri İle Şirket Performansı İlişkisine Dair Bir Uygulama*, Gebze Yüksek Teknoloji Üniversitesi, Yayınlanmamış Yüksek Lisans Tezi, Gebze.

Bahşi, H., (2010),"*Bilişim Sistemleri Güvenliğinde Yeni Eğilimler*", http//uekae.tubitak.gov.tr (10.02.2014).

Bahşi, H. ve B. Karabacak, (2014), *Ulusal Bilgi Sistemleri Güvenlik Programı*, TÜBİTAK-Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, http://www.emo.org.tr (10.02.2014)

Baykara, M., Daş, R. ve İ. Kardoğan, (2013), "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", *1st International Symposium on Digital Forensics and Security*, Elazığ, ss:231-239.

Bilgi Güvenliği Eğitimleri, (2014), "*ISACA, Denetim, Güvence ve Kontrol Uzmanları için Türkçe BT Standartları, Kılavuzları, Araç ve Teknikleri' nin Basımını Yayınladı*", www.isaca.org/cobit (22.03.2014).

Bilgi Kavramı, http://www.meb.gov.tr/AolKitaplar/Felsefe_1/2.pdf//(16.12.2013).

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

Bragg, B. (2011), "Common ISO 27001 Gaps" , *ISSA Journal*, ss:37-40.

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

Clarke, R.A. and R.K.Knake,(2010) *Siber Savaş*, (çev.) M. Erduran, İkü Yayınevi, İstanbul.

Cisco, (2012) "BYOD (Kendi Cihazını Getir): Küresel Bir Perspektif", *Anket Raporu* www.cisco.com (10.03.2014).

COBIT, (2000), *Control Objective*, www.isaca.org/cobit (21.02.2014).

COBIT 4.1 (Control Objectivesfor Information and Related Technology), (2007), *Framework Control Objectives Management Guidelines Maturity Models*, IT Governance Institute.

COBIT (2013), *Framework*, www.isaca.org/cobit (17.12.2013).

Çalıkuşu, F., Karamehmet, B., Denizci, Ö.M.,(2011), "Bilgi Güvenliği Yönetim Sistemi Kapsamında Risk Yönetimi Modeli", http://www.farukcalikusu.com/BGYS.pdf, (19.09.2011).

Dinçkan, A.(2007), *Bilgi Güvenliği Yönetim Sistemi Kurulumu*, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, İç Yayın, Ankara.

Disterer, G. (2013), "ISO/IEC 27000,27001 and 27002 for Information Security Management", *Journal of Iinformation Security*, April 2013, ss.92-100.

Doğantimur, F.(2009), *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği*, Yayınlanmamış Mesleki Yeterlilik Tezi, T.C. Maliye Bakanlığı, Ankara.

Eminağaoğlu, M. (2008), "Dikkat Casus Var!", Bilgi Güvenliği Yazı Dizisi. *Tekborsa Dergisi*, S:15-21 Haziran 2008, İstanbul.

Eminağaoğlu, M., ve Y. Gökşen,(2009), "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, C:11, S:4, ss.01-15.

Emiral, F. (2004), "Bilgi Güvenliği Bilincinin Genele Yayılması", *Deloitte.*

Ersnt&young, (2012),"Küresel Bilgi Güvenliği Anketi, "Dikkat! Kaçak Var!", *Basın Bülteni*.

Eskiyörük, D.(2007), *Risk Yönetim Süreci Kılavuzu*, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, İç Yayın, Ankara.

Eskiyörük, D.(2008), *Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Kılavuzu*, Sürüm 1.00, UEKAE, TÜBİTAK, Gebze.

Evrin, V. (2011), *Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği*, Hacettepe Üniversitesi Bilişim Hukuku Tezsiz Yüksek Lisans Programı Yayınlanmamış Proje Raporu, Ankara.

Evrin, V. ve M. Demirer, (2011), "Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO 27001 Örneği", *IV. Ağ Ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı*, ss:38-43.

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

Gemci, C. (2010), *Uzman Sistem Temelli Bilgi Güvenliği Yönetim Sistemi Yaklaşımı*, Gazi Üniversitesi, Bilişim Enstitüsü, Yayınlanmamış Doktora Tezi, Ankara.

Gemci, C. ve Ö. F. Bay, (2014), *Yapay Zeka Temelli Bilgi Güvenliği Yönetim Sistemi Yaklaşımı*, www.emo.org.tr (15.03.2014)

Gökçe, A. ve C. Kültür, (2014), "*Bir E-Öğrenme Uygulaması: Bilgi Güvenliği Bilinçlendirme*" www.bilgimikoruyorum.org.tr (11.03.2014).

Gülmüş, M. (2010), "*Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği*", Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Haklı, T.m (2012), *Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi*, Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Isparta.

Humphreys, T., ISMS Standarts The ISO 27000 Familyand BS7799-2 ", ISMS International User Group Seminar.

Humphreys,T. and P. Angelika, (2005), *Guide Totheımplementationnand Auditing of ISMS Controlsbased on ISO/IEC 27001*, British Standards Institution.

Introducing the official COBIT 5 Accreditation and Qualifications Scheme, *ISACA*., (2010), *COBIT, Val IT and Risk IT — Synergistic Relationship*.

ISO (2013), *Survey*, www.iso.org (19 Aralık 2013).

ISO 27001, (2013), *Information Security Management Systems* — Requirements, Switzerland.

ISO 27006 *Bgys Denetimini ve Belgelendirmesini Yapan Kuruluşlar İçin Gereksinimler*, Ankara.

ISO 27799, (2008), *Information Security Management in Health Using ISO/IEC 27002*, Switzerland.

ISO/IEC 27000, (2012), *Bgys Genel Bakış ve Sözlük*, Ankara.

ISO/IEC 27005. (2008), *Information Technology–Security Techniques–Information Security Risk Management*. ISO.

ISO/IEC 27035, (2013), *Information Security Incident Management*, Switzerland.

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

ITIL, (2014), *Overview,* www.itil.org (17.02.2014).

ITIL Çalıştayı, (2011), *ITIL: Bilişim Teknolojileri Hizmet Yönetimi* http://ise.atilim.edu.tr/ (12.04.2013)

ITIL, (2013), *Terim ve Tanımlar Sözlüğü,* Axelos Limited, E-Kitap.

İbrişim, A. (2008). *TS ISO 27001 Bilgi Güvenliği Yönetim Sistemi Eğitim Notları*, Türk Standartları Enstitüsü, Ankara.

Karpuz, F., A. Akay ve M. Yazıcı, (2013), "Bilgi İletişim Teknolojilerinin Faydalı Kullanımında Meslek Yüksekokulu Öğrencilerinin Farkındalıkları" ,*Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* ,Yıl:2013/1, Büro Yönetimi Özel Sayısı, ss:129-145.

Kandemirli, B. M. (2011), *Bilgi Teknolojileri Güvenliği ve Sigorta Şirketinde ISO/IEC 27001 Standartları Çerçevesinde Bilgi Güvenlik Yönetim Sistemi Uygulaması*", Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Karabacak B. (2009), "Kurumsal Bilgi Güvenliğinde Etkin Risk Analizi", *Bilgi Güvenliği Kapısı* (ww.bilgiguvenligi.gov.tr/risk-analizi/kurumsal-bilgi-guvenliginde-etkin-risk-analizi-3.html)

Karabacak B. ve S. Özkan, (2010), ISO 270001:*2005 Bilgi Güvenliği Yönetimi Sistemi için Süreç Tabanlı Risk Analizi*, Orta Doğu Teknik Üniversitesi Enformatik Enstitüsü, Ankara.

Koç, F. (2008), *BGYS - Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu*, Sürüm 1.00, UEKAE, TÜBİTAK Gebze.

Kosutic, D. (2012),*9 Steps to Cyber Security*, EPPS Services Ltd, Zagreb.

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

Kumaş, E. ve B. Birgören, (2010), "E-Devlet Kapısı Projesi Bilgi Güvenliği ve Risk Yönetimi: Türkiye Uygulaması*", Bilişim Teknolojileri Dergisi*, C:3, S:2, ss.29-35.

Mart, İ. (2012), *Bilişim Kültüründe Bilgi Güvenliği Farkındalığı*, Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Kahramanmaraş.

Mataracıoğlu, T. (2014), *657 Sayılı Kanunda Yer Alan Maddelerle ISO 27001 Standardındaki Maddelerin Haritalanması*, https://www.bilgiguvenligi.gov.tr (18.03.2014).

Mataracıoğlu, T. (2014), *Sosyal Mühendislik*, https://www.bilgiguvenligi.gov.tr (10.03.2014).

Mete, H. (2010), *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin Bilgi İşlem Merkezlerinde Uygulanması*, Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Sakarya.

Mitnick, K. D. (2005*), Aldatma Sanatı*. ODTÜ Geliştirme Vakfı Yayıncılık, 1. Basım.

Ottekin, F. (2011), "BGYS ve BGYS Kurma Deneyimleri", *6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı*, Ankara.

Ottekin, F. (2008), *ISO/IEC 27001 Denetim Listesi,* Sürüm 1.00, UEKAE, TÜBİTAK, Gebze.

Önel, D. (2008), *Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu*, Sürüm 1.00, UEKAE, TÜBİTAK, Gebze.

Özbilgin, İ.G. ve M. Özlü (2014), *Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi*, www.ab.org.tr (16.01.2014)

Özcan, B. (2009), *Kurumsal Bilgi Güvenliği,* Haliç Üniversitesi, Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi.

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

Öztürk, G., (2008), *Bilgi Güvenliği Politikası Oluşturma Kılavuzu*, Sürüm 1.00, UEKAE, TÜBİTAK, Gebze.

Perendi, Ü.,(2008), *Bgys Kapsamı Belirleme Kılavuzu*, Sürüm 1.00, UEKAE, TÜBİTAK, Gebze.

Saliba, R. (1998), *Callio Secura 17799 - A Tool for İmplementing the ISO 17799 / BS7799.*

Schmidt, A. H. (2004), "Building a Mosaic of Securityfor a Betterworld", *Security Matters*, AspatoreBooks, U.S.A.

Siber Güvenlik, (2014), http://sge.bilgem.tubitak.gov.tr/ (10.01.2014).

Şahinaslan, E. (2010), *Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının*

Geliştirilmesi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Doktora Tezi, Edirne.

Tanrıkulu, C. (2011), "Bilgi Sistem Yöneticilerinin Hukuki Yükümlülükleri", *6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı*, Ankara.

Tipton H. and F, Krause M. (2007), *Information Security Management Handbook*, Auerbach Publicaions.

Tok, H. (2010), *Kamu Kurumları İçin Bilgi Güvenliği Yönetişim Modeli*, Gebze Yüksek Teknoloji Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi.

TS ISO/IEC 20000–1,(2011), Hizmet Yönetimi Standardı, Ankara.

TS ISO/IEC TR 18044,(2007), *Bilgi Güvenliği İhlal Olayı Yönetimi*, Ankara.

TS ISO/IEC 27001 (Mart 2006), *Bilgi Teknolojisi –Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler*, Türk Standartları Enstitüsü, Ankara.

TSE Guide 13268-1, (2009), *TS ISO/IEC 27001'i Esas Alan Bilgi Güvenliği Yönetim Sistemi (Bgys) Kontrollerinin Gerçekleştirilmesi ve Denetlenmesi Kılavuzu*, Ankara.

Tuğlular, T. (2003), "Üniversitelerde Bilgi Güvenliği Politikaları", *Ulaknet Sistem Yönetimi Konferansı.*

UEKAE, "*BOME Eğitim*", http://csirt.ulakbilm.gov.tr/ (15.02.2014).

ULAK-CSIRT Deneyimi, http://csirt.ulakbim.gov.tr, (15.03.2014).

Uzunay, V. (2007), *COBIT (Control Objectives for Information and related Technology)*, İç Kontrol Merkezi Uyumlaştırma Dairesi, Yayınlanmamış Mesleki Yeterlilik Tezi, Ankara.

Vardal, N. (2009), *Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi İçin Bir Model Önerisi ve Uygulaması*, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Yayınlanmamış Doktora Tezi, Ankara.

Vural, Y. ve Ş. Sağıroğlu, (2007), "Kurumsal Bilgi Güvenliği: Güncel Gelişmeler", *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, Ankara, ss:191-199.

Vural, Y. (2007), *Kurumsal Bilgi Güvenliği ve Sızma Testleri*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, , Ankara.

Vural, Y. ve Ş. Sağıroğlu,(2008), "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme*", Gazi Üniversitesi. Mühendislik-Mimarlık Fakültesi Dergisi*, , C:23, No: 2, ss:507-522.

Yeni Türk Ceza Kanunu–Yeni TCK. 5237 Sayılı Kanun.

Yıldız, B. (2007), *Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması*, Gebze Yüksek Teknoloji Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Zobi, A. (2008), *TS ISO /IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi ve KOSGEB'de Uygulaması*, *KOSGEB*, Yayınlanmamış Uzmanlık Tezi, Ankara.

EK 1: BGYS DENETİMLERİ ESNASINDA OLUŞTURULAN GERÇEK DÖF ÖRNEKLERİ

	TETKİK UYGUNSUZLUK FORMU *Audit Discrepancy Form*	TARİH : 01.10.2010 *Date*

Baş Tetkikçi/Tetkikçi Tarafından Doldurulacaktır - *This area filled by Lead Auditor / Auditor*	
RAPOR NO *Report Number*	
UYGUNSUZLUK NO *Discrepancy Number*	01
REFERANS STANDARD *Reference Standart*	ISO/IEC 27001:2005
STD. MADDE NO *Standart Clause Number*	4.2
İLGİLİ PROSEDÜR V.B. NO *Related Procedure Number*	

UYGUNSUZLUK SINIFI *Discrepancy Kind* ☐ MAJOR ☒ MİNÖR

TAKİP TETKİKİ GEREKLİLİĞİ VAR MI ? *Is there a need to follow up audit* ☐ EVET / *YES* ☒ HAYIR / *NO*

AÇIKLAMA / *Comment*

Kabul edilebilir risk seviyesinin net bir şekil ifade edilmediği görülmüştür.

BAŞ TETKİKÇİ / TETKİKÇİ : *Lead Auditor/Auditor*	YÖNETİM TEMSİLCİSİ : *Management Representative*
İMZA : *Signature*	İMZA : *Signature*

Müşteri Tarafından Doldurulacaktır - *This area filled by customer*

UYGUNSUZLUK KÖK NEDEN ANALİZİ – *Discrepancy main cause analyse*

UYGUNSUZLUĞUN TEKRARINI ÖNLEMEK İÇİN YAPILACAK FAALİYET - *Corrective action to prevent the discrepancy*

KAPATMA SÜRESİ : *Completion Target* KAPATILMA TARİHİ : *Completion Date*	YÖNETİM TEMSİLCİSİ : *Management Representative* Tarih : *Date* İmza : *Signature*

Baş Tetkikçi Tarafından Doldurulacaktır - *This area filled by Lead Auditor*

DÜZELTİCİ FAALİYET SONUÇ DEĞERLENDİRMESİ - *Evaluation result of corrective action*

FAALİYET SONUCU : *Action Result* ☐ YETERLİ *Suitable* ☐ YETERSİZ *Nonsuitable*	BAŞ TETKİKÇİ : *Lead Auditor* Tarih : *Date* İmza : *Signature*

FR-31, Rev:03, 15.01.2010

	TETKİK UYGUNSUZLUK FORMU *Audit Discrepancy Form*	TARİH : 01.10.2010 *Date*

Baş Tetkikçi/Tetkikçi Tarafından Doldurulacaktır - *This area filled by Lead Auditor / Auditor*	
RAPOR NO *Report Number*	
UYGUNSUZLUK NO *Discrepancy Number*	02
REFERANS STANDARD *Reference Standart*	ISO/IEC 27001:2005
STD. MADDE NO *Standart Clause Number*	A.7.2.1
İLGİLİ PROSEDÜR V.B. NO *Related Procedure Number*	

UYGUNSUZLUK SINIFI *Discrepancy Kind* ☐ MAJOR ☒ MİNÖR

TAKİP TETKİKİ GEREKLİLİĞİ VAR MI ? *Is there a need to follow up audit* ☐ EVET / *YES* ☒ HAYIR / *NO*

AÇIKLAMA / *Comment*

27.09.2010, PR.7.2.2-01 Kullanıcı kimliği, E-posta, Bilgisayar İsmi Tanımlama dokümanında basılı dokümanların sınıflandırma metodolojisi görülmüştür. Fakat tüm bilgi varlıkları için sınıflandırmanın yapılmadığı gözlemlenmiştir.

BAŞ TETKİKÇİ / TETKİKÇİ : *Lead Auditor/Auditor*	YÖNETİM TEMSİLCİSİ : *Management Representative*
İMZA : *Signature*	İMZA : *Signature*

Müşteri Tarafından Doldurulacaktır - *This area filled by customer*

UYGUNSUZLUK KÖK NEDEN ANALİZİ – *Discrepancy main cause analyse*

UYGUNSUZLUĞUN TEKRARINI ÖNLEMEK İÇİN YAPILACAK FAALİYET - *Corrective action to prevent the discrepancy*

KAPATMA SÜRESİ : *Completion Target* KAPATILMA TARİHİ : *Completion Date*	YÖNETİM TEMSİLCİSİ : *Management Representative* Tarih : *Date* İmza : *Signature*

Baş Tetkikçi Tarafından Doldurulacaktır - *This area filled by Lead Auditor*

DÜZELTİCİ FAALİYET SONUÇ DEĞERLENDİRMESİ - *Evaluation result of corrective action*

FAALİYET SONUCU : *Action Result* ☐ YETERLİ *Suitable* ☐ YETERSİZ *Nonsuitable*	BAŞ TETKİKÇİ : *Lead Auditor* Tarih : *Date* İmza : *Signature*

FR-31, Rev:03, 15.01.2010

	TETKİK UYGUNSUZLUK FORMU *Audit Discrepancy Form*	TARİH : 01.10.2010 *Date*

Baş Tetkikçi/Tetkikçi Tarafından Doldurulacaktır - *This area filled by Lead Auditor / Auditor*	
RAPOR NO *Report Number*	
UYGUNSUZLUK NO *Discrepancy Number*	03
REFERANS STANDARD *Reference Standart*	ISO/IEC 27001:2005
STD. MADDE NO *Standart Clause Number*	A.7.2.2
İLGİLİ PROSEDÜR V.B. NO *Related Procedure Number*	

UYGUNSUZLUK SINIFI *Discrepancy Kind* ☐ MAJOR ☒ MİNÖR

TAKİP TETKİKİ GEREKLİLİĞİ VAR MI ? *Is there a need to follow up audit* ☐ EVET / *YES* ☒ HAYIR / *NO*

AÇIKLAMA / *Comment*

Basılı dokümanlarda etiketleme yapıldığı fakat diğer bilgi varlıklarında etiketleme yapılmadığı görülmüştür.

BAŞ TETKİKÇİ / TETKİKÇİ : *Lead Auditor/Auditor*	YÖNETİM TEMSİLCİSİ : *Management Representative*
İMZA : *Signature*	İMZA : *Signature*

Müşteri Tarafından Doldurulacaktır - *This area filled by customer*

UYGUNSUZLUK KÖK NEDEN ANALİZİ – *Discrepancy main cause analyse*

UYGUNSUZLUĞUN TEKRARINI ÖNLEMEK İÇİN YAPILACAK FAALİYET - *Corrective action to prevent the discrepancy*

KAPATMA SÜRESİ : *Completion Target* KAPATILMA TARİHİ : *Completion Date*	YÖNETİM TEMSİLCİSİ : *Management Representative* Tarih : *Date* İmza : *Signature*

Baş Tetkikçi Tarafından Doldurulacaktır - *This area filled by Lead Auditor*

DÜZELTİCİ FAALİYET SONUÇ DEĞERLENDİRMESİ - *Evaluation result of corrective action*

FAALİYET SONUCU : *Action Result* ☐ YETERLİ *Suitable* ☐ YETERSİZ *Nonsuitable*	BAŞ TETKİKÇİ : *Lead Auditor* Tarih : *Date* İmza : *Signature*

FR-31, Rev:03, 15.01.2010

EK 2: MÜLAKAT YAPILAN KURULUŞLARIN SAHİP OLDUKLARI ISO27001 BGYS SERTİFİKALARI

INTERNATIONAL REGISTRARS
QA TECHNIC

CERTIFICATE OF REGISTRATION

T.C. PENDİK BELEDİYESİ

BATI MAH. 23 NİSAN CD. NO:11 34890 PENDİK İSTANBUL

Sertifika No: AQ/ 27001/008

Yukarıda adı geçen kuruluş, aşağıda belirtilen kapsamda bir bilgi güvenliği yönetim sistemi yürürlüğe koymuş ve uygulamakta olup ilgili kalite standardına uygunluğu ALBERK QA TEKNİK tarafından onaylanmıştır.

ISO/IEC 27001:2005

BİLGİ İŞLEM VARLIKLARI VE SÜREÇLERİ

UYGULANABİLİRLİK BİLDİRGESİ 10.09.2010 TARİH (REVİZYON NO:1)

Bu belge, firma ISO 27001:2005 standardının gerekliliklerini yerine getirdiği ve ALBERK QA TEKNİK'e karşı sorumluluğunu taşıdığı sürece geçerlidir.

Sertifika Düzenleme Tarihi : 08 Ekim 2010
Sertifikasyon Bitiş Tarihi : 08 Ekim 2013
Sertifika Geçerlilik Tarihi : 08 Ekim 2011
Belgelendirme Periyodu : 3 Yıl

Genel Müdür
Latif Murat YILMAZ

ALBERK QA ULUSLARARASI TEKNİK KONTROL VE BELGELENDİRME LTD. ŞTİ.
Fevzipaşa Cad. No:59 Kandiş Plaza
K:4 D:4 K.Bakkalköy/İstanbul/ TÜRKİYE
Tel : 0216 572 49 10-11-12
Fax : 0216 572 49 14
www.qatechnic.com

FOR BUSINESS IMPROVEMENT
QA TECHNIC

TÜRKAK
Bilgi Güvenliği Y. S.
TS EN ISO IEC 17021
AB-0022-YS

Kalitest

SERTİFİKA–CERTIFICATE OF REGISTRATION

Bu sertifika aşağıdaki kuruluşa
This certificate has been awarded to the company

KEÇİÖREN BELEDİYESİ
BİLGİ İŞLEM MÜDÜRLÜĞÜ

Cumhuriyet Caddesi No:1 Kalaba Keçiören/ANKARA

Uygulanmakta olan bilgi güvenliği yönetim sisteminin
To certify that the implemented information security management system complies with

ISO/IEC 27001:2005

Standardına uygunluğunu belgelendirmek amacı ile aşağıdaki kapsamda verilmiştir.
For the activities described below

Belediyecilik Hizmetleri Sunumunda Kullanılan Bilgi İşlem Faaliyetlerine Yönelik Teknik Destek Yönetimi

Technical Support Management for Data Processing Operations Be Used To Present Municipal Services

SOA Rev 00

Sertifika No: K-BG-1008
İlk Belge Tarihi: 04.03.2013
Belge Periyodu: 3 yıl
Sertifika Tarihi: 04.03.2013
Bitiş Tarihi: 04.03.2016

Kalitest Belgelendirme ve Eğitim Hizmetleri Ltd. Şti.

İmza / Signed

T.C.
BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖĞRENCİ ÖZGEÇMİŞ FORMU

Fotoğraf

Adı-Soyadı	İsmayil Gökhan AKAY		
Lisans Öğrenimi	Kara Harp Okulu / Sistem Mühendisliği	**Doğum Yeri**	Balıkesir
Yüksek Lisans Öğrenimi	Bilecik Şeyh Edebali Üniversitesi / İşletme Anabilim Dalı	**Doğum Tarihi**	26.08.1985

İLETİŞİM BİLGİLERİ

ADRES

GSM: 505 7036605 E-Posta: igakay@gmail.com