T.C.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC/ ISO 27001 Standartının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi

YÜKSEK LİSANS TEZİ

Seyda Emir Erdoğan

1600007180

Anabilim Dalı: İşletme

Program: İşletme – Uzaktan Öğretim

Tez Danışmanı: Dr. Öğr. Üyesi Özgür ATILGAN

OCAK, 2020

T.C.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Bilgi Güvenliği Yönetim Sisteminin Oluşturulması, IEC/ISO 27001 Standartının Bir Sivil Havacılık Kurumunda Hayata Geçirilmesi

YÜKSEK LİSANS TEZİ

Seyda Emir Erdoğan

1600007180

Anabilim Dalı: İşletme

Program: İşletme – Uzaktan Öğretim

Tez Danışmanı : Dr. Öğr. Üyesi Özgür ATILGAN

Jüri Üyeleri : Dr. Öğr. Üyesi Murat Taha BİLİŞİK

Dr. Öğr. Üyesi Özge Nalan BİLİŞİK

OCAK 2020

ÖNSÖZ

Bilgi, günümüzün en değerli hazinesidir. Bu nedenle, bilginin korunması, güvenliğinin sağlanması herkes için önem arz etmektedir. Gelişen teknoloji ile birlikte bilginin muhafaza edilmesi için kullanılan yöntemlerde değişmiştir. Günümüzde, bilgi basılı olarak muhafaza edilmesinin yanı sıra elektronik ortamlarda da sıklıkla muhafaza edilmektedir. Teknolojik fırsatlar ve kazanç sağlaması açısından bilgi elektronik ortamlarda tutulmakta ve işlenmektedir. Bu durum, fırsatların yanında bazı önemli risklerde getirmektedir. Bilgiye olan erişimin kontrolü, kimler tarafından kullanıldığı, kötücül faaliyetler için kullanıldığı veya saldırganların eline geçmesi bu risklere örnek olarak verilebilir.

Her geçen gün bilgi güvenliğini tehdit eden yeni yazılımlar, saldırganlar ve saldırılar yayınlanmaktadır. Bu kötücül faaliyetler siber casusluk, kuruluşları zarara uğratma, veya çıkar amaçlı yapılmaktadır. Bilgi güvenliği saldırılarının tespit edilerek, yönetilmesi kurumların bilgi güvenliğini tüm iş süreçlerine entegre etmesi bu saldırıların olumsuz sonuçlarını azaltmaktadır. Özellikle, büyük ölçekli kuruluşlarda böyle bir yapıyı işletmek için yönetimin desteği alınmalı, tüm süreçler belirlenmeli, dökümante edilmeli ve bir yönetim sistemi oluşturulmalıdır. ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standartı, bir kuruluşun bilgi güvenliği yönetim sistemini nasıl oluşturması ve yönetmesi gerektiğine dair tüm yönleriyle bir çerçeve çizmektedir. Tüm gereklilikleri yerine getiren kuruluşlar yapılan belgelendirme denetiminde başarılı olmaları durumunda ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi sertifikasını almaya hak kazanmaktadır. Bu çalışmada ISO/IEC 27001:2013 standartına bir sivil havacılık kuruluşunun nasıl uyumlu olacağı, neler yapması gerektiği konuları ele alınmıştır.

Tez araştırmamda ve gerçekleştirilmesinde tavsiyeleriyle beni yönlendiren danışmanım Dr. Öğr. Üyesi Özgür ATILGAN'a, desteklerini esirgemeyen Didar Aysev KAYADENİZ'e teşekkürlerimi sunarım.

Sevgilerini esirgemeyen değerli eşim, annem, babam ve kardeşime sonsuz teşekkür ederim.

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

Enstitüsü : Lisansüstü Eğitim Enstitüsü

Dalı : İşletme

Programı : İşletme Uzaktan Öğretim Tezli Yüksek Lisans

Tez Danışman : Dr. Öğr. Üyesi Özgür ATILGAN

Tez Türü : Yüksek Lisans

ÖZET

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN OLUŞTURULMASI, IEC/ISO 27001 STANDARTININ BİR SİVİL HAVACILIK KURUMUNDA HAYATA GEÇİRİLMESİ

SEYDA EMİR ERDOĞAN

Günümüz gelişen teknolojisinde ve rekabetçi pazar koşullarında kuruluşların en değerli varlıklarından bir tanesi şüphesiz sahip olduğu bilgilerdir. Bu bilgilerin kötücül amaçlar besleyen kişilerin eline geçmesi veya çeşitli tehditlerin meydana gelmesi durumunda kuruluşlar maddi anlamda zarara uğrayacaktır. Dijital veya basılı olarak işlenen, saklanan bilginin uygun güvenlik süreçleri tanımlanarak koruma altına alınması oluşabilecek zararları en aza indirmektedir. Özellikle havayolu firmaları gibi ülkelerin stratejik öneme sahip kuruluşları kötü niyetli kişiler tarafından sıklıkla hedef alınmaktadır. Hassas bilgilere sahip olan sivil havacılık kuruluşlarının, bilgi güvenliği unsurlarını dikkate alarak, etkinliği sürekli denetlenen bir bilgi güvenliği yönetim sistemi oluşturması gerekmektedir.

Bilgi güvenliği yönetim sisteminin oluşturulması konusunda gereken tüm maddeleri içeren IEC/ISO 27001 standartı kuruluşlara bir çerçeve sunmaktadır. IEC/ISO 27001 standartı Sivil Havacılık Genel Müdürlüğü'nün yayınlamış olduğu bir genelge ile tüm kurumlara zorunlu hale gelmiştir. Bu nedenle, sivil havacılık kuruluşları IEC/ISO 27001 standartına sadece bilgi güvenliği'ne uygun bir yapının oluşturulması için değil SHGM tarafından yayınlanan genelgeye uygunluk sağlanabilmesi için uyumlu hale gelmelidir.

Kuruluşlar, IEC/ISO 27001 standartını uygulayarak bilgi güvenliği yönetim sisteminin hedeflenen çıktılarını tüm personele ve paydaşlara duyurmalı ve kurum genelinde bilgi güvenliği farkındalığı oluşturmalıdır. Kapsam içerisinde bulunan birimlerin risk ve fırsatları ele alarak değerlendirmeli, ve uygun risk işleme seçenekleri uygulanmalıdır. BGYS'nin hedeflenen çıktıları denetlenerek sürekli iyileştirme yapılmalıdır. IEC/ISO 27001 standartının maddeleri uygulanarak bir bilgi güvenliği yönetim sisteminin sivil havacılık kuruluşunda nasıl uygulanacağı araştırılmıştır. Bu amaçla, IEC/ISO 27001 standartına sahip olan Türkiye'nin bayrak taşıyıcısı Türk Hava Yolları A.O esas alınarak bilgi güvenliği müdürlüğü yönetişim ekibi ile mülakat çalışması gerçekleştirilmiştir. Yapılan mülakat sonucunda bilgi güvenliği yönetim sisteminin oluşturulması için önemli noktalar tespit edilmiştir.

Anahtar Kelimeler: BGYS, SHGM, Bilgi Güvenliği, IEC/ISO 27001 Standartı

Institude : Institude of Graduate Education

Department : Business Administration

Programme : Master of Business Administration

Supervisor : Asst. Prof. Dr. Özgür Atılgan

Degree Awarded : Master Thesis

ABSTRACT

BUILDING AN INFORMATION SECURITY MANAGEMENT SYSTEM, IMPLEMENTATION OF IEC / ISO 27001 STANDARD IN A CIVIL AVIATION ORGANIZATION

SEYDA EMİR ERDOĞAN

In this technological era and competitive market conditions, information is undoubtedly one of the most valuable assets of the institutions. In the event that malicious people capture information of the institutions, or if various threats are occurred, will cause negative effects on these institutions, like damaging their economies. However, identifying appropriate security processes for stored information, processed digitally or wirelessly, minimizes damages that need to be managed with protection. The organizations that have strategical importance for nation-states are especially targeted by cyber attackers around the world. Therefore, civil aviation organizations, which have sensitive information, should establish an information security management system that is continuously monitored by taking into consideration the information security elements.

IEC / ISO 27001 standard, which includes all the necessary elements for the establishment of an information security management system, provides a framework for organizations. The IEC / ISO 27001 standard has become mandatory for all institutions with a circular issued by the General Directorate of Civil Aviation in Turkey. Therefore, civil aviation organizations should comply with the IEC / ISO 27001 standard not only for the creation of a structure that complies with information security, but also for compliance with the circular issued by the SHGM.

By implementing the IEC / ISO 27001 standard, organizations should communicate the targeted outputs of the information security management system to all staff and stakeholders and raise information security awareness throughout the organization. The units within the scope should be evaluated by considering risks and opportunities, and some appropriate risk processing options should be applied. Continuous improvement should be made by monitoring the targeted outputs of ISMS. The provisions of the IEC / ISO 27001 standard were applied, and how an information security management system is implemented in a civil aviation organization was investigated. For this purpose, IEC / ISO 27001 standard with Turkey's flag carrier Turkish Airlines A.O director of information security governance based on interviews with team work was carried out. As a result of the interview, important points were determined for the establishment of information security management system.

Keywords: ISMS, SHGM, Information Security, IEC/ISO 27001 Standart

GİRİŞ

Günümüzde kuruluşların şüphesiz sahip oldukları en değerli varlık bilgidir. Bu bilgilere kuruluşun ticari ve finansal verileri işlevini devam ettirebilmek için müşterilerden alınan kişisel veri gibi hassas veriler örnek olarak verilebilir. Teknolojinin gelişmesi ile birlikte şirketler tarafından bilgilerin kullanılması, iştirak firmalara iletilmesi, üçüncü taraf firmalar ile paylaşılması ve saklanması işlemlerinde birtakım değişiklikler olmuştur. Özellikle, dijital çözümlerin sağladığı avantajlardan dolayı kuruluşlar bu yöntemlere sıklıkla başvurmaktadır. Operasyonel maliyetlerin azalması, süreçlerin otomatize edilebilmesi, daha geniş müşteri kitlesine ulaşabilmesi gibi avantajlardan dolayı sivil havacılık sektöründe yer alan firmalar için de önem arz etmektedir.

Dijital ve basılı duran bilgilerin kötücül aktivitelere karşı muhafaza edilebilmesi kuruluşların dikkat etmesi gereken önemli noktaların başında gelmektedir. Kötücül aktiviteler ve doğal etkenlerden kaynaklı tehditler sonrasında gerekli önlemi almamış olan kuruluşlar ciddi maddi ve itibari olumsuz sonuçlar ile karşılabilmektedirler. Bu nedenle, kuruluşlar bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişilebilirlik konularını dikkate alarak bir bilgi güvenliği yönetim sistemi oluşturmalıdırlar. Bilgi güvenliği tehditlerinin önemini vurgulayan otoriteler yayınladıkları genelgeler ile bilgi güvenliği yönetim sisteminin oluşturulmasını zorunlu kılmıştır. Bu nedenle, sadece tehditlerin oluşturacağı olumsuz sonuçlardan kaçınmak için değil, otorite kuruluşların yayınladıkları genelgelere uyumlu olmak için bilgi güvenliği yönetim sistemi oluşturulması gerekmektedir.

ISO/IEC 27001:2013, bir bilgi güvenliği yönetim sistemi'nin oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için bir süreç yaklaşımının adapte edilmesi olarak görülebilir. Bu yaklaşım ile planla, uygula, kontrol et ve önlem al modelini benimseterek kuruluşlara bir çerveve sunmaktadır. Standarta göre iç ve dış hususlar kuruluşlar tarafından belirlenerek kapsamı oluşturmalıdır. Kurumsal rol ve sorumlulukları belirleyerek yönetimin desteği ile herkesin uyması ve uygulaması gereken bir politika oluşturmalıdır. Kuruluşun risk ve fırsatlarını dökümante etmeli, ve uygun risk işleme planı hayata geçirmelidir. Bilgi güvenliği yönetim sistemi'nin işleyişini kontrol etmeli ve performans değerlendirmesi yapmalıdır. İç tetkikler yapmalı ve uygunsuzluk görüldüğünde eksik noktalar düzeltilmelidir. Sivil Havacılık

Genel Müdürlüğü(SHGM) tarafından tüm sivil havacılık kuruluşlarının ISO/IEC 27001:2013 standartına uygun bir bilgi güvenliği yönetim sistemi oluşturması zorunlu hale gelmiştir.

Bu çalışmada sivil havacılık kuruluşlarının ISO/IEC 27001:2013 standartına uygun bir bilgi güvenliği yönetim sistemi standartını nasıl oluşturacağı üzerine araştırmalar yapılmıştır. Çalışmada ilk olarak bilgi güvenliğinin önemi vurgulanmış, sivil havacılık kuruluşlarını tehdit edebilecek hususlara değinilmiştir. Daha önceden yaşanmış vakalar örnek olarak sunulmuştur. Sonrasında ISO/IEC 27001:2013 standartının tüm maddeleri detaylı olarak incelenmiş, bu maddelere uygunluğun nasıl sağlanacağı örnekler ile açıklanmıştır.

Türk Hava Yolları A.O'nın ISO/IEC 27001:2013 standartına uygun bir bilgi güvenliği yönetim sistemini nasıl oluşturduğunu, hangi konulara dikkat edilmesi gerektiğini açıklayan bir mülakat çalışması gerçekleştirilmiştir.

1. BİLGİ NEDİR?

Türk Dil Kurumu(TDK)'ya göre bilgi, öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat, vukuf. Yani, bir kişi veya konu hakkında öğrenilen doğruluğu kabul edilmiş olgulardır. Bilgiyi daha iyi ifade edebilmek için veri ile enformasyon kavramlarını da açıklamak gerekmektedir. Veri, ölçüm ya da sayım yolu ile toplanan sayısal değer bildiren ham enformasyon parçacığına verilen addır. Enformasyon, verinin kayda geçirilmiş halidir ve nesneldir. Bilgi ise kayda geçirilmiş enformasyon ve verinin işlenmesi sonucunda elde edilmiş çıktılardır.

Günümüzde bilgi her alanda en önemli bir faktördür. Kuruluşlar sahip oldukları bilgileri işleyerek faaliyetlerini yerine getirir ve var oluşlarını devam ettirirler. Kişiler edindikleri bilgiler ile iş hayatına atılır ve gelir elde ederler. Tüm bunlar dikkate alındığında herkes için bilgi değerlidir ve korunması gerekmektedir.

2. BİLGİ GÜVENLİĞİ NEDİR?

Sürekli gelişen bilişim teknolojileri, bilgilerin işlenmesi, transferi, paylaşılması ve saklanması gibi konularda işletmelere büyük faydalar sağladığı için işletmeler sürekli bu teknolojilere yatırım yapmaktadır. Her sektördeki işletmelerin faaliyetlerine yönelik yazılan uygulamalar, bu uygulamaların hızlı ve etkili bir şekilde çalışması için üretilen donanımlar, işletmelere zaman ve para kazandırdığı için işletmeler teknolojiye bağımlı hale gelmişlerdir. Tüm faaliyetlerini bilişim teknolojileri araç ve gereçleri üzerinden gerçekleştiren işletmelerin basılı halde duran bilgileri dahil elektronik ortamda bulunan tüm verilerinin güvenliğini sağlamak hayati önem taşımaktadır. Bilgiye erişmesi gereken kişilerin sürekli olarak erişim sağlaması, bilginin herhangi bir şekilde tahribata uğramadan, değiştirilmeden, yetkisiz kişilerce zarara uğratılmadan, bilginin yetkisi olmayan kullanıcılar tarafından erişimine izin verilmeyecek gizliliğin muhafaza edilmesi bilgi güvenliği olarak tanımlanabilir (Pfleeger, 1997).

Gelişen teknoloji işletmeler için fayda sağlamasının yanında bazı tehditleri de beraberinde getirmektedir. Bilgi güvenliği, bilginin gizliliğine, bütünlüğüne ve erişilebilirliğine gelebilecek zararları önleyerek sağlanabilir. Bilgi güvenliğinin temelini oluşturan bu üç temel bileşenin yanında inkar edememe, güvenirlilik ve

kimlik yönetimi de alt bileşen olarak eklenebilir. Küçük ölçekli firmalarda bu temel bileşenler kolaylıkla sağlanabilir. Fakat, büyük ölçekli işletmelerde binlerce çalışanın olması, kullanılan cihaz sayısının fazla olması, farklı bölgelerde ofislerin olması bilgi güvenliğinin sağlanmasını zorlaştırmaktadır. Bu nedenle, bilgi güvenliği sadece bilgi güvenliği çalışanlarının sorumluluğunda değil, herkesin sorumluğunda olmalıdır. Bilgi güvenliği sadece bilgi işlem personellerinin sorumluluğunda olan teknik bir husus olmayıp, işletmelerde çalışan tüm personelin sorumluluğundadır. Bilgi güvenliği işletmede herkes tarafından benimsenirse sağlanabilir (Johnson & Goetz, 2007). Bilgi güvenliğini tehdit eden etkenler sadece dış kaynaklı değil, iç kaynaklı da olabilmektedir. Çalışanların yetkilerini kötüye kullarak yanlış işlem ve davranışlar bilgi güvenliğini tehdit edebilmektedir (Thomson, Solms & Louw, 2006). Siber güvenlik araştırmaları ve uygulamaları geliştiren bir firmanın yaptığı araştırmaya göre 2018 senesinde siber saldırıların %46'sının kurum çalışanının sömürülmesi ile başladığı belirtilmiştir (Kaspersky, 2016).

Bilgi güvenliğinin sağlanmasında ki en önemli faktörlerin başında çalışanların bilgi güvenliğinin önemine inanarak, benimsemesidir. Bilgi güvenliğini tehdit eden unsurların değerlendirilmemesi, gerekli önlemlerin alınmaması veya alınan tedbirlerin yanlış kullanılması sonucu oluşan olumsuz sonuçlar bilgi güvenliğinin geçerliliğinin kaybedilmesine neden olmaktadır (Siponen, 2000). Maslow tarafından oluşturulan ihtiyaçlar hiyerarşisinde güvenlik gereksinimleri önemli bir yere sahip olsada, bilgi güvenliği söz konusu olduğunda birçok kurum bu sıralamaya uymamaktadır. Bilgi güvenliği tehditlerinin gerçekleşmesi sonrasında oluşabilecek bilgilerin çalınması, hırsızlık, bilginin tahribata uğraması gibi olumsuz sonuçları öngöremeyebilirler (Siponen, 2000).

2.1. Bilgi Güvenliğini Oluşturan Unsurlar

Gizlilik (confidentiality), bütünlük (integrity), kullanılabilirlik (availability), bilgi güvenliğinin en temel unsurlarıdır. Bu temel unsurlara ek olarak bilgi güvenliğinin sağlanması için alt unsurlarında bulunması gerekmektedir. Kimlik kanıtlama (authentication), inkâr edememe (non-repudiation), kayıt tutma, güvenilirlik (reliability) ve yetkilendirme (autharization) etkenleri de bilgi güvenliğini destekleyen unsurlardır. Bu unsurların tamamının gerçekleştirilmesiyle ancak bilgi güvenliği tam

olarak sağlanabilecektir. Bu unsurların bir veya birkaçının eksikliği, bilgi güvenliğinde aksamalara sebebiyet verebilecektir

2.1.1. Temel Unsurlar

Bilgi Güvenliğinin sağlanabilmesi için kurum içerisinde gizlilik(confidentialy), bütünlük (integrity) ve erişilebilirlik (Availability)) gibi temel unsurların gerçekleştirilmesi gerekmektedir. İngilizce terimleri ile birlikte telaffuz edildiğinde CIA üçlüsü olarak ta litaratürde yer almaktadır.

Bu üç temel unsura ek olarak bilgi güvenliğinin sağlanması ve devam ettirilmesi için yetkilendirme, kayıt tutma, süreklilik, güvenilirlik, inkar edememe ve kimlik doğrulaması gibi alt unsurlarında mutlaka bulunması gerekmektedir.

2.1.1.1. Gizlilik

Yetkisiz kişilerin bilgiye ulaşmasının engellenmesi amaçlanmaktadır. Bilgi saklanırken, işlenirken veya transfer edilirken yetkisiz kişilerin erişimlerine izin verilmemelidir. Kötü niyetli kişiler, siber casusluk, şirkete zarar verme gibi birçok amaçla bilgiye erişim sağlamayı hedeflemektedirler. Bu nedenle, bilginin gizliliğini sağlamak kurumun güvenliği açısından elzemdir. McCumber modelinde bilgi gizliliğinin sağlanması amacıyla, bilginin transferi ve depolanması süreçlerinde kripto kullanımı önerilmektedir (McCumber, 2005). Gizlik ilkesinin sağlanması için bilgi varlıklarının şifreli bir şekilde sistemlerde tutulması ve yetkisiz erişimlere karşı güvenlik politikalarınca mümkündür.

2.1.1.2. Bütünlük

Bilginin yetkisiz kişiler tarafından değiştirilmesinin, tahribata uğratılmasının ve bozulmasının engellenmesi demektir. Bilgi varlığının bütünlüğü transferi, işlenmesi veya saklandığı yer içerisinde saldırganlar tarafından bozulabilir. Özellikle, günümüzde yazılan birçok virüs ve solucan adı verilen zararlı yazılımlar bilginin tahribatını hedeflemektedir. Bu nedenle, bilgi varlığının bütünlüğü sağlamak için gerekli güvenlik önlemlerinin alınması gerekmektedir. Bilgi varlığının bütünlüğün sağlanması için en önemli metot dosya özet değerinin hesaplanması (file hashing) metotudur. MD5,SHA256,SHA1 benzeri bilgisayar algoritmaları kullanılarak dosya'nın özet değeri çıkartılır. Dosya içerisinde en ufak bir değişiklik yapıldığı takdirde özet değeri de değişmektedir. Özet değerinin değişmesi durumlarında dosya'nın yani bilginin bütünlüğü bozulmuştur diyebiliriz. Dosya özet değerinin

hesaplanması yöntemi bütünlüğün sağlanması için kullanılan en yaygın yöntemdir. Aynı dosyaların aynı algoritma kullanılarak hesaplanan özet değerleri farklı ise, kesinlikle dosya değiştirilmiştir, bu durumda bilgi varlığı bütünlüğünü kaybetmiştir (Whitman and Mattord, 2011).

2.1.1.3. Erişilebilirlik

Yetkili kişilerin veya sistemlerin zamanında herhangi bir engel ile karşılaşmadan bilgiye erişiminin sağlanmasıdır. Saldırganlar tarafından kullanılan servis dışı bırakma saldırısı gibi saldırılar bilgiye erişimin yetkili kişiler tarafından engellenmesini sağlamaktadır. Bu ve buna benzer saldırılar neticesinde kurumlar veri kaybı, finansal zararlar, temel hizmetlerinin aksamasından dolayı itibar kayıpları gibi problemler ile karşılaşmaktadır. Bu nedenle bilgiye erişebilirliğin sağlanması bilgi güvenliğinin en önemli unsurlarındandır.

2.1.2. Alt Unsurlar

Bilgi güvenliğinin sağlanabilmesi için gizlilik, bütünlük ve erişebilirlik maddelerine ek olarak birçok alt unsurunda var olması gerekmektedir. Bu alt unsurlar kayıt tutma, güvenilirlik, inkar edememe, kimlik doğrulaması ve yetkilendirme olacak şekilde sıralanabilir.

2.1.2.1. Kayıt Tutma

Bilgi sistemlerinde gerçekleşen olaylara ilişkin kayıtlar sistemlerin kendi üzerinde veya merkezi olarak tutulmalıdır. Bu kayıtlar, sistemlere erişen kişilerin yaptıkları tüm işlemlere ait bilgileri, erişim yaptıkları zaman bilgisi, nereden ve nasıl sistemlere bağlandıkları gibi bilgileri içermektedir. Özellikle, siber olaylara müdahale ekipleri bu kayıtlar üzerinde inceleme yaparak saldırgana ait izleri tespit etmektedir. Bilgi güvenliği açısından kayıt tutma özelliği önemli bir yer tutmaktadır. Saldırı tespit, saldırı inceleme, mevzuatlara uyumluluk gibi nedenlerden dolayı kurumlar kayıt tutma yazılımlarına yatırım yapmaktadır.

Kayıt tutmak, **5651 sayılı kanun** gereğince ve ayrıca TİB (**Telekomünikasyon İletişim Başkanlığı**) yönetmelikleri gereği her kurum, erişim kayıtlarını tutmakla ve bu kayıtları en az 2 sene saklamakla yükümlüdür.

5651 sayılı Yasanın çıkarılmasının iki amacı bulunmaktadır. Birincisi; İnternet'in önemli aktörlerinden olan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumluluklarını belirlemektir. Diğer amaç ise;

İnternet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemektir.

2.1.2.2. Güvenilirlik

Kurumların bilgi sistemlerinde yer alan cihazların ve bilginin transferi için kullanılan sistemlerin tasarımlarına ve kurumun hazırlamış olduğu şartnamenin maddelerine bağlı kalarak çalışması yeteneğidir.

Tasarım gereksinimlerine bağlı kalarak bekleyen işi her defasında eksiği fazlası olmadan tutarlı bir şekilde yerine getirmesidir. Güvenilirlik esasına bağlı kalınması bilgi güvenliğinin unsurlarının önemli bir parçasıdır.

2.1.2.3. İnkar Edememe

Bir bilginin transferi aşamasında ortaya çıkabilecek problemleri ele alarak oluşabilecek problemleri en aza indirilmesi amaçlanmıştır. Bilgi sistemleri arasında bir bilgi aktarımı yapılmışsa ne gönderen veriyi gönderdiğini, nede alıcı veriyi aldığını inkar edememelidir. Özellikle, finans sektöründe yer alan kurumlar gibi gerçek zamanlı işlemler gerçekleştiren kurumlar için hayati önem taşımaktadır.

2.1.2.4. Kimlik Kanıtlama

Kullanıcıların işlemlerinin tanınması, doğrulanması ve bir kullanıcının hangi sistem kaynaklarına erişim hakkının olduğunun belirlenmesidr. Bilgi güvenliğinin en önemli unsurlarından biridir. Kimlik yönetimi yapılarak yetkilerin kullanıcı bazlı yapılması, sadece kişinin işi ile alakalı kaynaklara erişim hakları tanınması bir kurumun ilk yapması gereken adımlardan biridir. Kimlik kanıtlama süreci, erişim sağlamaya çalışan kullanıcının böyle bir hakkı olup olmadığının sorgulanması ile başlamaktadır. Daha sonra kullanıcıya tanımlanan parola, pin veya biometrik (kişide bulunan bir şey) ile doğrulama yapılması talep edilir, sistem üzerinde ki kayıt ile eşleşmesi durumunda sisteme giriş hakkı verilir.

2.1.2.5. Yetkilendirme

Kullanıcı adı ve parola doğrulaması sağlanan kullanıcıların sisteme, programa veya ağa hangi yetkilerle erişim hakkına sahip olduklarını belirten sistemdir. Sisteme kayıtlı olan kullanıcılar gruplanarak, bu gruplara çeşitli yetkiler verilir. Kullanıcı içerisinde bulunduğu grubun bütün yetkilerine sahiptir. Eğer bir kullanıcı birden fazla gruba üye

ise bu gruplara verilen yetkilerin hepsine sahiptir. Güvenliğin tam olarak sağlanabilmesi için kullanıcılara gerekenden fazla yetki verilmemelidir.

Kimlik yönetimi bilgi güvenliğinin sürekliliği açısından büyük öneme sahiptir. Kullanıcının iş değişikliği veya işten ayrılması gibi durumlarda sahip olduğu tüm haklar geri alınarak kimlik yönetim süreci işletilmelidir. Özellikle, kurumlar kimlik yönetimini işten ayrılma süreçlerine dahil ederek otomatik olarak kullanıcıları sistemde kaldırsalarda, departman değişikliklerinde bu süreci işletmekte zorluk yaşamaktadırlar. Kullanıcılar bir önceki departmanda elde ettikleri haklara sahip olmaya devam etmektedirler. Bu durum, bilgi güvenliği açısından zafiyet oluşturmaktadır. Bu nedenle, kimlik kanıtlama unsuru konusunda bir süreç tasarlanarak kurumlar tarafından özenle işletilmelidir.

3. BİLGİ GÜVENLİĞİ TEHDİTLERİ VE İHLAL OLAYLARI

Bilgi sistemleri, önemli maddi kayıplara yol açabilecek farklı türden zararlara neden olabilecek çeşitli tehdit türlerine maruz kalmaktadır. Bu zararların etkileri, küçük kayıplardan tüm bilgi sisteminin imhasına kadar değişebilir. Bazıları verilerin gizliliğini veya bütünlüğünü etkiler, bazıları ise sistemin kullanılabilirliğini etkiler.
Kuruluşlar bilgi varlıklarına yönelik tehditlerin ne olduğunu tespit ederek, bu tehditlerin tamamen önlenmesi veya etkilerinin en aza indirgenmesi için çalışmalar yapmaktadır.
Önleme çalışmalarının yapılabilmesi için ilk olarak tehditleri sınıflandırmak gerekmektedir. Çünkü, tehditler birçok kaynaktan gelebilir ve etkileri çok farklı olabilir. Bir tehdit iç kaynaklı, dış kaynaklı veya hem iç ve dış kaynaklı olabilir, tehdit sınıflandırması tehditin nereden başladığını analiz edilerek yapılır. Her iki tehdit sınıfında ortak üç tehdit etkeni vardır. Bunlar, insan faktörü, çevresel etkenler ve teknolojik etkenlerdir. (Jouni, 2016)

3.1.Tehdit Çeşitleri

Bilgi Güvenliği tehditleri iç kaynaklı veya dış kaynakları olarak sınıflandırılır.

3.1.1. İç Kaynaklı Tehditler

İç kaynaklı tehditler bir bilgi sistemine erişim yetkisi olan yetkili bir kullanıcının bir hata sonucu veya sahip olduğu yetkiyi kötüye kullanarak sistem içerisinde zafiyet

oluşturmasıdır. Günümüzde, kurumlar iç kaynaklı tehditlerden dolayı ciddi bilgi güvenliği vakaları ile karşılaşmaktadır. Örneğin, Kişisel Verileri Koruma Kurulunca yapılan açıklamada Türkiyede faaliyet gösteren Türkiye İş Bankasının bir çalışanının görevini kötüye kullanması nedeniyle müşterilere ait kişisel verilerin sızdırıldığını duyurmuştur. Bu nedenle, finsanal, itibari kayıplar yaşamamak için iç kaynaklı olası tehditlere karşı koruyucu önlemler alınmalıdır.

3.1.2. Dış Kaynaklı Tehditler

Dış kaynaklı tehditler kurum lokasyonu içerisinde bulunmayan kötü niyetli kişiler, organizasyonlar veya kurum bilgi sistemlerine zarar verebilecek doğa olayları olarak gösterilebilir. Örneğin, Vodafone Türkiye, veri merkezinin bulunduğu İstanbul İkitelli bölgesinde yaşanan sel felaketinden dolayı ciddi zarar yaşamıştır. Dış kaynaklı tehditlerin en başında gelen siber saldırılarda tüm kurumların dikkat etmesi gereken en önemli tehditlerdendir.

3.2. Tehdit Etkenleri

Hem iç kaynaklı hemde dış kaynaklı tüm tehditlerde insan, çevresel ve teknolojik etkenler rol oynamaktadır.

3.2.1. İnsan Etkeni

İnsan kaynaklı etkenler nedeniyle oluşabilecek tehditler iki grupta incelenebilir. Kullanıcıların istem dışı yaptıkları hatalar sonucu oluşan olumsuz sonuçlar; .Bir kullanıcının sistemi bilmeden kullanması, nitelik eksikliği yüzünden olumsuz sonuçların ortaya çıkması sonucu oluşan aksaklıklar. Kötü niyete sahip olan kullanıcılar veya kişiler tarafından oluşan olumsuz sonuçlar; kuruluşun sistemine zarar vermek amacıyla yürütülen faaliyetler kaynaklı tehditlerdir. Kötü niyeti bu kişiler sistemde yer alan bilgi güvenliği zafiyetini sömürmektedir (Shephard, 2002).

3.2.2. Çevresel Etkenler

Bu tür tehditlerin önceden tespit edilmesi zordur. Çevresel etkenlere deprem, yangın, sel gibi doğal afetler örnek olarak verilebilir. Çevresel etkenler kaynaklı tehditlerin etkilerinin en aza indirilmesi için kurumlar bir takım önlemler almalıdır. Felaket planları yapılmalı, sistemler farklı lokasyonlarda yedekli bir şekilde konumlandırılmalıdır. Bilgi varlıklarının saklanacağı yerlerin jeopolitik konumları

dikkate alınarak, doğal afetlerin yaşanma olasılığının düşük olduğu yerlerde bulundurmalıdır.

3.2.3. Teknolojik Etkenler

Günümüzde, kurumlar iş süreçlerini devam ettirebilmeleri için teknolojik araçların gereçlerin ve yazılımların kullanımlarına bağımlı hale gelmişlerdir. Bu yazılımların bilgi sistemlerinde çalışmasıyla birlikte çeşitli tehditler ortaya çıkmaktadır. Bilgi sistemleri kötü niyetli kişiler tarafından tahrip edilebilir, değiştirilebilir, silinebilir veya değişikliğe maruz kalabilir. Genellikle saldırganların motivasyonları uzun süre sistemlerde varlıklarını devam ettirmektir, bu nedenle sistem üzerinde farkedilmeden uzun süre zararlı aktivitelerini sürdürmektedirler. Bir yazılımı yapması gereken tüm işlemleri yapacak ve aynı zamanda saldırganın amaçlamış olduğu kötü niyetli faaliyetleri de yapacak şekilde ayarlamak mümkündür(Shephard, 2002). Bu şekilde çalışan yazılımlara örnek verecek olursak truva atı(trojan horse) programı, görünürde olağan işleri yaparken gizlice zararlı faaliyetlerde yapılmasına olanak veren programlardır. Özellikle, Ağ içerisinde bulunan bilgisayarlar arasında hızlıca yayılarak etkilerini geniş alanda hissettirirler.

3.3. Bilgi Güvenliği İhlal Olayları, Tespiti Ve Yönetimi

3.3.1. Bilgi Güvenliği İhlal Olayı

Kurumun iş süreçlerinin ve bilgilerinin gizliliğini, bütünlüğünü ve erişebilirliğini herhangi bir biçimde tehdit eden veya tehdit potansiyeline sahip olaylardır.

Sağlık Bakanlığının hazırlamış olduğu örnek bilgi güvenliği ihlal olayları prosedürüne göre aşağıdaki hususlardan kaynaklanabilecek ihlaller bilgi güvenliği ihlali olayı olarak tanımlanmıştır.

- Kuruluş için önemli olan bilgilerin çalınması
- Bilgi güvenliği'nin 3 unsurunu etkileyen ihlaller
- İnsan hataları sonucu oluşabilecek ihlaller
- Yetkili makamlarca yayımlanmış olan bilgi güvenliği politikalara ve prosedürlere göre iş süreçlerinin uygulanmaması
- Fiziksel güvenliğin ihlali
- Kontrol dışı yapılan kayıtsız sistem üzerinde ki değişiklikler
- Yazılımsal ve donanımsal arızalar

- Yetkisiz erişim, yetkisiz bilgi varlıklarının erişimine izin veren uygulamalar
- Siber saldırılar
- Gizli bilginin yetkisiz kişilerce ifşa edilmesi

3.3.2. Bilgi Güvenliği Olay Türleri

Saldırganlar kurumların bilgi güvenliğini tehdit edecek birçok yöntem kullanmaktadır. Bu yöntemler casusluk, kurumun faaliyetlerinin durdurulması, kamuoyunda kuruma olan güvenin azalması ve maddi çıkar elde etmek amacıyla yapılmaktadır.

3.3.2.1. Servis Dışı Bırakma (DDOS)

Kuruma ait olan sistemlere kapasitelerinden fazla birçok çok cihazdan istek yapılarak sistemin durdurulmasını hedeflemektedir. Kurum sistemi kendisine gelen aşırı yüke cevap veremeyerek faaliyetlerini yerine getiremeyecek şekilde zarar görmektedir. 2015 senesinde Polonya menşei havayolu firmasına yapılan servis dışı bırakma saldırısında 10 uçuş iptal olmuş, 12 uçuş ise ertelenmiştir. Yaklaşık 1400 yolcunun bu saldırıdan etkilendiği duyurulmuştur.(Schwartz, 2015)

3.3.2.2. Bilgi Sızdırma (Data Leakage)

Kuruluş tarafından ürettiği, işlediği, kullandığı gizli veya hizmete özel olarak sınıflandırılmış bilgilerin bir şekilde kurum dışına çıkarılması olayıdır. Kuruluşlar bilgi sızdırılması vakası sonucu ciddi yaptırımlar ile karşılabilir.

3.3.2.3. Zararlı Yazılım (Malware)

Kuruluşun bilgi sistemlerine zarar vermek, kuruluş hassas bilgilerini çalmak veya kullanıcıları huzursuz etmek gibi amaçlarla yazılmış zararlı yazılımlara verilen isimlerdir. Zararlı yazılımlar sayesinde saldırganlar uzaktan kurum sistemlerinde işlem yürütmekte, kurum sistemlerinin durdurulması dahil birçok eylem gerçekleştirilebilir.

3.3.2.4. Dolandırıcılık (Fraud)

Kişileri kandırma amacı ile yapılan faaliyetlerdir. Doğrudan kurum sistemleri bu saldırı türünde hedef alınmaz. İnsan unsurunun manipüle edilmesi amaçlanmaktadır.

3.3.2.5. Port Tarama

Kurum sistemlerinin üzerinde çalışan servislerin hizmet verdiği mantıksal bağlantı noktalarını ve durumlarını tespit etmek için yapılan işlemdir. Saldırganların kurum

sistemlerini öncelikle bu saldırı türü ile keşfederek bilgi toplamaktadır. Sonrasında çalışan servisin türüne göre saldırılar gerçekleştirmektedir.

3.3.2.6. Veri Tabanı Saldırısı

Veri tabanı uygulamalarında oluşabilecek sistemsel zafiyetlerinden veya bilinçsiz kullanımından kaynaklı veri tabanının saldırganlar tarafından ele geçirilmesi, yönetilmesi ya da yetki yükseltilmesi şeklinde gerçekleşen saldırılardır.

3.3.2.7. Web Uygulamaları

Kurum sistemleri içerisinde müşterilere hizmet veren web sitesi dahil, müşterilerin erişimine açık olan tüm sistemlere yönelik yapılan saldırılardır. Web uygulamalarının maruz kaldığı saldırılar neticesinde kurumlar büyük zarar görmektedir. Web uygulamarının güvenliğine yönelik araştırmalar gerçekleştiren uluslararası bir organizasyon olan OWASP her sene yapılan en çok 10 web saldırı metodunu açıklayarak, kurumları bilgilendirmektedir. 2018 senesinde açıklanan OWASP TOP 10 listesi şu şekildedir.

- SQL Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- Cross Site Scripting
- Insecure Deserialization
- Using Component With Known Vulnerabilities
- Insufficient Loging and Monitoring

3.3.2.8. Sosyal Mühendislik

Bu saldırı türünde kurum sistemleri doğrudan hedef alınmamaktadır. İnsan unsurunun zafiyetlerinden faydalanarak çeşitli ikna ve kandırma yöntemleriyle istenilen bilgileri elde etmeye çalışmaktır. İnsanların karar verme süreçlerini değiştirmeye yönelik teknikler içermektedir.

3.3.2.9. Veri kaybı / ifşası

Kuruluş tarafından hassas veriler olarak sınıflandırılmış bilgilerin e-posta ve ağ üzerinden iletilmesi sonucu bilgilerin yetkisiz kişilerin veya yanlış kişilerin eline geçmesi veri kaybına örnek olarak verilebilir. Ayrıca, kuruluşların göz ardı ettiği diğer konu ise ortak yazıcıların yeteri kadar korunmaması, güvenliğine önem verilmemesi ve ortak alanlarda sahipsiz bir şekilde bırakılan dökümanların korunmamasıdır. Bu gibi durumlar sonucu veri kaybı bilgi güvenliği olaylarına sıklıkla rastlanılmaktadır.

Bu nedenle, kurum çalışanları verilerin güvenliğini ve bütünlüğünü korumanın önemini göz önünde bulundurarak bilinçli hareket etmeli, ihlal durumlarını rapor etmesi gerekmektedir.

3.3.2.10. Zararlı Elektronik Posta (Spam)

Talebiniz dışında size gönderilen ticari içerikli, siyasi bir görüşün desteklendiği ya da bir konu hakkında kamuoyu oluşturmak amacı ile gönderilen e-posta iletileridir. Genellikle kurum sistemlerini dolaylı hedef almamaktadır. İnsan unsuru üzerinden amaçlarını yerine getirilmesini hedeflemektedir.

3.3.2.11. Parola ele geçirme

Kişilerin parolalarının depolandığı bir yerden parolaları sızması veya çalınması durumudur. Siber saldırı yöntemi ile parolaların yetkisiz kişilerce ele geçirilmesidir. Kurum çalışanlarının açık bir şekilde parolarınını saklaması veya diğer kurum çalışanlarına parola bilgilerini rızası ile teslim etmesi bu saldırıların kök sebebi olmaktadır.

3.3.2.12.Taşınır Cihaz Kaybı

Kullanıcılar tarafından veri depolamak için kullanılan USB, CD, DVD veya harici/dahili diskler gibi cihazların kullanma sorumluluklarının tamamen farkında olunmamasından dolayı gerçekleşen ihlal olayını ifade etmektedir.

Dizüstü bilgisayarların, tabletlerin ve diğer taşınabilir aygıtların şifresiz bir şekilde erişilebilir olarak kullanılması, verilerin herkesin erişime açık hale gelmesine neden olabilir. Herhangi bir taşınabilir aygıtın yetkili kullanıcısı dışında kullanımı, kaybı veya bulunması durumunda. kuruma ait bilgiler sızabilir. Bu nedenle kurumlar cihaz yönetimini geliştirmeli, kuruma ait olan taşınabilir cihazlar içerisinde ki bilgilere erişimi şifreli hale getirmelidir.

3.3.2.13. Kimlik taklidi

Kullanıcıların fiziksel, dijital ortamda olmadığı bir kişi gibi davranıp, onun yetkilerini bilgisi dışında kullanmasıdır. Çalışan kurum kimliğini herhangi bir şekilde çaldırması veya kaybetmesi durumunda ilgili birimlere haber vererek bildirimde bulunmalıdır.

3.3.2.14. Oltalama

Oltalama saldırı türünde kurum sistemleri direk hedef alınmamaktadır. Kurum sistemlerine insan unsurunun zafiyeti sömürülerek erişilmesi hedeflenmektedir. Güvenlik yazılımları sürekli geliştirilerek saldırganların metotlarının uygulanmasını engellemektedir. Bu nedenle, saldırganlar yazılımların zafiyetlerini tespit etmeye çabalamak yerine çok daha az efor sarfederek insan unsuru üzerinden zararlı akvitelerini gerçekleştirmeyi amaçlamaktadır. Yani, saldırganların kurum çalışanının e-posta hesaplarına çalışanın ilgisi yönünde e-postalar göndererek çalışanın manipüle edilmesidir.

Genellikle oltalama saldırıları iki şekilde yapılmaktadır. E-posta içerisinde çalışanın yönlendirildiği bir link yer almaktadır. Çalışan bu linke tıklayarak kendisinden istenen bilgileri saldırganın yönlendirdiği sisteme girmektedir. Diğer bir yöntem ise e-posta eki olarak zararlı yazılım kurum çalışanının e-posta hesabına gönderilmektedir. Kurum çalışanın ek'te yer alan dosyayı bilgisayarına indirerek çalıştırmaktadır. Saldırgan bu sayede çalışanın bilgisayarına erişim sağlamakta kontrolu ele almaktadır.

Oltalama saldırı türünün kullanımının ciddi şekilde arttığı söylenilebilir. Güvenlik yazılımları üreten ve araştırmaları gerçekleştiren Trend Micro firmasına ait bir rapora göre 2019 senesinin ilk yarısında 2.4 milyon saldırı engellenmiş, ve bu sayı 2018 senesinin ikinçi yarısında yapılan oltalama saldırılarından %59 daha fazla olduğunu belirtmişlerdir.

3.3.3. Bilgi Güvenliği İhlal Olaylarının Tespiti ve Önlenmesi

Bilgi güvenliği olaylarının tespit edilerek düzeltici ve önleyici aksiyonların alınması kurumlar açısından büyün önem arz etmektedir. Kurumlar sistemlerinde bilgi güvenliği olaylarının tespitine yönelik yazılımlar edinilmeli, güvenlik cihazlarına yatırım yapılmalı, bu konuda bilgili yetişmiş insanlar istihdam etmelidir.

3.3.3.1. Merkezi Güvenlik Kayıt ve Olay Yönetimi Yazılımları

Merkezi güvenlik kayıt ve olay yönetimi yazılımları sayesinde kurum ortamındaki cihaz ve sunuculardan güvenlik loglarını (dijital kayıtlarını) merkezi olarak toplamakta ve bu logları anlamlandırarak güvenlik tehditlerinin/olaylarının tespit edilmesine olanak sağlamaktadır. Aynı zamanda toplanan bu kayıtlar sistemlerin yönetiminde ve araştırma/soruşturma işlemlerinde de kullanılmaktadır. Bu özelliklerin yanı sıra, mevzuatlara uyumluluk anlamında da kurumlara fayda sağlamaktadır.

3.3.3.2. Ağ Tabanlı Saldırı Tespit Sistemleri

Saldırganlara ait yazılımlar, betik dilleri kurumlara ait sistemler tarafından tespit edilerek engellenmektedir. Saldırı Tespit Sistemleri, ağlara veya sistemlere karşı yapılan kötü niyetli aktiviteleri ya da politika ihlallerini izlemeye yarayan cihaz ya da yazılımlardır. Bu cihazlar sayesinde kurumlar saldırıları tespit ederek saldırganların kötücül aktivitelerine başlamadan engellemektedir.

3.3.3.3. Son Kullanıcı Cihazları Tabanlı Saldırı Tespit Sistemleri

Saldırganlar sıklıkla kurum çalışanlarını hedef almaktadır. Kurum çalışanının manipüle edilmesinden sonra kurumlara ait sistemler üzerinde kötücül aktivitelerini yerine getirmektedir. Kurum çalışanlarına yönelik yapılan saldırıların artmasından sonra bu tip saldırı tespit sistemleri önem kazanmıştır. Kullanıcı cihazlarına bulunan Antivirus ve Endpoint Detection Response(EDR) gibi çözümler zararlı yazılımları tespit ederek akvitelerini engellemektedir.

3.3.3.4. Yetişmiş Bilgi Güvenliği Personeli

İhlal olaylarını tespit edebilecek, saldırgan bakış açısıyla kurum sistemlerini izleyecek gerektiğinde ihlal olaylarına müdahale edebilecek yetişmiş bilgi güvenliği personellerine kurumlar ihtiyaç duymaktadır.

3.3.3.5. Bilgi Güvenliği Farkındalığı

Kurum çalışanlarının bilgi güvenliği farkındalıklarının yüksek olması ihlal olaylarının tespitinin artmasına, ihlal olaylarının gerçekleşme sayısının azalmasına büyük katkı sağlamaktadır. Bu nedenle, bilgi güvenliği tehditlerinden korunmanın en iyi yolu tespit sistemlerine yapılacak yatırımlardan önce çalışanların bilinçlenmesi ve bilgi güvenliği'nin sadece ilgili bölümde çalışan kişilerin değil tüm çalışanların sorumluluğu olduğunun farkında olunmasıdır.

2007 yılındaki kurum içinde bilinçli ya da bilinçsiz bir şekilde yapılan güvenlik istismarları %59' den 2008 yılında bu durum bilgi güvenliği farkındalık çalışmaları ile %44'de kadar düşürülebildiği gözlemlenmektedir. Yine etkin bilgi güvenlik olaylarına ait yüzdelik dilimler incelendiğinde en büyük tehdit unsurunu iç tehditler olduğu görülmektedir. Bu durumda insan faktörünün kurum için önemini açık bir şekilde göstermektedir. (2008 CSI Computer Crime & Security Survey)

3.4. Bilgi Güvenliği İhlal Olayları Yönetimi

Bilgi güvenliği ihlal olaylarının gerçekleşmesi ile birlikte kurumlar ihlal olaylarını incelemeli, kök sebebini araştırmalı, düzeltici faaliyetleri tespit ederek aksiyon almalıdır. Bilgi güvenliği ihlal olaylarının tespiti, incelenmesi için tüm adımları dökümante ederek süreç oturtmalıdır. Sağlık Bakanlığı bilgi güvenliği ihlal olaylarının yönetimi için gereksinimleri aşağıdaki şekilde belirlemiştir.

- Bilgi güvenliği unsurlarının herhangi bir şekilde zarar görmesi, bilginin iletilmesi esnasında bozulması, yetkisiz kişilerce değişikliğe uğraması, başkaları tarafından ele geçirilmesi veya tahribata uğraması durumunda mutlaka kayıt altına alınmalıdır.
- Bilgi güvenliği olaylarının kayıt altına alınmasını, ilgili kişilere bildirilmesini, sonuçlarına göre işlem yapılmasını ve işlemin sonlandırılmasını sağlayan uygun bir iş süreci oluşturulmalıdır.
- Bilgi güvenliği ihlâl olayının oluşması durumunda kullanıcıların yapılması gereken faaliyetleri hatırlamasını sağlamak ve hızlı müdahale etmek amacıyla bilgi güvenliği olayı rapor formatı hazırlanmalıdır.
- Bilgi güvenliği ihlal olayının oluşması durumunda raporlanmalıdır.
- Eğer, bilgi güvenliği ihlal olayı iç kaynaklı ise kullanıcı tespit edilmeli ve ihlalin suç unsuru içerip içermediği belirlenmelidir.
- Bilgi güvenliği ihlaline neden olan kullanıcılar ve üçüncü taraflarla ilgili resmi bir disiplin sürecine başvurulur.
- Kuruluşlar bilgi sistemlerinde olası arızalara ve hizmet kayıplarına, zararlı uygulamaların çalıştırılmasına, servis dışı bırakma saldırılarılarına, bilgi akışı kaynaklı

hatalara, bilgi güvenliği unsurlarını tehdit eden tüm ihlal olaylarını azaltacak önlem ve tedbirler almalıdır.

- Bilgi sistemlerinde ki olay kayıtlarının izlenmesi, gerektiğinde adli analizler yapılabilmesi için izleme kayıtları(log) merkezi olarak toplanır ve yetkisiz erişimlere karşı koruma altına alınır.
- Bilgi güvenliği ihlal olaylarının olası olumsuz sonuçlarını en aza indirmek için gereken faaliyetler, bilgi sistemleri üzerinde oluşabilecek hataların düzeltilmesi hususları dikkate alınır.
- Bilgi güvenliği ihlal olaylarının detaylı olarak değerlendirilmesi sonucunda edinilen bilgi ile edinilen tecrübe ve yeni kontrollerin oluşturulması, aynı olayın tekrar etmesini önleyecek veya yüksek etkili olayların oluşmasını engelleyecektir.
- Kuruluş gerektiği durumda disiplin faaliyetleri yürütebilmek için uygun delil toplama kurallarını işletmelidir. Delil toplanırken uygulanacak kuralar aşağıdaki gibidir;
    - Mahkemede kullanılıp kullanılamayacağı'nın tespit edilmesi
    - Kanıtın niteliği ve tamlığını gösteren hususlar

Kuruluş tarafından hazırlanan bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması durumunda, yönetmelikler gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- Uyarma,
- Kınama
- Para cezası
- Sözleşme feshi.

Bilgi güvenliği ihlal yönetimi gereksinimlerinden olan bildirim formunu aşağıdaki şekilde hazırlanabilir.

İhlal Bildirimi Yapacak Kişinin		Olay Derecesi
Adı *		☐ Düşük ☐ Orta ☐ Yüksek ☐ Kritik
Soyadı *		
Telefon *		
e-posta *		
Departman *		
Tarih *		

Olay Tanımı

Yetkisiz Giriş ☐
Yazılım Arızası ☐
Virüs / Solucan / Trojan ☐
Web Sitesinin Hack Edilmesi ☐
Tehdit / E-Posta Bombardımanı ☐
Copyright Usülsüzlüğü ☐
Fraud / Spam ☐
Müstehcen veya Çirkin Mesaj Gelmesi ☐
Tehdit / E-Posta Bombardımanı ☐
Güvenlik Açıklarından Faydalanma ☐
Diğer ☐

Olay Açıklaması

Tablo 1. İhlal Bildirim formu

4. HAVACILIK SİSTEMLERİNE GENEL BAKIŞ

4.1. Bilişim Sistemlerinin Önemi

Hava taşımacılığı şehirler arası ve ülkeler arası toplu taşıma seçenekleri arasında en popüler taşımacılık yöntemidir. Can güvenliği, zaman ve konfor açısından insana kazandırdıkları şeyler nedeniyle sıklıkla tercih edilmektedir. Havalimanlarına milyonlarca kişinin gelmesi ve güvenli bir şekilde ayrılması, sivil havacılık firmalarının milyonlarca yolcuyu zamanında uçurabilmesi, bu yolcularının bagajlarının aksamadan uçaklara yüklenmesi gibi birçok iş süreci bilişim sistemleri vasıtasıyla yapılmaktadır. Bu nedenle havacılık sektöründe bilişim sistemlerinin önemi büyüktür. Herhangi bir sistem arızası uçuşların aksamasına, firmaların milyonlarca dolar zarar etmesine neden olabilir. Havayolları firmaları arasında ki

rekabetle birlikte, birçok havayolu firması maliyetlerini düşürmek müşteriler ile direk iletişim kurabilmek için bilişim sistemleri çözümleri geliştirdi. (Yoon et al., 2006) 2004 senesinde IATA havayolu firmalarının maliyetlerini azaltmak ve yolcu memnuniyetini arttırmak için "Simplifying The Business " adını verdiği bir program başlattı. Bu programın temel amacı havayolu endüstrisinin çalışma şeklini değiştirmek, yolcular için üst seviyede konfor sağlamak ve firmalar için düşük maliyetler sunmaktır. (Oktal, 2009) Bu program sayesinde her sene 14 milyar$ tassaruf edilmektedir. 60 sene önce bir grup havayolu firması tarafından kurulan küresel bir örgüt olan IATA bünyesinde şu an 230 havayolu firması bulunmaktadır. İcra edilen havayolu trafiğinin %93 lük kısma IATA tarafından yürütülmektedir. (IATA, 2009)

4.2. Sivil Havacılık Firmaları Tarafından Kullanılan Sistemler

Havayolu firmaları artan yakıt maliyetleri, güvenlik regülasyonları, ekoloji konusunda yükselene endişeler gibi birçok problemler ile mücadele etmektedir. Bu nedenle, havayolu firmaları değişken maliyetleri kontrol etme yeteneği havayolu şirketinin başarılı olup olmadığını belirlemektedir. Bu maliyetler şu şekilde sıralanabilir; yakıt maliyetleri, yemek hizmeti, personelin ücretleri yer hizmetleri gibi. (Sage, 2006)

Havayolu firmaları bu problemler ile başa çıkabilmek için bilişim sistemleri oluşturmakta ve yatırım yapmaktadır.

4.2.1. Havalimanı Operasyon Sistemleri

Havalimanı operasyonlarında kullanılan sistemlerin temel amacı yolcular ile alakalı uçuş bilgilerini, yolcuya ait bilgilerin havayolu firma ve havalimanı sistemleri arasındaki entegrasyonu sağlamaktır.

4.2.2. Uçuş Operasyon Sistemleri

Uçak bakımının analiz edilmesi, rotanın hesaplanarak planlanması, uçak içerisinde ki görevli personelin yönetimi ile alakalı süreçlerin işletimesinde kullanılan bilgi sistemleridir. Uçak operasyonlarında kullanılan sistemlerin temel amacı mürettabat ve uçuç planınını üst düzeye çıkarmak uçuş güvenliğinden ödün vermeden maliyetleri azaltmaktır.

4.2.3. Bagaj Operasyonları

Bagaj operasyonları, yolculara ait bagajların ilgili uçaklara hızlı ve doğru bir şekilde ulaştırılmasını sağlayan ve takibinin yapılmasını sağlayan bilgi sistemleridir.

4.2.4. Yolcu Operasyon Sistemleri

Havayolu firmalarının yolcunun uçağa yönlendirmesi, check-in ve boarding işlemlerinin doğru bir şekilde yapılmasını sağlayan sistemlerdir.

4.2.5. Ticari Sistemler

Havayolu firmalarının ticari faaliyetlerini yürüttüğü, yolcuya ulaştığı ve satış işlemleri dahil birçok işlemlerin gerçekleştiği sistemlerdir. Ticari Sistemlerinin kullanılmasının temel amacı yolcuların memnunuiyetini üst seviyede tutarak sadakatini edinmek, işin devamlılığını sağlayarak yüksek kar elde edebilmek müşteri memnunuiyetini artırmak ve yolcuların satın alma işlemlerini basitleştirmek olarak değerlendirilebilir.

4.2.6. Kargo Operasyon Sistemleri

Havayolu firmalarının ulusal ve uluslararası birçok noktaya kısaya uçmasından dolayı ana faaliyetlerine kargo operasyonlarını da eklemişlerdir. Kargo operasyonlarını yürütebilmek için yolcu sistemlerinden bağımsız kargo özelinde bilgi sistemleri kullanmak gerekmektedir. Kargo operasyonlarında ki sistemler kargo varlıklarının yönetim, kargo satış ve rezarvasyon işlemleri, iş ve gelir yönetimlerinin süreçlerinde kullanılmaktadır. Kargo operasyon sistemlerinin kullanımın temal amacı şu şekildedir; finansal yönetim sağlamak, navlun işlemlerinin anlık izlenmesi, küresel gümrük uyumluluklarını sağlanması, dünya çapında tedariklerin gerçekleştirilmesi ve yüksek satış yüzdeleri elde edilmesi, kağıt işini ortadan kaldırarak sürece hız kazandırmak.

4.2.7. Ulaşım Güvenliği

Uçuş güvenliğinin sağlanması için sürekli yolcuların izlenmesi, kolluk kuvvetlerine ait sistemler ile havayolu firmalarının sistemleri entegre edilerek maksimum güvenliğin sağlanması.

4.2.8. İletişim ve Altyapı Sistemleri

Havayolu firmalarının yolcularına bilgilendirme yapmak gibi çeşitli amaçlar ile milyarlarca e-posta,sms vb. iletişim kanallarını kullanmaktadır. Herhangi bir aksama olması durumunda yolculara ulaşılamayacapından ve ticari zararlar ile karşılaşabilir. Bunun haricinde, tüm sistemlerin birbirisi arasında iletişimin sağlanması, verilerin transferi için eksiksiz ve doğru bir altyapı kurulmalıdır.

4.3. Türkiyedeki Sivil Havacılık Firmalarında Bilgi Sistemlerinin Kullanılması

Dünya genelinde olduğu gibi, Türkiyedeki sivil havacılık firmaları kar yüzdesini arttırmak, maliyetleri azaltmak ve yolcu memnuniyetini üst seviyede tutabilmek için bilgi sistemlerini kullanmaktadır. SHGM 2018 istatistiklerine göre; Türkiyede 11 adet sivil havacılık kuruluşu bulunmakta ve bu havayolu kurumlarında toplam 515 uçak yer almaktadır. 2019 eylül ayında; havalimanlarına iniş-kalkış yapan uçak sayısı, iç hatlarda 77.365, dış hatlarda ise 75.465 oldu. Hizmet verilen toplam uçak trafiği üst geçişler ile birlikte 194.923'e ulaştı. Eylülde, Türkiye genelinde hizmet veren havalimanlarında iç hat yolcu trafiği 8.668.089, dış hat yolcu trafiği 12.240.602 oldu. Direkt transit yolcular ile birlikte toplam yolcu trafiği 20.929.426 olarak gerçekleşti. Havalimanları yük (kargo, posta ve bagaj) trafiği; eylül ayı itibarıyla iç hatlarda 81.084 ton, dış hatlarda 244.718 ton olmak üzere toplam 325.802 tona ulaştı. (DHMİ ,2019) Rakamlara bakıldığında ne kadar yoğun bir operasyon olduğunu ve bilgi sistemlerinin ne kadar önemli olduğu anlaşılabilir. 2009 senesinde yapılan bir araştırmaya göre havayolu firmalarının bilgi sistemlerini hangi modüllerde kullandıkları değerlendirilmiştir. 2009 senesinde kuruluşlar tarafından kullanılan bilişim sistemleri modülleri Tablo.2 içerisinde yer almaktadır.

Applications/Modules Using Information Systems	Airline Operators											
	THY	Onur Air	Atlasjet	Pegasus	Sun Express	Sky		Freebird	Inter Express	Corendon	Saga	MNG
Airports Operations												
Flight information	X	X	X	X	X	X	X	X	X	X		X
Aircraft Operations												
Maintenance management	X	X		X	X			X			X	X
Catering	X	X	X	X								
Fleet and crew management	X	X	X	X	X	X	X	X	X		X	
Online education	X		X		X							
Flight planning	X	X	X	X	X		X					
Baggage Operations												
Baggage tracking	X						X					
Passenger Operations												
Check-in to boarding	X		X	X								
Commercial Management												
Accounting	X	X	X	X	X	X	X	X	X	X	X	X
Financing	X	X	X	X	X	X	X	X	X	X	X	X
Purchasing		X	X	X	X	X	X		X			X
Procuring		X	X	X	X		X			X		
Costumer relations	X	X	X	X	X	X	X					X
Reservations and ticketing	X	X	X	X	X		X			X		
Cargo Operations												
Cargo management	X						X					
Transportation Security												
Passenger security					X	X						
Passenger tracking	X		X	X								
Communications and Infrastructure												
Web applications	X	X	X	X	X		X					

Şekil 1. Bilgi Sistemleri Kullanım Cetveli

5. HAVACILIK SİSTEMLERİNDE BİLGİ GÜVENLİĞİ

5.1. Ulusal ve Uluslararası Mevuzatlar

Sivil Havacılık kuruluşları ana faaliyetlerini yerine getirebilmek için yolcu kişisel verileri, yolculara ait kredi kartı verileri gibi son derece hassas verileri sistemlerinde bulundurduğu için uluslararası birçok kanuna uyumlu hale gelmelidir. Aksi halde yasal yaptırımlar veya para cezaları ile karşılalıabilir.

5.1.1. Kişisel Verilerin Korunması Kanunu

Kişisel veirlerin gelişigüzel işlenmesi, yetkisiz kişilerin erişimine açılması, ifşası , kötüye kullanımı veya amaç dışı kullanımı sonucu kişisel hakların ihlal edilmesinin önüne geçilmesi için ilgili kanun çıkarılmıştır. Anayasa Mahkemesinin 9 Nisan 2014 tarih ve E:2013/122, K:2014/74 sayılı kararında da; "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı […]" amaçladığı tespit edilerek, "kişisel verilerin ticari işletmeler için kıymetli bir varlık niteliği kazanması neticesinde, özel sektör unsurlarınca yaratılan risklerin daha yaygın ve önemli boyutlara ulaşması ve terör ve suç örgütlerinin kişisel verileri ele geçirme yönündeki faaliyetlerinin artması gibi etkenler" sebebiyle kişisel verilerin geçmişte olduğundan çok daha fazla korunmaya muhtaç olduğu ifade edilmiştir.(KVKK, 2019)

Veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek ile verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür(KVKK, 2019) Türkiye Cumhuriyeti içerisinde sivil havacılık faaliyetleri yürüten tüm kurumlar KVKK ya uyumlu olmak zorundadır.

5.1.2. Genel Veri Koruma Regülasyonu (GDPR)

Avrupa Birliği(AB) Genel Veri Koruma Regülasyonu (GDPR), tüm Avrupa genelinde AB vatandaşlarını korumaya yönelik uyumlu bir dizi veri gizliliği yasası hazırlamak için geliştirilmiştir. Genel Veri Koruma Regülasyonu, Avrupa Birliği sınırları içerisinde yaşayan herhangi birinin kişisel verilerini işleyen tüm şirketler için, şirketin kendi konumu fark etmeksizin geçerli sayılmaktadır. Özellikle, hemen hemen tüm havayolu firmaları Avrupa Birliği üye ülkelerine sefer düzenlediği, üye ülkelerde yaşayan kişilere bilet satış işlemi gerçekleştirdiği için GDPR regülasyonuna tabi olmaktadır.

GDPR ile uyumlu olmayan denetleyiciler ve işleyiciler dahil tüm kurum ve kuruluşlar, yıllık küresel cirolarının %4'üne veya 20 milyon avroya (hangisi büyükse) varan miktarlarda ceza alabilir.(GDPR 2019) Global havayolu firmalarının küresel yıllık cirolarının yüksek olması nedeniyle karşılaşacağı cezalarda bir o kadar ağır olacaktır.

Bu nedenle, havayolu firmalarının çok ciddi maddi yaptırımlar ile karşılaşmaması için bilgi güvenliği'ne yatırım yapmalı ve sürekli iyileştirmelidir.

5.1.3. Kartlı Ödeme Endüstrisi Veri Güvenlik Stardantı(PCI/DSS)

Kartlı Ödeme Endüstrisi Veri Güvenlik Standardı (PCI DSS), kredi kartının işlenmesi, iletilmesi ve saklanması aşamalarında uyulması gereken mantıksal ve fiziksel bilgi güvenliği kurallarını tanımlamaktadır. Bu kurallar PCI (Payment Card Industry) adı verilen ve aralarında American Express, MasterCard Worldwide, Visa, Discover Financial Services gibi üyeleri bulunan bir konsey tarafından geliştirilmekte ve yayımlanmaktadır. Havayolu firmaları bilet satış ve benzeri faaliyetlerde yolcu kredi kartı bilgilerini talep ettikleri için PCI/DSS standartına uyumlu olmak zorundadır. Belirli aralıklar ile gerçekleştirilen denetimler sonrasında alınacak uyumluluk sertifikasından sonra faaliyetlerini devam ettirebilirler. Ağır cezaları maddeleri bulunan PCI/DSS startına göre, bilgi güvenliği olay başına 500000 $ para cezası kesilebilmektedir. Havayolu firmalarının

5.2. Havacılık Sistemlerinde Yaşanılan Bilgi Güvenliği Vakaları

Sivil havacılık kuruluşları sahip olduğu veriler, milyonlarca kişiye hizmet vermeleri, ülke bayrak taşıyıcı kuruluşlar olarak isimlendirilmelerinden dolayı saldırganlar tarafından hedef haline gelmektedir. Siber casusluk faaliyetleri, maddi zarar verme içgüdüsü, saldırgan grupların prestij kazanmaları gibi nedenlerden dolayı saldırganlar için cazip durumdadır. Bu nedenle, sivil havacılık firmaları bilgi güvenliği saldırılarına karşı hazırlıklı olmalıdır.

5.2.1. Cathay Pasific Havayolu Firması Vakası

Hong Kong merkezli Cathay Pasific havayolları'na düzenlenen siber saldırı sonucu müşterilere ait kimlik verileri saldırganlar tarafından çalınmıştır. Cathay Pasific tarafından yapılan incelemelerde sızan kimlik verileri arasında isim, uyruk, telefon numarası, doğum tarihi, elektronik posta adresi gibi bilgilerin bulunduğu belirlenmiştir. Türkiye'de 1286 kişinin veri ihlalinden etkilendiği, 155 kişinin pasaport numarasına erişildiği anlaşıldı. Türkiye Cumhuriyeti vatandaşlarının bu sızıntıdan etkilenmesi nedeniyle Cathay Pasific havayolları Kişisel Verileri Koruma Kuruluna gerekli bildirimleri yapmıştır. Fakat, olayın tespit zamanından aylar sonra bildirim yapılması nedeniyle ve yeterli güvenlik önlemlerinin alınmaması nedeniyle para cezası uygulamıştır.

6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (1) numaralı fıkrası çerçevesinde veri güvenliğini sağlamaya yönelik gerekli teknik ve idari ve tedbirleri almayan Şirket hakkında Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca 450.000 TL,- Öte yandan Şirket tarafından 07.05.2018 tarihinde gerçekleşen siber saldırıya ilişkin Kurula 25.10.2018 tarihinde bildirim yapılmasının, ihlalden etkilenen ilgili kişilere ise 25.10.2018 tarihinden itibaren bildirim yapmaya başlanmasının, Kanunun 12 nci maddesinin (5) numaralı fıkrasında yer verilen "en kısa sürede" bildirimde bulunma yükümlülüğüne aykırılık teşkil etmesi nedeniyle, Kanunun 18 nci maddesinin (1) numaralı fıkrasının (b) bendi uyarınca Şirket hakkında 100.000 TL,olmak üzere toplam 550.000 TL idari para cezası uygulanmasına,karar verilmiştir. (KVKK , 2019)

5.2.2. British Airways Vakası

Saldırganlar Britanya Havayolu firmasına ait web sitesi içerisine yerleştirdikleri zararlı yazılım ile yolcuları kendilerine ait web sitesine yönlendirerek yolcuların kimlik bilgilerini çalmışlardır. 21 Ağusos ile 5 Eylül 2018 tarihi arasında britanya havayolları'na ait web sitesinden uçak bileti satın almak isteyen yolcular dolandırıcılık amacıyla kurulan sahte bir web sitesine yönlendirilmektedir. Britanya havayoluna ait web sitesi içerisine gizlenen zararlı yazılım ile yapılan bu kötücül aktivite sonrasında yolcular yönlendirildiklerini bilmeden isimlerini, ödeme yaptıkları kredi kartı bilgilerini, rezervasyon tarihlerini ve ilgili birçok detayı (pasaport bilgilerini) vererek kişisel verilerinin çalınması olayıyla karşılaşmışlardır. Yaklaşık 500 binden fazla kullanıcının bilgisinin çalınması 8 Eylül 2018 tarihinde ortaya çıkmıştır. Brisitih Airway'ın yaptığı duyuruda, Siber saldırıya en hızlı şekilde cevap verildiğini saldırıdan 380 bin yolcunun etkilendiğini ,Güvenlik açıklarının giderildiğini ve yolcuların seyahat detaylarının ve pasaport bilgilerinin hırsızlıktan etkilenmediğini şeklinde beyan etmiş olsa da Şirketin saldırıdan 16 gün sonra polisle iletişime geçmeleri sistemdeki zayıf güvenlik önlemlerini ortaya koymaktadır. "İhlal bildirimleri zorunludur ve kuruluşların ihlalin farkına varmasını takip eden 72 saat içinde bildirimde bulunması gerekmektedir." (GDPR) Bu kurala uymayan Britinya havayolu ve bağlı olduğu hava yolu şirketi IAG'ye (International Airlines Group), kişisel verileri koruma kanunu kapsamında şimdiye kadar verilen en yüksek ceza kesilmiştir. İngiltere Bilgi Komisyon Ofisi (ICO), sistemindeki güvenlik açığı nedeniyle 500 bin kadar müşterisinin kart bilgilerinin bilgisayar korsanlarının eline

düşmesine engel olamayan havayolu şirketine 183.39 milyon pound para cezasına çarptırmıştır. 2017 yılında 15 milyar dolar gelir elde eden British Airways bu olay neticesinde neredeyse gelirinin %1,5 'i kadar bir kayıp yaşamasına neden olmuştur.

Bu nedenle regülasyonlara tabi olmak ve ciddi maddi zararlar ile karşılaşmamak için havayolu firmaları bilgi güvenliği yönetim sistemi oluşturmalıdır.

6. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

6.1. BGYS Nedir ?

Bilgi güvenliği; bilginin yetkisiz erişimler, kayıplar veya hatalardan korumakla ilişkilidir. Ancak yine de bilgiye tek başına bakılmamalıdır. O bilginin nerede bulunduğunu, nasıl ve nerede dolaştığını bilmek önemlidir. Bilgiye uygun koruma metotları geliştirmek için ilgili tüm bilgi işleme tesislerinin de, yani sistemler, servisler ve lokasyonların da korunmasının sağlanması gerekmektedir.

Tam anlamıyla bilgi güvenliğini ele alan tüm süreçlerin dahil olduğu bir yönetim sistemi kuruluşun iş risklerini belirleyerek azaltılmaktadır ve etkin bir kurumsal yönetim sağlamaktadır.

6.1.1. BGYS Gereksinimleri

BGYS gereksinimleri şu şekilde sıralanabilir;

- Hedeflerinin, iş hedeflerine uygun olduğundan ve bunları desteklediğinden emin olunabilmesi için üst yönetim tarafından sahiplenmelidir.
- İlgili tarafların ihtiyaç ve beklentilerini karşılamak üzere tasarlanmalıdır, böylece kuruluşun itibarı ve imajı iyileşecektir.
- İş içerisindeki tüm ekiplere ve faaliyetlere uygulanabilir olmalıdır. İşin çalışma şekli etrafında inşa edilmiş olmalıdır.

6.1.2. BGYS Oluşturmanın Faydaları

BGYS oluşturulduğu takdirde kuruluşlar iyileşecek ve gelebilecek tehditlere karşı korunacaktır. Kurum çalışanlarının bilinçlenmesini sağlayacak, etkin ve uzun soluklu bilgi güvenliği uygulama yapısı kurulacaktır. BGYS oluşturulması ile birlikte kapsamlı kaliteli güvenlik kontrolleri yapılacak ve tüm paydaşların kuruma olan güvenleri artacaktır.

6.2. Bilgi Güvenliği Yönetim Sistemi (BGYS) Standartları

BGYS sağlayabilmek için bazı standartlar kullanılmaktadır. Bu standartlar, 1993 yılında BS-7799 olarak duyurulan İngiltere tarafından geliştirilmiş bir yönetim standartı, 1999 yılında uluslararası bir standart olarak kabul edilmiş Ortak Kriterler (Common Criteria), 2000 yılında ise BS-7799 standartlarının ilk bölümü esas alınarak yayınlanan ve 2005 yılında revize edilen ISO/IEC 17799:2005 ve ISO 27001 standartlarıdır (Guan vd., 2003)- (Duan- Wu, 1999).

BGYS olarak adlandırılan ve daha birçok bilgi teknoloji standartlarıyla desteklenen bu yeni yönetim sistemi standartlarında, bilişim teknolojilerinin güvenliği ile ilgili kriterler ile bu sistemlerin yeterliliği ve denetimlerini ilgilendiren konu başlıkları altında ele alınarak sorgulama ve detay kontrolleri yapılmaktadır (Duan- Wu, 1999).

Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi için Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır.(Marttin, 2010)

6.2.1. ISO/IEC 27001:2013 Standartı

ISO/IEC 27001 standartı kuruluşların bilgi güvenliği yönetim sistemini nasıl kuracaklarını, yönetim sisteminin sürdürülebilmesi için dikkat edilecek hususları, kuruluş içerisinde nasıl uygulayacağını ve sürekli iyileştirme için gereken şartları ortaya koymak amacıyla hazırlanmıştır. Bilgi güvenliği yönetim sistemi'nin kurularak bemimsenmesi kuruluşlar için stratejik bir karardır. Kuruluşun bilgi güvenliği yönetim sisteminin kurulması ve uygulanmasında, kuruluşun ihtiyaç ve amaçları, güvenlik gereksinimleri, kullanılan kurumsal prosesler, kurumun boyutu ve yapısı etkilidir. Tüm bu etkileyen faktörlerin zaman içinde değişmesi beklenir. Bilgi güvenliği yönetim sistemi, bilginin gizliliği, bütünlüğü ve erişilebilirliğini risk yönetimi prosesini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir.

Bilgi güvenliği yönetim sisteminin kurumsal prosesler ve genel yönetim yapısının bir parçası olması ve bunlar ile entegre olması ve bilgi güvenliğinin süreçlerin, bilgi sistemlerinin ve kontrollerin tasarımında dikkate alınması önemlidir. Bir Bilgi güvenliği yönetim sisteminin kuruluşun ihtiyaçları doğrultusunda ölçeklenmesi beklenir. (ISO/IEC 27001/ 2013)

Bu standard, iç ve dış taraflar tarafından kuruluşun kendi bilgi güvenliği gereksinimlerini karşılayıp karşılamadığına ilişkin kabiliyetinin değerlendirilmesi amacıyla kullanılabilir.Bu standarda ortaya konulan şartların sıralaması, önem derecelerini yansıtmaz veya uygulanmaları gereken sıra ile ilgili bir zorunluluk ifade etmez. Liste halindeki maddeler sadece atıf amacı ile numaralandırılmıştır. ISO/IEC 27000, bilgi güvenliği yönetim sistemleri ailesine (ISO/IEC 27003 [2], ISO/IEC 27004 [3], ISO/IEC 27005 [4], de dâhil olmak üzere) ilgili terim ve tanımlar kapsamında atıfta bulunarak, bilgi güvenliği yönetim sitemlerine genel bakışı ve terimler sözlüğünü tarif eder.(ISO/IEC 27001/ 2013)

6.2.1.1. Faydaları

ISO/IEC standartına uygun bir BGYS kurulması kuruluşun bilgi güvenliği ile ilgili amaçlara daha fazla odaklanmasını sağlayarak bir bilgi güvenliği yönetim çerçevesi sunmaktadır.

Faydaları şunları içermektedir:

- Güvenlik ihlal olaylarında azalma
- Çalışanları elde tutmada artış
- Finansal kayıpları azaltma örn. Cezalar,sigorta
- İhlal olaylarının düzeltme maliyetlerini azaltma
- Marka ve itibarin korunması
- Müşterileri elde tutma
- Sektöderdeki diğer kurumlar ile olan rekabette avantaj sağlama
- Müşterilere güven aşılayarak sadakatlerini kazanma
- Çalışanların politika ve prosedürlere uyumunu sağlama

7. ISO/IEC 27001:2013 STANDARTI'NIN SİVİL HAVACILIK KURULUŞLARINDA UYGULANMASI

7.1. Planla, Uygula, Kontrol Et ve Önlem Al (PUKÖ) Yaklaşımı

ISO/IEC 27001 standartının uygulanarak bir BGYS'nin oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için bir süreç yaklaşımının kuruma adapte edilmesi gerekmektedir. Bu yaklaşım planla,uygula,kontrol et ve önlem al (PUKÖ) modeli olarak adlandırılır. PUKÖ yaklaşımı tüm BGYS süreçlerinde uygulanmalıdır.

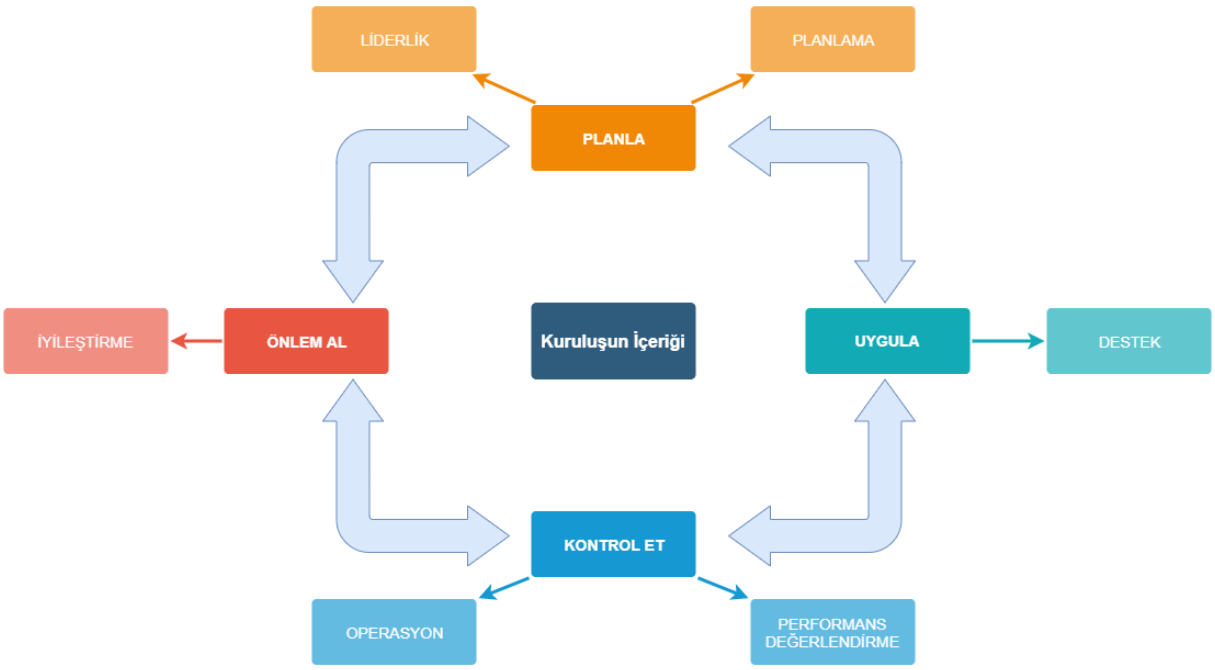
Planla (BGYS'nin Kurulması): Kuruluş bilgi güvenliği gereksinimlerini, ilgili taraflardan gelen şartları anlayarak ve politikalar, süreçler ve prosedürler oluşturarak planlama yapmalıdır.

Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi): Politikaları, kontrolleri, süreçleri ve prosedürleri uygulamak ve tarif edilen işletme yöntemiyle BGYS uygulanması.

Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi): BGYS'nin performansı değerlendirilmeli, ölçülmeli, izlenmeli ve gözden geçirilmelidir.

Önlem Al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi): Kuruluşlar BGYS'ni sürekli iyileştirmek için aksiyonlar almalıdır.

Şekil 6'da ISO 27001 standartının ana maddelerinin PUKÖ döngüsü içerisinde nereye işaret ettikleri belirtilmiştir.



Şekil 2. PUKÖ Döngüsü

7.2. BGYS ‘nin Kurulması

BGYS’nin kurulması ve uygulanması 3 aşamadan oluşmaktadır diyebiliriz. Bu aşamalar şu şekildedir;

1.Aşama (Neredeyiz ?): Kurumların mevcut durumları öncelikli olarak standartın şartları ile karşılaştırılır. Karşılaştırma sonucunda kuruluşun standart uyumluluğu anlamında nerede olduğu, hangi konularda boşluklarının ve eksiklerinin olduğu belirlenir.

2.Aşama(Uygula, İşlet): Kuruluşun yaklaşımındaki boşlukların doldurulması ve böylece standarta göre tetkik edilebilmesini ve memkünse sertifika edinilmesini kapsayan aşamadır.

3.Aşama(Yönet, İyileştir): BGYS takip edilmesi gereken ve sürekli iyileştirilme zorunluluğu olan bir yönetim sistemidir. Bu aşamada sistem ile ilgili iyileştirmeler yönetilmelidir.

7.3. Boşluk(GAP) Analizinin Yapılması

Kuruluş ilk olarak BGYS kapsamında olması planlanan sistemlerde mevcut durumun izlenmesi ile eksikliklerin ortaya konulması için Gap (Boşluk) analizi uygulaması yapmalıdır. Kuruluşun hedeflediği konum ile şuanda bulunduğu durum arasındaki farkın ne olduğunun detaylı olarak çıkarıldığı bir analiz yöntemidir.

7.3.1. GAP Analizinin Uygulanması

GAP analizinin gerçekleştirilmesi için kontrol listeleri, mülakatlar, önceki tetkik veya gözden geçirme sonuçları, önceki vakalar ile ilgili kayıtların incelenmesi gibi yöntemler kullanılabilir. Genellikle mülakat üzerinden giden GAP analiz çalışmalarında ISO 27001 standartının 4. Ve 10. Maddeler arasında ki maddelere verilen cevaplar değerlendirilir. Daha sonra, ISO 27001 EK-A kontrol maddeleri gözden geçirilir. Çalışma sonucunda standartın tüm maddelerine ne kadar uygun olunduğu değerlendirilerek çalışma tamamlanır.

7.4. Kuruluşun Bağlamı

Madde 4 kuruluşun BGYS'ni etkileyen iç ve dış hususların belirlemesi gerektiğini ve bu hususların ihtiyaç ve beklentilerini idrak ettikleri ile ilgilidir. Bu konuların neler olduğu kuruluşun ne tür bir kuruluş olduğuna göre değişir. Bu hususların gereksinimleri yasal ve düzenleyici kuruluşların maddeleri ve sözleşmeden doğan yükümlülükleri içeriyor olabilir.

Daha sonrasında kuruluş iç ve dış hususlarını içeren, gereksinimleri de belirleyerek BGYS kapsamı belirlemelidir. BGYS kapsamı standartın diğer maddelerinin işletilmesi gereken bir alanı ifade etmektedir.

7.4.1. İç ve Dış Hususların Belirlenmesi

Havacılık sektöründe ki kurumlar iç ve dış hususları belirlerken BGYS'yi neden oluşturmak istediğini yasal zorunluluk veya kuruluş içerisinde ki bilgi güvenliğini sağlanması gibi hedefleri değerlendirmelidir. Dış hususlara örnek verecek olursak Türkiyede sivil havacılık kurumlarının otoritesi olan Sivil Havacılık Genel Müdürlüğü (SHGM) dış husus olarak değerlendirilebilir. İç hususlar ise kuruluşun yapısı, kurumun kültürü gibi iç yapı ile alakalı konulardır.

7.4.2. İlgili İlişkili Taraflar ve Bunların İhtiyaçları

İlişkili olabilecek tarafların ve ihtiyaçlarının belirlenmesi gerekmektedir. Bu ihtiyaçlar yasal ve düzenleyici şartları, sözleşmeye bağlı zorunlulukları da içerebilir. Örneğin, SHGM 93582559-200/E.826 sayılı genelge ile sivil havacılık sektöründe ki kurumlara ISO/IEC 27001 standartını zorunlu hale getirmiştir. Kurumlar bu genelge'yi bir gereklilik olarak kabul edebilir. Ayrıca, KVKK gibi bilgi güvenliği ile alakalı kanunlara uyumlu olabilmek için kuruluşlar BGYS oluşturarak kendilerini daha güvenli hale getirebilir.

7.4.3. Kapsam

Kuruluşlar kapsamı oluşturabilmek için bilgi güvenliği yönetim sisteminin sınırlarını ve uygulanabilirliğini belirlemelidir. Kuruluşlar iç ve dış hususları, bu hususların gereksinimlerini, kuruluş tarafından gerçekleştirilen faaliyetler arasındaki arayüzler, bağımlılıklar ve diğer kuruluşları değerlendirek kapsamı oluşturmalıdır.

SHGM'nin yayınlamış olduğu genelgede aşağıdaki maddeler kuruluşların kapsamını oluşturmasında yardımcı olmaktadır.

“b.İlgili kurum/kuruluşların kişisel verilerin, uçuş operasyon ve havayolu operasyon bilgilerinin tutulduğu sistemlerinin ISO/IEC 27001:2013 sertifikasyonlarını TÜRKAK’a ya da Ülkemizde tanınırlığı olan uluslararası eşdeğerlerine akredite olmuş belgelendirme firmalarına 01.01.2018 tarihine kadar yaptırmaları,

c. İlgili kurum/kuruluşların bilişim sistemleri ve endüstriyel kontrol sistemlerinin tamamının ISO/IEC 27001:2013 sertifikasyonlarını TÜRKAK’a ya da Ülkemizde tanınırlığı olan uluslararası eşdeğerlerine akredite olmuş belgelendirme firmalarına 31.12.2018 tarihine kadar yaptırmaları gerekmektedir.”(SGHM, 2018)

İlgili maddeler değerlendirilerek, kuruluşlar kapsam olarak ilgili bilgi sistemlerini, sistemlerin bulunduğu lokasyonları veya ilgili süreçleri dahil edecek şekilde kapsamlarını belirleyebilir.

Örneğin; İstanbul merkez ofisinden, müşterilere havayolu bilet satış işlemleri gerçekleştirilen sistemler, bu sistemlerdeki fonksiyonları destekleyen personel ve varlıkları kapsam dahilindedir.

Kapsam yazılı bilgi olarak mevcut olmalıdır.

7.5. Liderlik

Üst yönetim sorumluluğu ve katılımı yıllardır yönetim sistemi standartlarının özelliklerinde olagelmiştir, ancak ISO/IEC 27001:2013 bunu daha bariz bir şekilde yeniden vurgulamakta, katılımın gösterilmesi için belirli yolları zorunlu tutmaktadır.

Üst yönetim bir kuruluşun kültürünü ortaya koymaktadır. Çalışanlar ancak üst yönetimin aşağıdam belirtilen maddeleri yaptıkları zaman bilgi güvenliğini benimseyeceklerdir.

- Çalışanları BGYS’nin etkinliğine katkı sağlamaları için motive etmek ve yetkilendirmek
- BGYS gerekliliklerini oluşturmak ve kuruluşun süreçleri ile entegre etmek
- Bilgi güvenliği yönetim sonuçları için kurumsal sorumluğu pekiştirmek
- Kuruluşun bilgi güvenliği hedeflerine ulaşmasında insanların tam olarak dahil olabileceği bir iç ortam yaratmak ve sürdürmek
- Sürekli iyileştirmeyi desteklemek

- Kendi sorumluluk alanlarına uygun olan liderlik vasıflarını göstermek için örnek olarak yönetmek ve diğer ilgili yönetim görevlerini desteklemek.

7.5.1. Liderlik ve Bağlılık

Üst yönetim liderlik ve katılımı aşağıdaki şekillerde göstermelidir:

- Bir bilgi güvenliği politikası oluşturmak
- Bilgi güvenliği hedefleri oluşturmak
- BGYS için gerekli kaynakların mevcut olmasını sağlamak
- BGYS görev, sorumluluk ve yetkilerinin atanmış olmasını sağlamak
- Etkin bilgi güvenliği yönetim sisteminin öneminin anlatılabilmesi

Bilgi güvenliği yönetiminin yönetim kurulu seviyesinde ele alınması kuruluş genelinde risklerin yönetilmesi ve anlaşılması için kapsamlı bir yaklaşımın uygulanmasını garanti altına alacaktır.

7.5.2. Politika

Bu madde bilgi güvenliği politikası ile ilgili gereklilikleri ele almaktadır. Üst yönetim aşağıdakileri karşılayan bir bilgi güvenliği politikası oluşturmalıdır.

- Kuruluşun amaçlarına uygun
- Bilgi güvenliği hedeflerini içeren veya bilgi güvenliği hedeflerinin oluşturulması için çerçeve sağlayan
- Bilgi güvenliği ile ilgili uygulanabilir gereklilikleri sağlamak için taahhüt içeren
- BGYS'nin sürekli iyileştirilmesi için bir taahhüt içeren

İdeal olan, politikanın kuruluşun bilgi güvenliği amaçlarını ana hatlarıyla belirlemesive 2 sayfadan uzun olmamasıdır. Politikanın dökümante edilmiş bilgi olarak mevcut bulunması ve kuruluş içerisinde ilgili taraflara iletilmesi gerekmektedir. Bir politikanın iletişimi tam olarak sağlanmadığı sürece kurum içerisinde işlemeyecektir. Bunun iletişiminin nasıl yapılacağı kuruluşa, kuruluşun yapısına ve kültürüne göre değişmektedir. İç iletişim için birçok yöntem kullanılabilir. İlgili taraflara personel el kitabı, duyuru panoları, kuruluş içi dergiler, iç eğitimler ve oryantasyon veya kurum içi ağ üzerinden bilgi güvenliği politikası duyurulmalıdır.

Sivil havacılık kuruluşlarının otoritesi konumunda bulunan SHGM'nin bilgi güvenliği politikası şu şekildedir;

BİLGİ GÜVENLİĞİ POLİTİKAMIZ
Sivil Havacılık Genel Müdürlüğü bilgi işlem faaliyetleri, bilgi varlıkları ve bu varlıkları korumak amacıyla kullandığı iş süreçleri dahilinde; Bilgi Güvenliği Yönetim Sistemimiz tüm faaliyetlerimizin ISO 27001:2013 standardına uygun yürütülmesini garanti altına alır. Bilgi İşlem faaliyetleri kapsamında; • Genel Müdürlüğümüz ve Genel Müdürlüğümüz ile ilişkili tüm kurum, kuruluş ve şahısların bilgi varlıklarına güvenli bir şekilde erişim sağlanmasını, • Bilginin kullanılabilirliğini, bütünlüğünü ve gizliliğini korumayı, • Genel Müdürlüğümüzün bilgi varlıkları üzerinde oluşabilecek riskleri değerlendirmeyi ve yönetmeyi, • Genel Müdürlüğümüzün güvenilirliğini ve marka imajını korumayı, • Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygulamayı, • Tabi olduğu ulusal ve uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerinden ve anlaşmalardan doğan bilgi güvenliği gereksinimlerini sağlamayı, • İş / Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisi azaltmayı ve işin sürekliliğini ve sürdürülebilirliğini sağlamayı, • Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumayı ve iyileştirmeyi taahhüt eder.

Tablo 2. Bilgi Güvenliği Politikası

7.5.3. Görevler, Sorumluluklar ve Yetkiler

Üst yönetim bilgi güvenliği ile alakalı görevler için sorumlulukların ve yetkilerin atanmasını ve iletişiminin yapılmasını sağlamalıdır. Kendisine bir faaliyet için sorumluluk atanan herkesin görevlerini iyi anlaması gerekmektedir. Kimin hangi konuda yetkisinin olduğunun iyi anlaşılması BGYS'nin sağlıklı yürüyebilmesi açısından önemlidir. Örneğin, bilgi güvenliği müdürünün günlük BGYS yönetimi sorumluluğu olabilir, fakat BGYS ile ilgili değişiklikleri onaylamaya veya karar vermeye yetkisi olmayabilir.

ISO/IEC 27001 standartının 5. Maddesine göre yönetim aşağıda belirtilen maddeler için sorumluluk ve yetki ataması yapmalıdır:

a) Bilgi güvenliği yönetim sisteminin IEC/ISO 27001 standartında yer alan şartlarına uyum sağlamasını temin etmek,

b) Yönetime bilgi güvenliği yönetim sisteminin performansını düzenli olarak raporlama.

Roller ve Sorumlulukların atanmasına aşağıdaki şekilde örnek verilebilir.

“Bilgi varlıklarının teknik sahipleri bilginin gizlilik bütünlük ve kullanılabilirliğini sağlamak için;

- Bilgi varlıklarına yetkisiz olarak erişilmesini; bilgi varlıklarının yetkisiz olarak değiştirilmesini veya tahribatını önlemek suretiyle, bilgi varlıklarını korurlar.
- Operasyonun mümkün olan en kısa hizmet kesintisi ile devam etmesini sağlamak için gerekli süreçlerin tanımlanmasını ve uygulanmasını sağlarlar.
- Bilgi güvenliği gerekliliklerini gözetirken, ihtiyaç duyulduğunda bilgiye hızla erişilebilmesi için karmaşıklığı ortadan kaldıracak dengeyi kurarlar.
- Çalışanlarını ve birlikte çalıştıkları üçüncü taraf çalışanlarını bilgi güvenliği gereklilikleri, rolleri ve sorumlulukları konusunda bilgilendirirler ve bilinçlendirirler

Bütün bu faaliyetlerin kurumsal ISO/IEC 27001 standardı ile uyumlu bir çerçevede ele alınması için, tüm kuruluşun süreç ve hizmetlerini kapsayan bir Bilgi Güvenliği Yönetim Sistemi kurulmuş ve İnsan Kaynakları ve Yönetim Sistemleri Müdürü, “BG Yönetim Temsilcisi” olarak atanmıştır.**”(YDA Havacılık, 2018)**

7.6. Planlama

Standartın 6. maddesi beklenmeyen etkileri önleyerek veya azaltarak BGYS’nin istenen sonuçlarını elde edip edemeyeceğini ve sürekli iyileştirmeyi başarıp başaramayacağını belirlemek için kuruluşun yapı taşlarının mevcudiyetini sağlar. Planlama maddesinin kavranabilmesi için risk,zafiyet, varlık ve tehdit gibi kavramların kuruluşlar tarafından anlaşılması gerekmektedir. ISO/IEC 27001:2013 standartı risk tabanlı bir standarttır desek yanlış olmaz. Bu nedenle, kuruluşlar risklerini çalışmalı ve kuruluşlar riskleri ele alarak BGYS sürekliliğini planlamalıdır.

Şekil 3. Risk Yönetimi

7.6.1.Kavramlar

7.6.1.1.Risk

Zafiyet, varlık ve tehditlerin kesişimidir. Mevcut kontrollerin yetersiz gelmesi durumunda oluşan zafiyetler, tehditlerin karşısında riskin gerçekleşme olasılığını arttırır. Risk, gerçekleştiğinde en az bir varlığın gizlilik, bütünlük, erişilebilirlik unsurlarına zarar gelmesi durumunda, varlıkları ya da kurumu finansal, stratejik, uyumluluk, oprasyonel, itibari vb. açıdan olumsuz etkileyen olay ya da durumdur. Risk çeşitleri aşağıdaki gibi sayılabilir.

a. Stratejik Risk

Kurumun ileriye yönelik değişiklikleri önceden fark ederek faaliyet alanının olumsuz etkilenmemesi için önlemler almasını gerektiren risklerdir. Örneğin, Sunucuların üç yıllık kullanım süresi varsa, 3 yıl sonra destek alınamayacak, güncel olmayan sistemlere sahip olma riskinin azaltılması için her 3 yılda bir sunucuların upgrade edilmesi gerekir. Bugünden 3 yıl sonraki bakım, destek süreçlerini yönetmek, bütçe ayırmak, bakım anlaşmalarında ilgili maddeleri eklemek bu stratejik risk için uygulanan kontrollerdir. Kontroller riskin gerçekleşme olasılığını azaltır.

b. Uyumluluk Riski

Uymakla yükümlü olunan kanunlar, regülasyonlar, standart ve yönetmeliklere göre bir dizi gereksinimin yerine getirilmesi gerekmektedir. Uyumluluğun sağlanamadığı durumlarda cezai yaptırımlar olabilmektedir. Aynı zamanda ilgili faaliyetin uyumluluk sağlanana kadar durdurulması riski de mevcuttur. Örneğin kredi kartı ile işlem yapılabilmesi için PCI-DSS uyumluluğunun korunması gerekmektedir. İlgili tüm personelin PCI-DSS gereksinimlerini yerine getirmesi gerekmektedir. Bu kapsamsa yapılan iç kontroller, gereksinimlerin sağlanması riskin yönetimi için kontroldür ve olasılığı düşürmektedir.

c. Finansal Risk

Kurumun finansal kayıp risklerini yönetmesi amacıyla ödeme kanallarının güvenliğinin sağlanması için PCI-DSS uyumlu olması ya da IT sistemleri ve altyapısının saldırılara ve ataklara karşı güvenli olabilmesi için IT güvenlik projelerine bütçe ayırması finansal kayıp risklerine karşı uygulanan kontrollere örnektir.

d. Operasyonel Risk

Operasyonel kesintilere neden olacak dahili sistem hatalarına yönetmek için izleme , acil müdahale planlarını yapma ya da iş sürekliliğinin sağlanması için yedekli yapıda çalışma operasyonel risk yönetimine örnektir.

e. İtibari Risk

Kurumun itibar kaybetmesine neden olabilecek risklerdir. Örneğin, veri sızıntısı tehditinin karşısında kritik verilerin yetkisiz kişilerin eline geçmesi ve sosyal medyada paylaşılması kuruma hukuki, finansal zararların yanı sıra itibari zararda verecektir. Bu örnekte finansal ve hukuki zarar ,sözleşme ve sigorta ile transfer edilebilir durumdadır fakat itibari zararın transferi mümkün değildir.

f. Diğer Riskler

Doğal afetlerden deprem için bina güçlendirme çalışmaları deprem riskinin yönetimine bir örnektir.

7.6.1.2. Zafiyet

Bir tehdite karşı, riskin oluşma olasılığını arttıran zayıflık, açıklıktır. Örneğin: Sistem tasarımı, uygulama, yazılım geliştirme eksiklikleri, hatalı konfigüre edilmiş yazılım veya network cihazları önleyici kontrollerin yetersiz kalması vb.

7.6.1.3. Tehdit

Varlıkları, kurumu tehlikeye sokan, gizlilik, bütünlük ve erişebilirliğine zarar veren durum, olaydır. İç tehditler (çalışanlar vb), dış tehditler (siber saldırılar, zararlı yazılımlar vb) ve doğal tehditler(deprem, sel, yangın vb) örnektir.Kuruluşlar tarafından dikkate alınması gereken birçok tehdit çeşidi bulunmaktadır.

a. Çelişen Tehditler

Güvenilen personel, rakipler, tedarikçiler, müşteriler vb

b. Kaza Tehditleri

Hatalar, dikkatsizlikler

c. Yapısal Tehditler

Cihaz, yazılımlarda meydana gelen yapısal bozulmalar örneğin sunucuların hard disk'lerinin bozulması

d. Çevresel Tehditler

Doğa ya da insan kaynaklı çevresel tehditler (Deprem, yangın, sel vb)

7.6.1.4. Varlık

Kurum için değerli olan her hangi bir nesne varlık olarak tanımlanır. Bilgi varlıkları ise , bilgiyi işleyen, saklayan, depolayan, transfer eden varlıklardır.

Örneğin: Bilgisayarlar, Sunucular, firewall, dokümanlar, uygulamalar, insan kaynakları, fiziksel tesisler, süreçler vb.

7.6.2. Riskleri ve Fırsatları Ele Alan Faaliyetler

Kuruluşların standartın 4. Maddesi içerisinde belirtilen maddeleri, yani; uygulanabilir iç ve dış konuları, ilgili taraflar ve bunların ele alınacak risklerin ve fırsatların belirlenmesi ile ilgili gereklilikleri de dahil ederek risk değerlendirme ve risk işleme faaliyetlerini nasıl yapacaklarını planlamaları gerekmektedir. Bir şekil üzerinden ifade edilmesi gerekirse Standart risk yönetimine aşağıdaki noktalardan yaklaşmaktadır

7.6.2.1. Risk Değerlendirme

ISO/IEC 27001 standartının en önemli maddelerinin başında risk değerlendirme gelmektedir. Özellikle, belgelendirme denetimlerinde denetçiler kapsam içerisinde yer alan birimlerin yöneticileri ile birimlerinin risklerini konuşmaktadır. Risk ve fırsatların kuruluşlar tarafından bilinerek dökümante edilmesi denetçilerin ilk baktığı noktalardan biridir.

Kuruluşlar risk değerlendirmelerini nasıl yapacaklarını planlamalı ve süreçlerini dökümante etmeleri gerekmektedir. Riskleri kabul etmek için kriterleri, risk değerlendirmelerini ne zaman yapılacağını içeren bir bilgi güvenliği risk değerlendirme süreci tanımlanmalıdır. Aynı zamanda tekrarlanan bilgi güvenliği risk değerlendirmelerinin tutarlı ve geçerli sonuçlar ürettiğinden emin olunmalıdır. Riskin kuruluş tarafından herhangi bir işleme tabi olup olmayacağını belirlemek için risk kabul kriterleri belirlenmelidir.

Risk değerlendirmeleri planlı aralıklarla veya önemli değişiklikler gerçekleştirildiğinde yapılmalıdır. Kuruluşlar aşağıdaki durumlarda risk değerlendirmesi yapmaya karar verebilir.

- İşle ilgili, bilgi güvenliğini etkileyecek önemli değişiklikler varsa
- Bilgi güvenliği gereklilikleri içeren yeni bir sözleşme var ise
- Bir bilgi güvenliği vakası yaşanmış ise
- Periyodik aralıklarla

7.6.2.2. Risk Kabul Kriterlerinin Oluşturulması ve Sürdürülmesi

Kuruluşlar risklerinin kabul kriterlerini belirlemeli, risklerini bu kabul kriterlerine göre işlemelidir. Özellikle, bu kriterlerin ölçülebilir değerler üzerinden oluşturulması kuruluşlar tarafından önemlidir.

Kuruluşlar riskleri tehdit eden unsurları tanımlayarak gerçekleşme olasılıklarına göre değerler vermelidir. Tablo 3 içerisinde yer alan benzer tehditler tanımlanabilir ve Tablo 4'te ki gibi olasılık ölçümleri yapılabilir.

Tehtid/Konu / İçerik
Bilgi güvenliği süreciyle İK sürecinin entegre olarak yürütülmemesi

	İşe alım, işten ayrılma ve transfer süreçlerinde gerçekleştirilecek faaliyetlerin belirli bir standarta veya metoda dayandırılmaması
	Bilgi güvenliğiyle ilişkili farkındalık eğitimlerinin verilmemesi veya farkındalık eğitimlerinin personel tarafından alınmaması, tekrarlanmaması
	Disiplin sürecinde eksikliklerin ve yetersizliklerin bulunması
	Varlık yönetiminin etkin olmaması
	Uygulamalara ilişkin sahipliklerin belirlenmemesi ve sorumluluk atamalarının yapılmaması
	Varlık yönetiminin gerekliliği olan bilgi sınıflandırmasının yapılmaması
	Dışarıya gönderilen cihazlar için takip gerçekleştirilmemesi ve herhangi bir takip formu kullanılmaması
	Yetkisiz erişimlerin meydana gelmesine ilişkin sistem zafiyetlerinin bulunması
	Erişim yetkilerinin verilmesine/alınmasına yönelik tanımlı süreçlerin bulunmaması
	Görevler ayrılığına uygun olarak yetki tahsisinin gerçekleştirilmemesi
	Erişim yetkilerinin düzenli olarak gözden geçirilmemesi
	Yönetici yetkilerinin çok sıkı kontrollerle verilmemesi ve ortak yönetici hesaplarının kullanılması
	Transfer olan, işten ayrılan ve geçici yetkilendirilen kullanıcıların yetki sürelerinin dolmasıyla birlikte yetkilerinin zamanında alınmaması
	Mobil cihazlarında yeterli güvenlik kontrollerinin bulunmaması
	Ortak kullanılan jenerik hesapların bulunması
	VPN erişimlerinin sürelerinin gözden geçirilmemesi ve mümkün olabilecek erişim kontrollerinin uygulanmaması
	Güçlü yapıda şifrelerin kullanılmaması ve kullanıcıların bu şifreleri kullandırmaya yönelik sistemsel zorlamaların bulunmaması
	Şifrelerin kriptolanmadan saklanması
	Verilerin gizliliğinin sağlanmasına yönelik risk değerlendirme sonuçlarına istinaden ortaya çıkan gizli verilerin kriptolanmaması
	Kriptolamayı sağlayan anahtarların yetkisiz kişilerin eline geçmesi
	Veri aktarımları için (FTP vb.) şifrelemeye sahip olmayan servislerin kullanılması
	Fiziksel açıdan kritik alanların erişim güvenliğinin sağlanamaması
	Fiziksel açıdan kritik alanların çevresel güvenliğinin sağlanamaması
	Fiziksel erişim yetkilerinin verilmesine/alınmasına yönelik tanımlı süreçlerin bulunmaması
	Bilgi sınıflandırması kapsamında ortaya çıkan kurumun belirlemiş olduğu standartlara uygun olarak fiziksel önlemlerin alınmaması

	Yerleşkeye giriş gerçekleştirmek isteyen ziyaretçilerin kayıt altına alınmaması (ziyaret nedeni, ziyarete gelinen kişi, firma ismi, isim soyisim vb. bilgiler) ve ziyarete yönelik kurum bünyesinde çalışan yetkili biri tarafından refakatin gerçekleştirilmemesi
	Data center, öteki sistem odaları ve depo ve arşiv alanlarına nem ve su ölçer konmaması
	Kameraların olmaması/kapı girişleri, jeneratör cihazı gibi hassas yerleri görmemesi
	Kameraların merkezi bir yerden izlenmemesi ve kayıt altına alınmaması
	3. parti firmalar ile kurum arasındaki ağ bağlantılarının güvenliğinin sağlanmasına ilişkin gizlilik anlaşmaların bulunmaması
	Değişikliklere ilişkin denetim izlerinin tutulmaması değişikliklerin kim tarafından, ne zaman, hangi uygulama/tablo üzerinde ve hangi talebe istinaden gerçekleştirildiğine yönelik bilgiye erişilememesine sebep olabilir.
	3. parti firmalarla yapılan, hizmete yönelik resmi sözleşmenin bulunmaması
	3. parti firmalara verilen erişimlerin sınırlandırılmaması ve sürekli takibin gerçekleşmesine ilişkin mantıksal ve fiziksel güvenlik önlemlerin oluşturulmaması
	3. parti firmalara verilen erişim haklarının ve yetkilerin düzenli olarak kontrol edilmemesi
	Hizmet sağlayıcısı firmalar ile kurum arasında servis seviyesi anlaşmalarının bulunmaması
	Temin edilen hizmete yönelik yedek tedarikçilerin/hizmet sağlayıcıların bulunmaması
	Servis sağlayıcılar ile kurum arasında imzalanan sözleşmelerde bilgi güvenliği ve gizlilik içerikli maddelerin ve güvenlik taahhütnamelerinin bulunmaması
	Tedarikçi ve destek hizmeti firmaların takibine yönelik kurum bünyesinde envanterin oluşturulmaması, sorumlulukların belirlenmemesi, tedarik edilen hizmetin/ürünün, destek hizmeti firmasının iletişim adresinin vb önemli bilgilerin belirtilmemesi
	Periyodik olarak tedarikçi firmaların teknik yeterliğinin, performansının ve müşteri memnuniyetinin değerlendirilmemesi
	Kritik sistemlere/uygulamalara ilişkin maksimum kabul edilebilir veri kaybı ve maksimum geri dönüş zamanı kriterlerinin ilgili sistem/uygulama sahipleriyle belirlenmemesi
	Kritik çalışanın yedeğinin bulunmaması ve sistemlerin yedeklenmemesi
	Sürekliliğin sağlanmasına ilişkin periyodik test/tatbikatlarının yapılmaması ve iş sürekliliğiyle ilgili farkındalık eğitimlerinin verilmemesi
	İç denetim çalışmalarının, Kurum tarafından gerçekleştirilmemesi
	Kurumun ilgili mevzuatlara uyumla alakalı eksikliklerinin bulunması
	Kurum bünyesinde Bilgi Güvenliği Risk Değerlendirme çalışmalarının ve gözden geçirmelerin yapılmaması
	Deprem/yangın/sel gibi doğal afetler vb. nedenlerle oluşan sorunlara karşı gerekli önlem alınmaması nedeniyle BT faaliyetlerinin kesintiye uğraması
	Kurumda tutulan kart verisi bileşenlerinin tümüne/herhangi birinin gizliliğine/bütünlüğüne/erişilebilirliğine yönelik kötü niyetli eylemler gerçekleştirilmesi
	Kurumda imtiyazlı kullanıcıların erişim haklarının ve aksiyonlarının izlenmemesi
	Sistem verisinin kazayla değiştirilmesi

Sözleşme şartlarına uyumsuzluk / Sözleşmelerin fesh edilmesi/Sözleşmesel hukuki yaptırımlar
Tedarikçi aktiviteleri tarafından oluşan hasarlar
Sızma Testleri sırasından hasarların oluşması
Kayıtların yetkisiz imhası
Medyaların bozulması/işlevselliğini yitirmesi
Şifrelerin açığa çıkması
Gizli konuşmaların ilgisiz kiişiler tarafından dinlenmesi
Kayıtlarda oynama (doğrulupa aykırı)
Dolandırıcılık
Endustriyel Casusluk
Bilginin sızması, gizliliğinin açığa çıkması, ifşası

Tablo 3. Tehditler Listesi

Tehdit Olasılığı Değeri	Tehdit Olasılığı Tanımı
1	Olası değil / Daha önce karşılaşılmamış. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında etkin bir şekilde çalışmakta ve tehdidin oluşmasını/etkisini önlemektedir.
2	Son 3 yılda yaşanmış / Üç yılda bir ortaya çıkması muhtemel. Mevcut kontrol ya da kontroller kısmen etkin ve tehdidin her ortaya çıkışında çoğunlukla doğru işlemektedir ve önleyici etki göstermektedir.
3	Son bir sene içerisinde yaşanmış / sene içerisinde tekrarlaması muhtemel. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında başarısız olabilmektedir veya bu tehdidi bertaraf edecek bir kontrol bulunmamaktadır.
4	Son bir sene içerisinde iki kere yaşanmış / sene içerisinde altı ayda bir tekrarlaması muhtemel. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında başarısız olabilmektedir veya bu tehdidi bertaraf edecek bir kontrol bulunmamaktadır.
5	Son bir sene içerisinde dört kere yaşanmış / sene içerisinde üç ayda bir tekrarlaması muhtemel. Mevcut kontrol ya da kontroller tehdidin her ortaya çıkışında başarısız olmaktadır veya bu tehdidi bertaraf edecek bir kontrol bulunmamaktadır.

Tablo 4. Tehdit Olasılık Değerleri

Kuruluşlar risklerini bilgi güvenliğinin üç temel unsuru olan gizlilik, bütünlük ve erişebilirlik unsurlarını dikkate alarak gözden geçirmelidir. Riskin gerçekleşmesi durumunda kuruluş bu üç unsur açısından ne gibi etkiler ile karşılaşır tanımlamalı ve ölçülebilir değerler atamalıdır. Tablo5,6 ve 7 içerisinde gizlilik,bütünlük ve erişilebilirlik için örnek etki değeri tanımları bulunmaktadır.

Etki Değeri	Etki Değeri Tanımı	GİZLİLİĞİN KAYBI
1	ÇOK DÜŞÜK	- Bilgi güvenliği vakası durumunda hassas bilgi ifşa olmaz. İfşa olan bilgi, kurumu hiç etkilemez veya etkisi göz ardı edilebilir. - Bilgi'nin kaybı veya gerçekleşen olay sadece yönetim tarafından bilinir. - Sözleşme şartlarında veya kanuni düzenlemelerde, kolay giderilebilecek bir problem veya uyumsuzluk oluşur.
2	DÜŞÜK	- Bilgi güvenliği vakası durumunda hassas bilgi ifşa olmaz. İfşa olan bilgi, kurumu çok az etkiler. - Bilgi'nin kaybı veya gerçekleşen olaylar kurum bünyesinde ve doğrudan ilişkili taraflarca (bankalar, il meclisi, düzenleyici kuruluşlar vb) bilinir. - Sözleşme şartlarında veya kanuni düzenlemelerde, bir problem veya uyumsuzluk oluşur.
3	ORTA	- Bilgi güvenliği vakası durumunda hassas bilgi ifşa olmaz. İfşa olan bilgi, kurumu çok az etkiler. Meydana gelen etki telafi edilebilir. - Bilgi'nin kaybı veya gerçekleşen olaylar düzenleyici kuruluş tarafından incelemeye alınır. - Sözleşme şartlarında veya kanuni düzenlemelerde oluşan problem sebebi kriz çıkabilir. Kriz sebebi ile cezai hükümler uygulanmasa bile, kurum nezdinde itibar kaybı yaşanır.
4	YÜKSEK	- Bilgi güvenliği vakası durumunda hassas bilgi ifşa olur. İfşa olan bilgi, kurumu etkiler. - Bilgi'nin kaybı veya gerçekleşen olaylar medyada (yerel, ulusal basın vb.) olumsuz olarak bahsedilir. - Kurumda uygunsuzluk sebebi ile ciddi itibar kaybı yaşanır.
5	ÇOK YÜKSEK	- Bilgi güvenliği vakası durumunda hassas bilgi ifşa olur. İfşa olan kritik bilgi, kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. - Bilgi'nin kaybı veya gerçekleşen olaylar medyada sürekli olarak gündeme getirilir ve vatandaşlar üzerinde kalıcı bir itibar kaybı oluşturur. - Kurum sözleşmelerinde yer alan gizlilik şartlarını yerine getiremediği için, üst yönetim kadrosunda görevden almalar başlar.

Tablo 5. Gizlilik Etki Değerleri

Etki Değeri	Etki Değeri Tanımı	BÜTÜNLÜĞÜN KAYBI
1	ÇOK DÜŞÜK	- Bilgi güvenliği vakası durumunda hasas bilgi kontrolsüz değişmez. Kontrolsüz değişen hassas bilgi, kurumu hiç etkilemez veya etkisi göz ardı edilebilir. - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %1'i şikayetçi olur veya hiç şikayet yaşanmaz. - Kanuni düzenlemelere uyumluluk konusunda kolay giderilebilecek problemler ortaya çıkar.
2	DÜŞÜK	- Bilgi güvenliği vakası durumunda hasas bilgi kontrolsüz değişmez. Kontrolsüz değişen hassas bilgi, kurumu çok az etkiler. - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %5'i şikayetçi olur. - Kanuni düzenlemelere uyumluluk konusunda oluşan problemler sebebi ile kurum uyarı cezası alır.
3	ORTA	- Bilgi güvenliği vakası durumunda hasas bilgi kontrolsüz değişir. Kontrolsüz değişen hassas bilgi, kurumu etkiler, orta vadede etkileri giderilir. - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %10'u şikayetçi olur. - Kanuni düzenlemelere uyumluluk konusunda oluşan problemler sebebi ile ilgili konuda düzenleyici kuruluş tarafından bir inceleme başlatılır.
4	YÜKSEK	- Bilgi güvenliği vakası durumunda hasas bilgi kontrolsüz değişir. Kontrolsüz değişen hassas bilgi, kurumu etkiler, orta vadede etkileri giderilir. - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %20'si şikayetçi olur. - Kanuni düzenlemelere uyumsuzluk yüzünden kurumun idari kadrosuna soruşturma açılır veya idari işlem başlatılır.
5	ÇOK YÜKSEK	- Bilgi güvenliği vakası durumunda hasas bilgi kontrolsüz değişir. Kontrolsüz değişen hassas bilgi, kurumu etkiler. Etkileri giderilemez - Varlığın bütünlüğünün bozulması sebebi ile oluşacak sorunlardan dolayı müşterilerin %20'den fazlası şikayetçi olur. - Kanuni düzenlemelere uyumsuzluk yüzünden yönetim değişikliği yapılır.

Tablo 6. Bütünlük Etki Değerleri

Etki Değeri	Etki Değeri Tanımı	ERİŞİLEBİLİRLİĞİN KAYBI
1	ÇOK DÜŞÜK	- Bilgi güvenliği vakası durumunda hassas bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi, kurumu hiç etkilemez veya etkisi göz ardı edilebilir. - Kurumun operasyonlarında kesinti yaşanmaz veya yaşanan kesinti en fazla yarım saatliktir.
2	DÜŞÜK	- Bilgi güvenliği vakası durumunda hassas bilgiye erişilebilir. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi, kurumu çok az etkiler. - Kurumun operasyonlarında yaşanan kesinti yarım saatin üzerindedir ancak 8 saati geçmez ve etkileri çok yüksek değildir.
3	ORTA	- Bilgi güvenliği vakası durumunda hassas bilgiye erişilemez. Erişilebilirliğine zarar gelen kritiklik seviyesi altındaki bilgi, kurumu etkiler. Etki orta vadede telafi edilebilir. - Kurumun operasyonlarında yaşanan kesinti 8 saat ile 12 saat arasında olur. Kısa vadede itibar kaybı olsa da, kurumun operasyonları devam eder.
4	YÜKSEK	- Bilgi güvenliği vakası durumunda hassas bilgiye erişilemez Erişilebilirliğine zarar gelen bilgi, kurumu etkiler. Etki orta vadede telafi edilebilir. - Kurumun operasyonlarında yaşanan kesinti 12 saat ile 1 gün arasında olur. Kurumun operasyonlarının durmasından dolayı, itibarı negatif etkilenir ve uzun vadede kapatılması zor problem oluşur.
5	ÇOK YÜKSEK	- Bilgi güvenliği vakası durumunda hassas bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi, kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir. - Kurum operasyonları ilgili varlığa ulaşılamadığı için gerçekleştirilemez veya 1 günden uzun bir süre sekteye uğrar.

Tablo 7. Erişilebilirlik Etki Değerleri

Risk etki değeri hesaplamasında gizlilik, erişilebilirlik ve bütünlük perspektifleri için ayrı değerler hesaplanır. Bunlardan en yüksek olanı baskın etki değeri olarak belirlenir. Riskler, riskin etki değeri ve tehdit olasılığı seviyesine bağlıdır. Etki ve olasılıklara değerler atanmasının ardından, nihai risk değerlerine, Risk Değeri=Baskın Etki Değeri*Olasılık hesaplaması ile ulaşılır ve riskin kabul edilmesine, azaltılmasına, kaçınılmasına ya da transfer edilmesine (risk işleme planına) karar verilir. Risk Kabul Kriteri değerlendirilmesi tablo 8' e göre yapılır.

RİSK DEĞERİ		Tehdit Olasılığı				
		1	**2**	**3**	**4**	**5**
Baskın Etki Değeri	**1**	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Tablo 8. Risk Kabul Kriteri

Renk Kodu	Risk Değeri	Risk Aksiyonu
	1 – 9	Kabul edilebilir risk
	10– 16	Risk İşleme Planı Gerektirir
	20– 25	Risk İşleme Planı Gerektirir

Tablo 9. Risk Aksiyonu

Örneğin;

Kuruluş yerleşkelerinden birinde yer alan uçuş operasyonlarını etkileyen kritik bir sunucu için:

Baskın Etki Değeri 5 ve Tehdit Olasılığı 3

Risk değeri, risk değerlendirme matrisinde de belirtildiği gibi 5 x 3= 15 olarak hesaplanır. 15 değeri tablo 9'ta belirtilen aksiyon planlarına göre, orta seviyede bir risk değeri olup, riski iyileştirme amaçlı olarak orta vadede aksiyon almayı gerektirir.

Her bir risk için, Bilgi Güvenliği Yürütme Kurulu riski azaltmaya, transfer etmeye, kaçınmaya veya kabul etmeye karar verir.

7.6.3. Risk Belirleme

Risk değerlendirme süreci BGYS kapsamı içerisindeki bilgiler için gizlilik, bütünlük ve erişilebilirliğin kaybı ile ilgili riskleri belirlemelidir.

Bir risk çeşitli unsurlardan oluşmaktadır. İlk olarak, hangi bilgilerin BGYS kapsamında olduğunu ve bu bilginin oluşumundan yok olmasına kadar nerede ve nasıl işlendiği bilinmesi gerekmektedir. Bu iş için varlık envanterinin oluşturulması iyi bir yoldur. Sivil havacılık kuruluşları için örnek bir varlık envanteri aşağıdaki şekilde oluşturulabilir.

Varlık Ana Kategorisi	Varlık Alt Kategorisi	Varlık Adı	Varlık Statüsü (Aktif mi?)	Varlık Tanımı	Adet	Varlık Türü	Varlık Sahibi (Zorunlu) (kişi veya grup)	Varlık Sahibi Departman	Kullanılan Süreç	Varlığın Bulunduğu Lokasyon
YAZILI_BİLGİLER	Elektronik Kayıtlar	Uçuş Raporları	Aktif	Uçuş ait tüm bilgileri içeren raporlar	1	Fiziksel	Uçuş Müdürlüğü	Uçuş Müdürlüğü	Uçuş Sürecii	Genel Müdürlük
DONANIMLAR	PC'ler	KIOSK Cihazları	Aktif	Check-in işlemleri gerçekleştirilen cihazlar	4	Elektronik	Operasyon Ekibi	Operasyon Müdürlüğü	Uçuş Sürecii	Genel Müdürlük
YAZILIMLAR	İş Yazılımları	Personel Takip	Aktif	Personel Bilgilerin Saklanığı yönetildiği yazılım	1	Elektronik	İnsan Kaynakları	İnsan Kaynakları Müdürlüğü	Personel Yönetim Süreci	Genel Müdürlük

Şekil 4. Varlık Envanteri

Risk belirlemek için risklerin kaynaklarının ve sebeplerinin değerlendirilmesi gerekmektedir. Riskin kaynağı zarar ile oluşabilecek istenmeyen bir olay olabilir. Hava durumu nedeniyle uçuşların aksaması, elektrik kesintisi, sel gibi doğal afetlerin veya saldırganlar tarafından oluşabilecek muhtemel riskler örnek olarak verilebilir. Riskin meydana gelme olasılığı var mı veya meydana gelen riskten kaynaklanacak sonuçlar analiz aşamasının bir parçası mıdır şeklinde sorular sorularak riskler belirlenebilir. Kuruluşlar, tespit edilen her riskin, risk işleme planlarından sorumlu olacak risk sahibini ataması gerekmektedir. Risk sahibi, aksiyon planlamaları dahil tüm risk yönetim süreçlerinden sorumlu olmaktadır.

Havayolu firmalarının karşıya karşıya gelebileceği örnek riskler tablo 11 içerisinde belirtilmiştir.

Tehtid/Konu / İçerik	Risk Tanımı	Muhtmel ilgili birim
Bilgi güvenliği süreciyle İK sürecinin entegre olarak yürütülmemesi	Bilgi güvenliği süreciyle İK sürecinin entegre olarak yürütülmemesi, sözleşmesel eksikliklerden doğabilecek bilgi güvenliği zafiyetlerinin meydana gelmesine ve bu anlamda finansal zarara ve itibar kayıplarına neden olabilir.	İnsan Kaynakları(IK)
İşe alım, işten ayrılma ve transfer süreçlerinde gerçekleştirilecek faaliyetlerin belirli bir standarta veya metoda dayandırılmaması	İşe alım, işten ayrılma ve transfer süreçlerinde gerçekleştirilecek faaliyetlerin belirli bir standarta veya metoda dayandırılmaması, süreçlerin işletiminde sorunların ve/veya eksikliklerin meydana gelmesine ve iş sürekliliği kayıplarına neden olabilir.	IK
Bilgi güvenliğiyle ilişkili farkındalık eğitimlerinin verilmemesi veya farkındalık eğitimlerinin personel tarafından alınmaması, tekrarlanmaması	Bilgi güvenliğiyle ilişkili farkındalık eğitimlerinin verilmemesi, çalışanların dış veya iç kaynaklı bilgi güvenliği tehditlerine (sosyal mühendislik, oltalama vb.) zaafiyet göstermesine ve buna bağlı olarak, itibar, iş sürekliliği ve finansal kayıplara yol açabilir.	Tüm Personel(TUM)

Disiplin sürecinde eksikliklerin ve yetersizliklerin bulunması	Disiplin sürecinde eksikliklerin ve yetersizliklerin bulunması, çalışan kaynaklı tehditlere ilişkin caydırıcılığı azaltabilir ve itibar kayıplarına neden olabilir.	IK
Varlık yönetiminin etkin olmaması	Varlık yönetiminin olmaması mevcut varlıklarının durumlarının bilinmemesine, varlıklara zor erişilmesine ve iş sürekliliğinde aksaklıklara yol açabilir.	TUM
Uygulamalara ilişkin sahipliklerin belirlenmemesi ve sorumluluk atamalarının yapılmaması	Uygulamalara ilişkin (Varlıklara ilişkin demek daha kapsamlı olabilir.) sahipliklerin belirlenmemesi ve sorumluluk atamalarının yapılmaması uygulama bilgilerinin güncelliğinden emin olunamamasına, uygulamalara yönelik sınıflandırmaların yapılamamasına, yetki atamalarının ve yetki alımlarının gerçekleşmesinde eksikliklerin oluşmasına ve finansal kayıplara yol açabilir.	TUM
Varlık yönetiminin gerekliliği olan bilgi sınıflandırmasının yapılmaması	Varlık yönetiminin gerekliliği olan bilgi sınıflandırmasının yapılmaması varlıklara yönelik alınması gereken önlemlerin alınamamasına ve bilginin korunması, saklanması ve sürekliliğinin sağlanması konularında eksikliklerin yaşanmasına neden olabilir.	TUM
Dışarıya gönderilen cihazlar için takip gerçekleştirilmemesi ve herhangi bir takip formu kullanılmaması	Dışarıya gönderilen cihazlar için takip gerçekleştirilmemesi ve herhangi bir takip formu kullanılmaması (ve içinde tuttuğu bilginin cihazdan silinmemesi/silinemiyorsa şifrelenmeden gönderilmiş olmasının tanımlı olduğu sürecin olmaması ya da sürece uyulmaması da değerlendirilebilir), kurum bünyesinde bulunan varlıkların izlenememesine ve finansal zararların oluşmasına ve yasal ihlallere neden olabilir.	TUM
Yetkisiz erişimlerin meydana gelmesine ilişkin sistem zafiyetlerinin bulunması	Yetkisiz erişimlerin meydana gelmesine ilişkin sistem zafiyetlerinin bulunması ve bu zafiyetlerin gözlemlenmesinin yetersiz	TUM

	olması nedeniyle, uygulamaların suistimale açık faaliyetlerde kullanılmasına neden olabilir ve buna bağlı finansal zarar ve itibar kayıpları meydana gelebilir.	
Erişim yetkilerinin verilmesine/alınmasına yönelik tanımlı süreçlerin bulunmaması	Erişim yetkilerinin verilmesine/alınmasına yönelik tanımlı süreçlerin bulunmaması, süreçlerin standart bir şekilde yönetilmemesine ve iş sürekliliği kayıplarına yol açabilir.	TUM
Görevler ayrılığına uygun olarak yetki tahsisinin gerçekleştirilmemesi	Görevler ayrılığına uygun olarak yetki tahsisinin gerçekleştirilmemesi, uygulamalara yetkisiz erişimlerin olmasına, yetkisiz yazılım kurulmasına ve finansal kayıplara ve mevzuatsal eksikliklere neden olabilir.	TUM
Erişim yetkilerinin düzenli olarak gözden geçirilmemesi	Erişim yetkilerinin düzenli olarak gözden geçirilmemesi, verilen ve olması gereken erişim yetkileri arasında uyumsuzlukların zamanında tespit edilememesine ve buna bağlı olarak finansal, itibar ve iş sürekliliği kayıplarına yol açabilir.	TUM
Yönetici yetkilerinin çok sıkı kontrollerle verilmemesi ve ortak yönetici hesaplarının kullanılması	Yönetici yetkilerinin çok sıkı kontrollerle verilmemesi ve ortak yönetici hesaplarının kullanılması ilgili hesapla gerçekleştirilen işlemlerin takibinde sorunların yaşanmasına, mevzuatsal eksikliklere, yetkilerin suistimaline ve bu bağlamda finansal kayıplara yol açabilir.	TUM

Tablo 10. Risk Tanımı

7.6.4. Risk İşleme

Kuruluş risk değerlendirme sonuçlarını değerlendirerek uygun risk işleme seçenekleri seçmek ve seçilen risk işleme seçeneğini uygulamak için gerekli tüm kontrolleri belirlemeli, risk işleme sürecini tanımlamalı ve uygulamalıdır.

7.6.4.1. Risk İşleme Seçenekleri

Genel risk işleme seçeneklerine aşağıdaki gibi örnek verilebilir.

Risk Azaltma:

- Güvenlik kontrolleri kurulması,
- Prosedürlerin geliştirilmesi,
- Ortamın değiştirilmesi,
- Tehditle karşı karşıya kalındığında bu tehdidi saptayabilecek ve sebep olabileceği muhtemel zararı azaltacak erken tespit yöntemlerinin uygulanması,
- Belirli bir tehdit ortaya çıktığında, yeni oluşacak hasarları azaltarak işin devamlılığını sağlayacak bir acil durum planının oluşturulması,
- Tehdidin karşısına engeller konulması,
- Güvenlik farkındalığı eğitimlerinin düzenlenmesi.

Risk Transferi: Bazı risklerin transferi için sigorta yapılması ya da ilgili sorumluluğun sözleşmelerle üçüncü bir tarafa devredilmesi.

Risk Kabulü: Risklerin devam etmesi ancak giderilmesine yönelik herhangi ek bir çalışmanın ya da yatırımın/harcamanın yapılmaması.

Riskten Kaçınma: Riske sebep olan faaliyetin ortadan kaldırılması ya da faaliyete devam edilmemesi.

Risk derecesi belirlendikten sonra, risk işleme planları belirlenir ve buna uygun olarak aksiyon planları hazırlanır.

Örneğin, yukarıdaki örnek için geliştirilen bir risk işleme planı, binanın depreme dayanıklı hale getirilmesiyle ilgili zayıflığının azaltılması olabilir. Kontrolün hayata geçirilmesinden sonra yönetimin zafiyet seviyesini düşürüp tehdidin oluşma ya da etki etme olasılığını indirgemeye karar verdiği varsayıldığında, yeni risk derecesi,

5 x 1= 5, yani kabul edilebilir seviyede olacaktır.

7.6.4.2. Kontroller

Kuruluş seçilen bilgi güvenliği risk işleme seçeneklerinin uygulanması için gereken tüm kontrolleri belirlemelidir.

Bir kuruluşun kullanabileceği kontroller kuruluş tarafından tasarlanabilir veya herhangi bir kaynaktan; örn. yasal düzenleyici gerekli kontroller, müşterinin talep ettiği veya ürüne/hizmete özel kontroller, belirlenebilir. Seçilen kontroller Ek-A standartın referans kontrol amaçlar ve kontroller bölümünde yer alan kontroller listesi ile, gerekli kontrollerin hiç birinin atlanmadığını doğrulamak için karşılaştırılmalıdır.

Standartın Ek A'sı insan kaynakları güvenliğinden sistem alımı, geliştirmesi ve bakımına kadar değişen 14 güvenlik başlığına ayrılmıştır. Her güvenlik başlığı çeşitli güvenlik kategorilerine bölünmüştür. Her biri o kategori için bir amaç içeren, toplamda 35 güvenlik kategorisi mevcuttur.

Örneğin:

Güvenlik Kategorisi: Bilgi Sınıflandırması

Amaç: Bilgilerin kuruluş için önem durumuna bağlı olarak uygun bir koruma seviyesi ile alınmasını sağlamak.

Her güvenlik kategorisi içerisinde, uygulanması durumunda güvenlik kategorisinin amacına ulaşmasını sağlayacak belirli kontroller vardır. Dahil edilen tüm kontroller ve Ek-A'da hariç tutulan kontrolleri için gerekçelendirmeler ile birlikte, seçilen tüm kontrolleri belirleyen bir uygulanabilirlik bildirgesi oluşturulmalıdır. Kuruluşlar uygulanabilirlik bildirgesini aşağıdaki formatta oluşturalabilir.

ISO 27001 İlgili Maddesi	İlgili Alt Madde	Kontrol Detayları	Uygulanabilirlik	Kapsam Dahili Kontroller/Harici Tutma Nedenleri	Doküman Referansı
A.11 Fiziksel ve Çevre Güvenliği	A.11.2.5 Varlıkların taşınması	Teçhizat, bilgi veya yazılım ön yetkilendirme olmaksızın kuruluşun dışına çıkarılmamalıdır,	Evet	Donanım, bilgi veya yazılım; onay alınmadan hiçbir koşulda bina dışına çıkarılmaz	EK.10.85.001 Bilgi Güvenliği Yönetim Sistemi El Kitabı / 5,10,5, Varlıkların Taşınması
A.11 Fiziksel ve Çevre Güvenliği	A.11.2.6 Teçhizat ve kuruluş dışındaki varlıkların güvenliği	Kurum dışındaki varlıklara, kuruluş yerleşkesi dışında çalışmanın farklı riskleri de göz önünde bulundurularak güvenlik uygulanmalıdır.	Evet	Tesis dışına çıkarılan donanım için (dizüstü vs.) maruz kalabileceği riskler düşünülerek gerekli güvenlik önlemleri alınır.	EK.10.85.001 Bilgi Güvenliği Yönetim Sistemi El Kitabı / 5.10.6. Teçhizat Ve Kuruluş Dışındaki Varlıkların Güvenliği
A.11 Fiziksel ve Çevre Güvenliği	A.11.2.7 Teçhizatın güvenli şekilde yok edilmesi veya tekrar kullanılması	Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımından önce tüm hassas verilerin lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla kontrol edilmelidir.	Evet	BT donanım ve ekipmanları onay alındıktan sonra imha edilir. İmhadan önce, donanımların üzerindeki veri ve ortam uygun yöntemlerle silinir. Kullanılmayan donanım ve elektronik ortamların imhası mevcut çevre, yasa ve yönetmeliklerine uygun gerçekleştirilir,	EK.10.85.001 Bilgi Güvenliği Yönetim Sistemi El Kitabı / 5.10.7. Teçhizatların Güvenli Olarak Yok Edilmesi veya Tekrar Kullanımı
A.11 Fiziksel ve Çevre Güvenliği	A.11.2.8 Gözetimsiz kullanıcı teçhizatı	Kullanıcılar, gözetimsiz teçhizatın uygun şekilde korunmasını temin etmelidir.	Evet	Bina dışına çıkarılan donanım ve veri saklama ortamı, kamuya açık alanlarda gözetimsiz bırakılmaz,	EK.10.85.001 Bilgi Güvenliği Yönetim Sistemi El Kitabı / 5,10,8, Gözetimsiz Kullanıcı Techizatı
A.11 Fiziksel ve Çevre Güvenliği	A.11.2.9 Temiz masa temiz ekran politikası	Kağıtlar ve taşınabilir depolama ortamları için temiz masa ve bilgi işleme olanakları için temiz ekran politikası uygulanmalıdır,	Evet	Kullanıcılar masaları başında olmadıklarında hassas bilgi içeren basılı dokümanları masa üstünde bırakmamalıdırlar ve bilgisayar ekranlarını açık terk etmemelidirler. Hassas bilgi içeren basılı dokümanlar kullanılmadıklarında masadan kaldırılır ve gerekiyorsa kilit altında tutulur.	EK.10.85.001 Bilgi Güvenliği Yönetim Sistemi El Kitabı / 5,10,9, Temiz Masa ve Temiz Ekran Politikası PR.88.045 Temiz Masa/Temiz Ekran Prosedürü

Tablo 11. Uygulanabilirlik Bildirgesi

7.6.5. Artık Risk

Kuruluşların belirlenen risklerin işleme planlarının sonrasında ve alınan aksiyonların neticesinde riskin halen devam etme durumudur. Sayıştayın hazırlamış olduğu risk yönetim rehberinde artık şu şekilde ifade edilmiştir; belli bir riski ortadan kaldırmak için gerekli görülen kontrol faaliyetleri uyguladıktan sonra arta kalan risktir. Kuruluşlar artık risklerini risk kabul kriterlerine göre değerlendirerek uygun risk işleme planı uygulamalıdır.

7.6.6. Fırsatların Değerlendirilmesi

Riskin kuruluşa olumlu yansımalarına fırsat adı verilir. Riskler, kuruluşların için bazı fırsatlar getirebilir. Örneğin, kuruluşun müşterileri etkilemesi, yeni ürün ve hizmetler geliştirmesi, atığı azaltması veya verimliliği artırmasına katkı sağlar. Fırsatları belirleme faaliyetleri, ilgili risklerin değerlendirmelerini de kapsayabilir. Risk, belirsizliğin etkisidir ve böyle bir belirsizlik olumlu veya olumsuz etkilere sahip olabilir. Bir riskten kaynaklanan olumlu bir sapma, fırsat oluşturabilir ancak riskin bütün olumlu etkileri fırsat ile sonuçlanmaz.

Riski tamamen ortadan kaldırmak mümkün olmasa da, olumsuz etkilerini azaltmak için bazı fırsatları değerlendirebiliriz. Diğer yandan, zaman zaman faaliyetleriyle ilgili alanlarda kurumun başarısını arttıracak fırsatlar ortaya çıkabilir. Bu tür fırsatların değerlendirilmesine ilişkin kurumun önceden bir stratejiye sahip olması ve bu doğrultuda eylemde bulunması, bu fırsatlardan azami ölçüde faydalanmasını mümkün kılar. (Sayıştay Risk Yönetim Rehberi, 2006)

7.7. Destek

Standartın 7. maddesi BGYS'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli olan desteği içermektedir.

7.7.1. Kaynak

Kuruluşlar BGYS sağlanabilmesi için yeterli kaynağa sahip olup olmadıklarını irdelemektedir. Kaynaklar; insanları, sistemleri , bilgi, birikim, beceri ve finansal unsurları ifade etmektedir.

7.7.2. Yeterlilik

Bilgi güvenliği performansını etkileyebilecek görevler atanmış kişilerin bu görevi yerine getirebilmeleri için uygun yeterliliğe sahip olmaları gerekmektedir. Örneğin, bir BGYS kurulum projesi yönetiliyorsa proje liderinin sadece iyi bir lider olması beklenemez. İyi bir lider olmasının yanında uygun davranış ve becerileri de göstermesi gerekmektedir.

Kuruluşlar görevler için gerekli yeterlilikleri belirlemeli sonrasında bu görevlere atanan kişilerin yeterlilikleri karşılayıp karşılamadıklarını değerlendirmelidir. Eğer kişilerin gereken yeterliliği sağlanamadığı gözlemlenirse bu boşluğu ele almak için periyodik olarak Tablo 6 içerisinde ki gibi yetkinlik boşluk analizi gerçekleştirilerek bir aksiyon planı oluşturulmalıdır. Bu aksiyonlar eğitim, koçluk, mevcut çalışanların yeniden atanması veya yeterli kişilerin işe alınması veya sözleşmeli çalıştırılmasını içerebilir.

Kuruluş, yeterlilik kanıtı olarak uygun dökümante edilmiş bilgileri saklamalıdır.

GEREKLİ VASIFLAR	**0-5 arası puanlayınız. 5 en gerekli ve 0 uygulanamaz olarak değerlendirilecektir.**						Mevcut Planlama
	5	**4**	**3**	**2**	**1**	**0**	
Problem Çözme Analiz							
İletişim							
İşbirlikçilik							
Liderlik							
Çözüm Odaklılık							
sorumluluk							

Tablo 12. Yetkinlik Boşluk Analizi

7.7.3. Farkındalık

Kuruluşun kontrolu altında çalışan herkes, Standartın gerekliliği olarak aşağıdakilerin farkında olamlıdır:

- BGYS politikası
- Bu kişilerin, görev ve sorumlulukları dahil, BGYS etkniliğine katkıları
- BGYS gerekliliklerine uymanın sonuçları

Farkındalık sınıf, e-öğrenme, bültenler, işaretler, duyuru panoları, e-postalar gibi pek çok şekilde olabilir. Ancak farkındalık tek seferlik değildir periyodik olarak çalışanlara bildirilmelidir.

7.7.4. İletişim

Kuruluşlar BGYS ile ilgili hem iç hem de dış taraflarla nasıl iletişim kuracağını belirlemelidir. İnsanların kendilerini etkileyen BGYS boyutlarından haberdar edilmesi önemlidir. Herkesin herşeyden haberdar edilmesi durumunda, bildirimlerin önem değeri azalacak insanlar dikkate almayacaktır. Bu nedenle, ilgili madde kuruluşlardan aşağıdaki konularda iletişim yöntemini belirlemelerini ifade etmektedir.

- Hangi konuda iletişimin yapılacağı,
- İletişimin ne zaman kurulacağı,
- İletişimin kiminle kurulacağı,
- İletişimi kimin kuracağı,
- Hangi süreçlerin iletişimi etkilediği.

İletişimden sorumlu kişiler sorumlu olduklarının farkında olmalı ve kendilerine atanan bu görevleri yapmak için uygun yeterliliğe sahip olmalıdır.

7.7.5. Dökümante Edilmiş Bilgi

Standart dökümante edilmiş bilgi olarak mevcut bulunması gereken unsurları belirtmektedir., örn. bilgi güvenliği politikası, uygulanabilirlik bildirgesi, BGYS'nin tam olarak etkin olabilmesi için gerekli olan kuruluşa uygun bilgiler dökümante edilmelidir.

Standart bazı maddelerde uyumluluk sağlanması ve etkin bir BGYS oluşturulabilmesi için kuruluşun fiziksel veya elektronik formatta döküman oluşturması gerektiğini ifade etmiştir.

Aşağıdaki tablo içerisinde standartın maddelerine göre hazırlanması gereken dökümanlar belirtilmiştir.

ISO 27001 maddesi:	Dökümante Gereklilikler
4.1	-
4.2	-
4.3	Kapsam
4.4.	-
5.1.	-
5.2.	Politika
5.3.	-
6.1.1.	-
6.1.2	Bilgi güvenliği risk değerlendirme süreci
6.1.3	Uygulanabilirlik bildirgesi Bilgi güvenliği risk işleme planı Bilgi güvenliği risk işleme süreci
6.2.	Bilgi güvenliği amaçları
7.1.	-
7.2	Yetkinliğin Kanıtı
7.3	-
7.4	-
7.5.1	Bu uluslararası Standartın gerekliliği olan dökümante bilginin yanısıra, bilgi güvenliği yönetim sisteminin etkinliği için gerkli görülerek kuruluş tarafından belirlenen dökümante bilgiler
7.5.2	-
7.5.3	Kuruluş tarafından gerekli olarak tanımlanan dış kaynaklı dökümante bilgiler
8.1	- Sürecin planlanan şekilde yürütüldüğüne dair güvenceye sahip olmak için gerekli görülen seviyede bilgi.
8.2	Bilgi güvenliği risk değerlendirme sonuçları
8.3	Bilgi güvenliği risk işleme sonuçları
9.1	İzleme ve ölçüm sonuçlarının kanıtları
9.2	- Tetkik programları - Tetkik programlarının yürütüldüğüne ve tetkik sonuçlarına dair kanır
9.3	Yönetim gözden geçirmelerinin sonuçlarının kanıtı olan bilgiler
10.1	Uygunsuzlukların yapısına ve devamında alınan aksiyonlara dair bilgiler ve herhangi bir düzeltici faaliyete ilişkin bilgiler
10.2	-

Tablo 13. Dökümantasyon Gereklilikleri

ISO 27001 Maddesi:	Süreç & Prosedür Gereklilikleri(dökümante edilmesi şart değil)
7.4	İletişim süreci
7.5	Dökümante bilgi kontrolü
8.1	- Bilgi güvenliği gerekliliklerini yerine getirmek için süreçler. - Dış kaynaklı süreçler
9.1	İzleme, ölçme, analiz etme ve değerlendirme için metotlar

Tablo 14. Şart Olmayan Döküman Gereksinimleri

Aşağıdaki dökükamanlar standart tarafından 'gerekli olarak' tanımlanmamıştır. Fakat, bu bilgilerin bir formatta mevcut olması halinde kuruluşun standarta uygunluğunu göstermesi daha kolay olacaktır.

ISO 27001 maddesi:	
5.3	Görevler, sorumluluklar ve yetkiler
7.4	İletişimler

Tablo 15. Faydalı Dökümanlar

Dökümante edilmiş bilgilerin sahip olması gereken bazı özellikleri vardır. Bu özellikler şu şekilde sıralanabilir;

- Uygun tanımlama ve açıklaması olmalıdır (başlık,tarih, yazan kişi, referans numarası, vb)
- Uygunluk ve yeterlilik için gözden geçirilmeli ve onaylanmalıdır.
- Yeterli şekilde bilgi güvenliği unsurlarının ihlalilne karşı korunmuş olmalıdır.
- Kuruluş için uygun yapıda ve ortamda bulunmalıdır.

7.8. İşletim

Standartın 8. Maddesi olan işletim maddesi 6.madde planlama ile yakından bağlantılıdır. Madde 6 içerisinde belirtilen süreçler yapılması gerekenler bu madde içerisinde işletilecektir. Yani standart kuruluşların riskleri ve fırsatları ele alabilmek

için gerekli süreçleri planlamasını, uygulamasını ve kontrol etmesini kuruluşlardan beklemektedir.

Kuruluşların standartın işletme maddesine uyumlu olabilmek için aşağıdaki konularda çalışma yapması gerekmektedir.

- Süreçler için belirli kriterler oluşturmak
- Oluşturulan kriterle uygun gereken kontrolleri sağlamak
- Süreçlerin planlandığı şekilde yapıldığını kanıtlamak ve bu kanıtları dökümante ederek yazılı bilgi olarak muıhafaza etmek
- Planlanan değişiklikleri kontrole etmek ve istenmeyen değişikliklerin sonuçlarını gözden geçirmek
- Dış kaynaklı süreçlerin kontrol edilmesini sağlamak
- Bilgi güvenliği risk işleme planını uygulamalı, ve dökümante etmelidir.

7.9. Performans Değerlendirme

Kuruluşlar standartın bu maddesine uyumluluğu sağlayabilmek için kendi BGYS performanslarını izlemeli , ölçülebilir metotlar ile değerlendirmeli, periyodik olarak tetkikler gerçekleştirmeli ve yönetimin gözden geçirmesini sağlamalıdır.

7.9.1. İzleme,Ölçme, Analiz Ve Değerlendirme

Kuruluşun nelerin izlenmesi ve ölçülmesi gerektiğini bilgi güvenliği süreçleri ve kontrollerini dahil edecek şekilde belirlemesi gerekmektedir. Kuruluş tarafından izleme, ölçme, analiz ve değerlendirme için seçilen yöntemler karşılaştırılabilir ve yeniden oluşturulabilir sonuçlar üretmelidir. Aksi halde, bu yöntemler geçerli kabul edilmeyecektir.

Buna ek olarak, kuruluş aşağıdaki husuları belirlemesi gerekmektedir.

- İzleme ve ölçmenin ne zaman yapılacağı
- İzleme ve ölçmenin kim tarafından yapılacağı
- Sonuçların ne zaman analiz edileceği ve değerlendirileceği
- Sonuçların kim tarafından analiz edileceği ve değerlendirileceği

ISO 27001 Bilgi Güvenliği Yönetim Sistemi KPI Listesi									
KPI #	Standart Başlığı	KPI Açıklama	KPI Amaç	KPI Kontrol Raporu Sunulacak Kurul	Sorumlu Başkanlık/ Başkan Yardımcılığı	Ölçüm Verileri	Ölçüm Verisi Kaynağı	Ölçüm Frekansı	Formülasyon
KPI.1	Politika & Standartlar Çerçevesi	Bilgi güvenliği politikaları ve standartları yılda en az bir kez gözden geçirilmektedir.	Bilgi güvenliği politikalarına ve standartlarına yönelik düzenli aralıklar ile gözden geçirmelerin yapılması	Bilgi Güvenliği Üst Kurulu Bilgi Güvenliği Yürütme Kurulu Denetim Kurulu	BT Strateji ve Yönetişim Başkanlığı	x: Bir yıldan fazla sürede gözden geçirilmeyen politika ve standartlar.	Uyumluluğu Gözden Geçirme toplantı tutanakları	Yıllık	KPI: x = 0
KPI.2	Bilgi Güvenliği Farkındalığı	Bilgi güvenliği farkındalık eğitimlerinin, Kurum bünyesinde bulunan tüm personel için yapılma oranı değerlendirilmektedir.	Bilgi güvenliği farkındalık eğitimlerinin Kurum bünyesinde bulunan tüm personele verilmesi	Bilgi Güvenliği Üst Kurulu Bilgi Güvenliği Yürütme Kurulu Denetim Kurulu	BT Strateji ve Yönetişim Başkanlığı	x: Eğtim alan personel sayısı y: Toplam personel sayısı	Eğitim Başkanlığı raporları	Yıllık	KPI: (x/y) * 100 > 60
KPI.3	İnsan Kaynakları	Tüm personel tarafından, geçici personel de dahil olmak üzere Kabul Edilebilir Kullanım Politikasına da atıf yapılan Personel Gizlilik Politikası imzalanır.	Bilginin bilerek veya bilmeyerek gizliliğin ifşasının ve bilgi güvenliği ihlallerinin azaltılması için caydırıcı önlem alınmalıdır	Bilgi Güvenliği Üst Kurulu Bilgi Güvenliği Yürütme Kurulu Denetim Kurulu	BT Strateji ve Yönetişim Başkanlığı GMY (IK)	x: Gizlilik anlaşması imzalı personel sayısı y: Toplam personel sayısı	İnsan Kaynakları Başkanlığı raporları	Yıllık	KPI: (x/y) * 100 > 99
KPI.4	Varlık Yönetimi - Konfigürasyon ve Yama Yönetimi	Yamalar, belirlenmiş yama gerçekleştirme hedef süresine göre hedeflenmiş tamamlanma yüzdesine uygun olacak şekilde güncellenir.	Sunucular, belirlenmiş zaman çerçevelerinde gerçekleşir.	Bilgi Güvenliği Yürütme Kurulu Denetim Kurulu	Altyapı ve Operasyon Başkanlığı	x: Yama geçilme tarihi 60 günden önce olan sunucu sayısı y: Yama geçilmesi gereken toplam sunucu sayısı	SCCM (windows) Sattelite (linux, unix)	3 Aylık	KPI: (x/y)*100 > 90

Şekil 5. Performans Ölçüm

Yukarda örnek olarak belirtilen performans ölçüm kriterlerine bakıldığına formülasyon seçeneğinde oluşacak sonuçların bir önceki sonuçlar ile karşılaştırılabilir olduğunu gözlemleyebiliriz. Kuruluşların aşağıdaki örneğe benzer bir performans izleme yöntemi oluşturması ve bunları yazılı bilgi olarak dökümante etmesi gerekmektedir.

Ölüçüleblir bir kontrol örneği;

Eğitim başkanlığı raporlarına göre toplam personel sayısı 5000 olan bir havayolu firmamızda 2018 senesinde bilgi güvenliği farkındalığı eğitimi alan kişi sayısı 1000'dir. 2019 senesinde ise personel sayısı 500 artmış ve bilgi güvenliği farkındalığı eğitimi alanların sayısı 4000 e çıkmıştır. Bu durumda BGYS Bilgi güvenliği farkındalığı başlığının performansını şu şekilde ölçebiliriz.

KPI : (x/y) *100 > 60

KPI (2018) : (1000/5000) *100 > 60 ; 20 < 60 sonucu çıkmıştır ve kurumun 2018 senesinde Bilgi Güvenliği farkındalığı performansı istenilen düzeyde olmadığı sonucuna varılmıştır.

KPI (2019) : (4000/5500) *100 > 60 ; 72,72 > 60 sonucu çıkmıştır ve kurum 1 sene içerisinde Bilgi Güvenliği farkındalık eğitimlerini istenilen düzeye çıkarmıştır.

7.9.2. İç Tetkik

Diğer yönetim standartlarında olduğu gibi, iç tetkikler ve yönetimin gözden geçirmesi BGYS'nin performansının gözden geçirilmesi için anahtar yöntemlerdendir. Sürekli iyileştirilmesi için anahtar bir yöntem olmaya devam etmektedir.

Bir kuruluşun kendisi tarafından, sisremlerinin, prosedürlerinin kendisi ve ilgili taraflar için bilgi güvenliği sağlama yeteneklerini sürekli iyileştirip iyileştirmediklerini belirlemek, standarta uygunluklarını değerlendirmek üzere yapılan tetkiklerdir.

BGYS'nin standart gerekliliklerine ve kuruluşun şartlarına uygun olup olmadığı ile ilgili bilgi sağlamak için planlı aralıklarla iç tetkikler yapılmalıdır. Bu nedenle söz konusu süreçlerin önemini dikkate alan bir tetkik programı oluşturulmalı ve BGYS'nin tüm alanlarının tetkik edilmesi sağlanmalıdır. Ancak, kuruluş tarafından önemli kabul edilen uçuş harekat merkezi gibi alanlar daha sık tetkik edilmelidir.

Yani, iç tetkik programı süreçler, fonksiyonlar ve kontrol tetkiklerinin bir karışımını içerebilir. Aşağıda belirtilen örnekte ki gibi bir tetkik programı belirlenebilir.

- Kurumsal bir bölüm veya alan örn. Uçuş Harekat Merkezi
- Bir süreç veya faaliyetler örn. Uçak iniş kalkış süreci, Analiz raporlama
- Fiziki alanlara ve cihazlara yetkisiz erişime karşı koruma

Tetkik programı tetkik sıklığını, tektkik için kullanılacak yöntemleri, planlama ve raporlama gerekliliklerini de içermelidir. İç tetkikler yapılırken ISO 27001 EK-A kontrol maddelerinden faydalanılarak soru setleri hazırlanabilir. Yukarda belirtilen örnekteki gibi bir erişim kontrolu özelinde iç tetkik yapılmak istenirse EK-A9 Erişim kontrolü maddesi kullanılabilir. Tablo 8'deki gibi sorular üzerinden iç tetkik yapılabilir.

A.5	BG Politikaları	Kontrol	Sorular	Evet	Hayır	Kısmen	Not
A.9	Erişim Kontrolü						
A.9.1	Erişim kontrolünün iş gereklilikleri						
A.9.1.1	Erişim kontrol politikası	Kontrol: Bir erişim kontrol politikası, iş ve bilgigüvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.	Dokümante edilmiş erişim kontrol politikası mevcut mu?				
			Politika iş gereksinimlerine göre mi oluşturulmuş?				
			Politika uygun şekilde duyurulmuş mu ve ulaşılabilir mi?				
A.9.1.2	Ağlara ve ağ hizmetlerine erişim	Kontrol: Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir	Sadece yetkili kullanıcıların, görevlerini yerine getirebilmeleri için ağ ve ağ kaynaklarına erişimini sağlayan bir kontrol var mı?				
A.9.2	Kullanıcı erişim yönetimi						
A.9.2.1	Kullanıcı kaydetme ve kayıt silme	Kontrol: Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanmalıdır.	Resmi bir kullanıcı kaydı oluşturma ve silme süreci mevcut mu?				
A.9.2.2	Kullanıcı erişimine izin verme	Kontrol: Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.	Tüm kullanıcı tipleri ve servisleri için kullanıcı erişimine izin verilmesi için resmi bir süreç var mı?				
A.9.2.3	Ayrıcalıklı erişim haklarının yönetimi	Kontrol: Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.	Ayrıcalıklı erişim hesapları ayrı olarak yönetilip, kısıtlanıp kontrol ediliyor mu?				
A.9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgileirnin y	Kontrol: Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.	Gizli doğrulama bilgisinin tahsis edilmesi, resmi b,r yönetim yoluyla kontrol ediliyor mu?				
A.9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi	Kontrol: Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.	Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçiriyor mu?				
A.9.2.6	Erişim haklarının kaldırılması veya dzenlenmesi	Kontrol: Tüm çalışanların ve dış taraf kullanıcıların bilgi ve bilgi işleme tesislerine erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir.	Tüm çalışanlar ve dış taraf kullanıcıların erişim yetkileri istihdamları, sözleşmeleri, veya anlaşmaları sona erdiğinde kaldırılıyor yada değişiklik olduğu zaman yetkilendirme tekrar düzenleniyor mu?				
A.9.3	Kullanıcı sorumlulukları						
A.9.3.1	Gizli kimlik doğrulama bilgisinin kullanımı	Kontrol: Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.	Gizli doğrulama bilgilerinin nasıl korunması gerektiğini kapsayan bir prosedür/politika mevcut mu?				
			Tüm kullanıcılara duyurulmuş, iletilmiş mi? Erişilebilir mi?				
A.9.4	Sistem ve uygulama erişim kontrolü						
A.9.4.1	Bilgiye erişimin kısıtlanması	Kontrol: Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.	Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası yada prosedürü ile kısıtlanmış mı?				
A.9.4.2	Güvenli oturum açma prosedürleri	Kontrol: Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.	Erişim kontrol prosedürünün şart koştuğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol ediliyor mu?				
A.9.4.3	Parola yönetim sistemi	Kontrol: Parola Yönetim sistemleri etkileşimli olmalı ve kaliteli parolalar temin edilmelidir.	Parola yönetim sistemleri etkileşimli mi?				
			Kompleks parola kullanılması zorunlu tutulmuş mu?				
A.9.4.4	Ayrıcalıklı destek programlarının kullanımı	Kontrol: Sistem ve uygulamaların kontrolleri geçersiz kılma yeteneğine sahip olabilen destek programlarının kullanımı kısıtlanmalı ve sıkı bir şekilde kontrol edilmelidir.	Ayrıcalıklı destek programları kısıtlanmış mi ve izleniyor mu?				
A.9.4.5	Program kaynak koduna erişim kontrolü	Kontrol: Program kaynak koduna erişim kısıtlanmalıdır.	Yazılım / Program kaynak koduna erişim kısıtlanmış mı?				

Şekil 6. İç Tetkik Soru Listesi

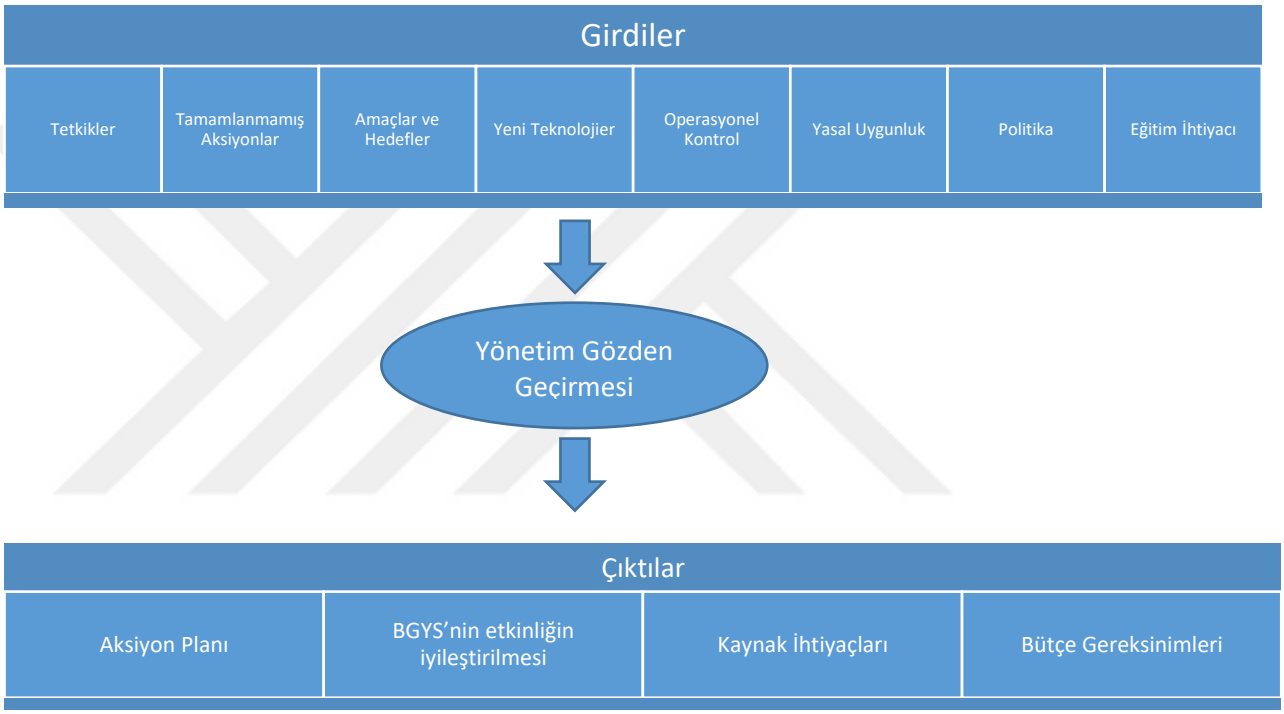
7.9.3. Yönetim Gözden Geçirmesi

Yönetimin BGYS'nin etkin olup olmadığını belirlemek açısından periyodik olarak gözden geçirmesi önemlidir. Kısaca, yönetimin gözden geçirmesi işin ne olacağını söylediğiyle(politika, amaçlar, süreçler vb) gerçekte ne olduğu arasındaki boşluk analizi olarak görülebilir. Yönetimin gözden geçirmeleri planlı aralıklarla yapılmalıdır. Kuruluşunuz halihazırda yönetim gözden geçirmesi yapıyor ise Bilgi Güvenliği'nin, ayrı bir toplantı olarak planlanmasındansa bir gündem maddesi olarak eklenebilir.

Kuruluşlar kapsam içerisindeki tüm iş alanlarını temsil eden yetkili kişiler ile BGYS'nin unsurlarını gözden geçirmek ve görüşmek için düzenli operasyonel

toplantılar yapmayı tercih edebilir. Bu, kuruluşun yönetim gözden geçirmesini daha az sıklıkla yapmasını sağlayabilir. Özellikle, BGYS yeni oluşturan kuruluşlar önemli ölçüde bazı kararlar alması gerektiğinden yönetim gözden geçirme toplantıları daha sık yapılmalıdır.

Bir yönetim gözden geçirmesi yapmanız, iş ile ilgili hangi konuların önemli olduğunu bilmenizi sağlayacaktır. Bunu bilmediğiniz takdirde, yüksek riskli faaliyetlere odaklanmak yerine daha düşük riskli faaliyetler için boşa zaman, çaba ve para harcayabilirsiniz.



Şekil 7. Yönetim Gözden Geçirmesi

7.10. İyileştirme

7.10.1. Uygunsuzluk Ve Düzeltici Faaliyet

Bir uygunsuzluk, yani bir gerekliliğin yerine getirilememesi, ortaya çıktığında kuruluşun bunları belirlemesi ve bunlara yanıt vermesi için süreçleri olması gerekmektedir. Kuruluşların uygunsuzlukların doğru kişilere zamanında raporlanması ve böylece uygun aksiyonların alınabilmesini sağlamak için bir olay ve/veya vaka raporlama süreci uygulamalıdır. BGYS uygunsuzlukları ele alınmalı, ve düzeltici faaliyetler ile birlikte tekrarlamaları önlenmelidir.

Bir uygunsuzluğun neden meydana geldiğini belirlemek kuruluş için önem arz etmektedir. Uygunsuzluğun kök sebebi araştırılırken kuruluş yalnızca semptomu çözmek yerine birşeyin neden olduğunu araştırmaya devam etmelidir. Kuruluş kök sebebi belirledikten sonra benzer uygunsuzlukların var olup olmadığını veya ortaya çıkma olasılığı olup olmadığını belirlemelidir.

Bir uygunsuzluğun neden olduğu bilindikten sonra, kuruluş düzeltici faaliyetin ne olacağını belirleyebilir. Tek bir uygunsuzluğu çözmek için çoğu zaman birden fazla düzeltici faaliyet gerekebilir. Düzeltici faaliyetler, etkinliklerinden emin olmak için gözden geçirilmelidir.

Uygunsuzluk ve düzeltici faaliyetlerin kanıtı olarak bilgiler dökümante edilmelidir.

7.10.2. Sürekli İyileştirme

BGYS'nin uygunluğu, BGYS'nin etkinliği ve BGYS'nin doğruluğu için kuruluşular sürekli iyileştirme süreci işletmelidir. Bu süreç aşağıdaki belirlenebilir bir dizi faaliyetleri içerebilir.

- BGYS'yi iyileştirmek için fırsatların bulunması
- Olası çözümlerin belirlenmesi
- Çözümlerin uygulanması
- Alınan aksiyonların etkinliğinin ölçülmesi
- Gerektiğinde düzeltici faaliyetlerin yapılması
- Değişikliklerin dökümante edilmesi ve bilmesi gerekenlerin bildiğinden emin olunması

7.11. ISO/IEC 27001 Standartı Ek-A Referans Kontrol Amaçları ve Kontroller

Standartın 6.1.3 maddesinde yer alan bilgi güvenliği risk işleme planının uygulanması, uygun risk işleme seçeneklerinin seçilmesi ve gerekli hiçbir kontrolün gözden kaçmaması için bir çizelge hazırlanmştır. Bu çizelge içerisinde kurumların dikkat etmesi gereken tüm başlıklara yer verilmiştir. Standarta uyumlu olabilmek için risk işleme planında Ek-A referans kontrol maddelerine kesinlikle yer verilmelidir.

Ek A geniş kapsamlı bir kontrol amaçları ve kontroller listesi içermektedir. ISO/IEC 27002:2013 içerisinde yer alan bilgi güvenliği kontrol ve teknikler madde 5'ten

madde 18'e kadar çıkarılmış ve sıraya konulmuştur. EK-A kontrol maddelerinin başlıklarına aşağıda yer verilmiştir.

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

Tablo 16. EK-A Referans Kontrol Maddeleri

8. IEC/ISO 27001 STANDARTININ TÜRK HAVA YOLLARINDA UYGULANMASINA YÖNELİK MÜLAKAT ÇALIŞMASI

Merhaba hoş geldiniz, öncelikle biraz kendinizden bahsedebilir misiniz?

Ben Didar Aysev Kayadeniz 1999'dan beri Türk Hava Yolları'nda çalışıyorum. Marmara Üniversitesi Elektronik Haberleşme bölümünden mezunum, daha sonra Bilgi Üniversitesi'nde MIS üzerine yüksek lisans yaptım. 2003-2005 yılları arasında UCLA' da proje yönetimi, network güvenlik gibi konularda exalşın yaptım. Böylece 2 yıl Amerika deneyimim olmuş oldu. Aynı zamanda orada full time öğrenci olduğunuzda çalışma alternatifiniz de oluyor, 1 yıl kadar da çalışma deneyimim oldu. O dönem ücretsiz izin almıştım, Türk Hava Yolları'na ilk girdiğimde part time olarak başlamıştım, şuan Bilgi Güvenliği Müdürlüğündeyim ancak Bilgi Teknolojileri altında çeşitli müdürlüklerde görev yaptım. Son kullanıcı hizmetleri müdürlüğünden Bilgi Güvenliği Müdürlüğüne kadar portföy yönetimine deyinen IT tabanlı birçok konuda uzmanlık alanlarım var. 2006 yılından itibaren de Bilgi Güvenliği Müdürlüğünde aktif olarak çalışıyorum. Daha çok görlscompayrs süreçleri içerisinde dâhil oldum. Özellikle ISO 27001 Bilgi Güvenliği yönetimi sisteminin kurulmasından ve şuanki yaşatılma sürecinden sorumluyum. Aynı zamanda diğer uymakla yükümlü olduğumuz

regülasyonlar PCI DSS gibi standartların da aynı şekilde uyum sürecinden sorumluyum.

Peki, biriminizin 27001'in kurulmasından ve yönetiminden sorumlu olduğundan bahsetmiştiniz, bize biraz bilgi güvenliği yönetimi sisteminin kurulmasından ve bu belgenin alınmasına nasıl karar verildiği konusunda bilgi verebilir misiniz?

Kurumumuzda aslında biz 2010 yılından beri bilgi güvenliği yönetimi sistemi üzerinde çalışmalar yapıyorduk. Benim dâhil olduğum ve dahil olmadığım bizden önceki süreçte müdürlüğümüz içerisinde çalışma arkadaşlarımızla farklı çalışma gruplarımız var. 2010 yılından beri istenilen bir şeydi. Türk Hava Yolları büyük bir organizasyon. ISO 27001 de ISO adı altında olduğu için belki de bu işin challengelarından bir kısmı. Projenin sahipliği söz konusu oldu. Orada birimler arasında bir uzlaşma gerektiği için bir süre proje askıya alındı. Aslında biz 2010 yılından beri IT birimi olarak ISO 27001 sertifikasını almak istiyoruz. Bu bizim hem bilgi güvenliği kurallarımızın politikalarımızın dünya standartlarında dünyanın kabul gördüğü çerçeveleri bir referans alıp o doğrultuda ilerleyerek kuracağımız süreçleri daha somut referanslara dayandırmak istiyorduk. Daha sonra biz bu çalışmalarımıza devam ederken, tabi bu süre içerisinde organizasyonlar oluyor kurum içerisinde, yer değişebiliyor. 2015 yılında tekrar çalışmalara başladık. Fakat o sırada zaten Sivil Havacılık Genel Müdürlüğünün yayınladığı bir genelgeyle 2016-2017 sonuna kadar Sivil Havacılık kurumlarının ISO 27001 belgesini alması zorunlu kılındı. Bu bizim için çok güzel bir fırsattı. Dolayısıyla 27001 projesine öncelik verilebilecek, yönetimimizin desteği zaten her zaman vardı. Fakat diğer önceliklerin arasına 27001 de eklenebileceği için bizim için çok güzel bir fırsat oldu. Bunun akabinde aynı zamanda Gümrük Bakanlığının gümrük işlemlerinin daha kolay yapılabilmesi için yetkili yükümlü statüsü var. Kargo başkanlığımız, kargo genel müdür yardımcılığımız bünyesinde de gümrük işlemlerini kendimiz yapabilmemiz için uçak aksamları ya da kuruma ait teçhizatların yurt dışındaki ofislerimize daha hızlı, daha rahat gönderilebilmesi için kendi bünyemizde bir takım öncelik, ayrıcalık statüsüne sahip olmamız gerekiyordu. Bizim için ticari kazanç sağlayacak artı operasyon olarak çeviklik sağlayacak bir durum. Fakat bunun yaklaşık yanlış hatırlamıyor isem 135 tane gereksinimi var, bunlardan bir tanesi de ISO 27001 belgesinin alınmasıydı. Dolayısıyla elimiz bir kere daha güçlenmiş oldu. Özellikle bilgi sistemleri kapsamında her iki gereksinim de bilgi sistemlerinin yoğun süreçlerinin ve havacılık ile ilgili tüm uçuş ve uçuşa yardımcı sistemlerin ISO 27001 konusunda uyumlu olması gerekiyordu. Bizim en büyük

motivasyonlarımız aslında Sivil Havacılık'ın genelgesi ve Gümrük Bakanlığının yetkili yükümlü statüsü oldu.

Ama bu demek oluyor ki Türk Hava Yolları, Sivil Havacılık Genel Müdürlüğü genelge yayınlamadan önce de bunu istiyordu ve bunun için çalışmalar yapıyordu.

Zaten bu bizim yol haritamızda vardı, evet. Önceliğimiz olsun istiyorduk, bu arada uyumluluk çalışmalarımız zaten devam ediyordu ve belgelendirilmemiş olsa bile o dönemde belgelendirme için süreç başlatılmamış olsa bile biz zaten 27001'e uyumlu bir süreç daha doğrusu bilgi güvenliği süreçlerimizi 27001 olsun ya da diğer çerçeveler diğer prame and nist gibi frameler olsun PCI IDSS olsun bu tarz dünyaca kabul görmüş standartları uyguluyoruz.

Bilgi güvenliği yönetim sistemi kurmadan önce 27001 sertifikası da dâhil olmak üzere, buradaki kapsamı nasıl belirlediniz yani hangi kriterlerle? Az önce mesela Turkish Kargo'nun Gümrük Bakanlığı'ndan dolayı bu kapsam içerisine girdiğini söylemiştiniz.

Şimdi biliyorsunuz Türk Hava Yolları çok büyük bir organizasyon. Ki bu organizasyondan yine diğer sorularınızda bahsediyor olacağım. Ama bizim amacımız her şeyden önce IT departmanını hiçbir şekilde dışarda bırakmayacak bir kapsam belirlemek. Zaten kapsamı Sivil Havacılık Genel Müdürlüğü ve Gümrük Bakanlığı belirlediği için biz ilk önce mevzuata uygun kapsama göre hareket ettik. Zaten o kapsama da baktığımızda IT ile ilgili hiçbir konu dışarıda kalmıyor. İnsan kaynakları süreci zaten işin doğasında olduğu için insan kaynakları süreçlerimiz İnsan kaynakları genel müdür yardımcılığındaki personel yönetim ve istihdam başkanlığımız otomatik olarak bu sürece dâhil oluyor. Artık kargo genel müdür yardımcılığı kapsamıda tamamıyla bizim belgelendirme için kullandığımız kapsama dahil oldu.

Yani bu kapsamı Sivil Havacılık Genel Müdürlüğü belirledi aslında ?

Evet, Sivil Havacılık Genel Müdürlüğü'nün kapsamı bütün IT'yi kapsıyor aslına bakarsanız. Ek olarak da Kargo genel müdür yardımcılığının gümrük süreçleri ile ilgili belirlemiş olduğu kapsam da var artı kişisel verilerin işlendiği sistemler.

2010 senesinde zaten bilgi güvenliği yönetim sisteminin kurulması için ilk adımlar atılmıştı Türk Hava yollarında peki neden bilgi güvenliği yönetim sisteminin

kurulması için çalışmalar başladı? Yani neden önemli Türk Hava yolları için bilgi güvenliği yönetim sistemi?

Biz her şeyden önce sektörde başta Türkiye'de olmak üzere dünyada da öncü bir havayolu olmak istiyoruz. Türkiye'de zaten öncü havayolu şirketi olduğumuz zaten aşikâr. Dünyada da rakiplerimiz gene belli sıralamaya girmiş firmalar ve bilgi güvenliği konusunda da hem örnek olmak istedik özellikle Türkiye'de ki diğer firmalara, artı olgunluk seviyesini belirli bir noktaya çekmemiz gerekiyor, farklılık yaratmamız gerekiyor. O dönemlerde 2009-2010 yıllarında çok fazla bilgi güvenliği farkındalığı aslında bütün kurumlarda yoktu. Yeni yeni ortaya çıkan bir kavramdı. Bunların tüm paydaşları, adları ne olursa olsun gerçekten büyük bir efor gerektiriyordu. Biz biraz da hem bu ihtiyacı görerek, bilgi güvenliğinin sürekliliğinin, sürdürülebilirliğinin sağlanması için ISO 27001 ile bunu perçinlemek istedik.

ISO 27001 projesinde kaç kişilik bir proje ekibi oluşturdunuz ve bu kişileri hangi kriterlere göre belirlediniz?

Proje ekibi belirlenirken ben de proje ekibinin içindeydim. Ekip sayısı gene organizasyon yapısına bağlı, danışmanlık alıp almamanıza göre değişecektir. Bizim şuan kapsamımızda üç genel müdür yardımcılığı vardı. Bunları Kargo, İK ve IT olarak düşünebilirsiniz. Yaklaşık 5-6 kişilik bir proje ekibi vardı. Özellikle tabi ki bu proje ekibinden beklentiler bilgi güvenliği konusunda bilgi sahibi, mümkünse ISO 27001 konusunda eğitim almış, farkındalığı olan bir ekip. Aynı zamanda iş birimleriyle iletişim kurabilecek analitik düşünme yeteneğine sahip, hem IT tarafıyla hem iş süreçleri arasında yani birazda analist rolü gibi düşünebilirsiniz çünkü sadece IT yok, aslında bilgi güvenliği yönetim sistemi çok teknik değil baktığınız zaman, sonuçta bir yönetim sistemi. Bunu iş birimlerine de aktarabilecek, buradaki iş birimlerinin de karşılığının ne olduğunu aktarabilecek, iletişim kurma becerisine sahip kişiler olması gerekiyor. IT kökenli olması bence projeye bir katma değer sağlayacaktır. IT kökenli dedik ama bu nereye bir 27001 sertifikası alacağınıza göre değişiyor. Ben biraz IT kökenli olduğum için burada yanlış bir ifade kullanmış olabilirim, 27001 sertifikasını sadece bir IT organizasyonuna ya da IT bölümüne değil, aynı zamanda biliyorsunuz bilgi işleyen her kuruma alabilirsiniz. Tekstil acentesine alabilirsiniz, bir süpermarkete alabilirsiniz, bir mağazaya alabilirsiniz, eğitim kurumuna alabilirsiniz. Bunların hiçbiri ne yazılım geliştirme yapar baktığınız zaman ya da iş süreçleriyle ilgili bir veri merkezi işletir ya da yazılım donanım süreçleriyle ilgilenir. Baktığınız zaman bizim IT dünyasında yorumladığımız sistemleri kullanmıyorlar ancak bilgiyi işliyorlar. Yani

belki dijital dünyada çok fazla kayıtları yok ya da dijital dünyada çok fazla iş yapmıyorlar ama baktığınız zaman ellerinde mutlaka bir bilgi var, müşteri verileri var, faturaları var. Dolayısıyla buradaki IT proje ekibindeki kişinin illa da IT kökenli olması gerekmiyor ama sürece hâkim birinin olması işte 27001'in ne anlama geldiğini bilmesi tabiiki fayda sağlayacaktır.

Hem IT hem de bilgi güvenliği açısından yetkinliği olan kişiler fayda sağlıyorlar yani. Evet.

Peki bu proje ekibindeki kişiler bilgi güvenliği yönetimi yani ISO 27001 konusunda eğitim aldılar mı? Yani hem ekip üyeleri hem de kapsam içerisine giren müdürlükteki çalışanlar.

Bu konuda Türk Hava Yolları hakikaten üst yönetimimizin liderliği çok ön planda ve bu proje için hem öncelik gösterdi üst yönetimimiz hem kaynak sağladı hem de eğitime çok önem verirler zaten destek sağlarlar. Bu proje kapsamında da proje ekibine bütün ISO 27001 eğitimleri olmak üzere aldırıldı artı proje ekibindeki tüm arkadaşlara lead auditor baş tetkikçi eğitimi aldırıldı sertifikalı olarak proje ekibi middle term sertifikasına da sahip oldu aynı zamanda. Bu sadece proje ekibiyle kalmadı, burası daha önce bahsettiğim gibi çok büyük bir organizasyon. Üç genel müdür yardımcılığının altında altmış tane müdürlük var, her birimden ISO 27001 projesi boyunca projeye destek olması için anahtar kullanıcılar seçildi. Bunlar birazcık bizim proje paydaşları, paydaş birimlerdeki kendi iş süreçlerini bilen, aynı zamanda ISO 27001 gereksinimlerini kendi iş süreçlerinde uygulayabilecek kişiler istendi. Ve bu kişilerin hepsine ISO 27001 uygulama eğitimi ve aynı zamanda gerek ISO 27001 gerekse bilgi güvenliği farkındalığı eğitimi atandı. Ve hepsinin eğitimini sağlamış olduk. Bu altmış kişinin hepsi aslında ISO 27001 konusunda aslında farkındalığı yüksek kişiler oldu. Proje ekibinin altında aslında alt çalışma grupları olarak düşünebiliriz.

Peki Türk Hava Yolları gerçekten büyük bir organizasyon 60 müdürlük 3 genel müdür yardımcılığı, burada özellikle 27001 standartlarına uyumluluk çalışmalarında dikkat edilmesi gereken hususlar sizce nelerdir? Çünkü sivil havacılık kuruluşu olarak büyük bir yapı, özellikle zorlandığınız konular oldu mu?

Bir kere bütün kurumlar için muhtemelen geçerlidir, en önemli şey yönetimin desteği. Yönetim bu süreçte ne kadar fazla destek olursa proje çıktısı o kadar başarılı olacaktır. Aynı zamanda kaynak ayrılması. Onun haricinde proje süresi boyunca dikkat edilmesi

gereken konular, bazı durumlarda şablon dökümantasyonlar kullanılıyor. Bazı firmalar mesela danışmanlık alıyor, siz bir dökümantasyon veriyor ve sadece isminizi değiştirin diyerek o dokümantasyonlarla denetimlere katılıyorlar. Burada amaç belgeyi almak oluyor. Yani önce amacın ne olduğunu belirlemek önemli. Aslında biz hiçbir zaman ISO 27001 belgesini amaç olarak görmedik. Bizim için her zaman araç oldu. Bilgi güvenliği politikalarımızı iyileştirebilmemiz için sürdürülebilir kılmamız için, ISO 27001 belgesini almak bizim için bir araçtı. Bu bakış açısıyla yaklaşılması özellikle uzun vadede kazanç sağlayacaktır. Risk metodolojisi tabi en önemli konulardan bir tanesi. Çünkü risk bakış açısıyla yaklaşıyorsunuz. Risk aslında günlük hayatımızda da yönettiğimiz bir şey. Arabamızı kaskolatmak da bir risk yönetimi. Fakat tam olarak risk yönetimi yapıyoruz diyemiyoruz yaptığımız halde, yani yeni bir kavram diyebiliriz. Gerek kurumsal şirketler, gerek orta ölçekli firmalar. Aslında risk yönetimi hayatımızın her köşesinde bununla ilgili belki yöneticilere yönelik özellikle risk yönetimi nedir, risk yönetiminin faydaları nedir aslında bunları anlatan küçük bir sunum eğitim bile olabilir. Yöneticileri de masaya davet etmek uzun vadede gene fayda sağlayacaktır. 27001 ailesinin kılavuzları var yönetim sisteminin kurulmasına yönelik, risk analizinde tehditler olan 27005 var, yine risk analizini anlatan ISO'nun 30001 di yanlış hatırlamıyorsam. Bunlardan faydalanılabilir ve mümkün olduğu kadar başlarken tabi kurumun ölçeğine göre değişir eğer daha önceden bir risk metodolojisi uygulanmıyorsa yeni bir şeyse, kültürde bir değişiklik olacaksa bence en basitinden başlayarak ilerlemek çok daha faydalı olacaktır. Zaten denetim belgelendirme yapıldıktan sonra 2 yıl boyunca ara denetimler oluyor. Belgeniz 3 senelik, 2. Ara denetim, 3. Ara denetim sonra 3. Yılda tekrar belge yenileme dönemine giriyorsunuz. Genellikle o 3. Belge yenileme dönemine kadar da bir olgunluk süreci diyebilirsiniz. Belgeyi aldığınızda aslında emekleme dönemindesiniz sonra yürüme ve koşmaya başlıyorsunuz. Bekleme dönemine ne kadar kompleks bir metodoloji ile yaklaşırsanız katılımcıları da o kadar uzak tutacaksınız. Yani genelde yaşadığımız tecrübelere istinaden benim öngörüm o oldu. İlk başta yalın tutmak, risk bakış açısını sahiplendirmek daha sonra belki ileriye yönelik risk metodolojisi olgunlaştırılabilir.

Peki, yönetimin desteğinden bahsettiniz. Türk Hava Yolları yönetimi bilgi güvenliği yönetim sistemi kurulması fikrini nasıl değerlendirdi ve bu projeye nasıl destek verdiler? Tüm eğitimler bir maliyet, bütçe sonuçta.

Genel Müdürümüz tarafından takip edilen bir projeydi. Re-organizasyon öncesi ve sonrası ikisi için de geçerli 2 genel müdür yardımcımız, biz Temel Bey zamanında

projeye başladık ve o zaman Bilal Bey Sivil Havacılık Genel müdürü idi. Bilal Bey'in zamanında yayınlanan bir genelgeydi ve Türk Hava Yolları'na atanmasının ardından geldiğinde sorduğu projelerden bir tanesi ISO 27001 oldu. Dolayısıyla yönetimin desteği çok fazla ve bizler bu konuda oldukça şanslıyız. Danışmanlık hizmeti satın aldık, ilk başta yönetim sisteminin kurulması için, eğitimler için kaynak ayrıldı. İş birimlerine dâhil olan 60 kişilik bir ekibe eğitimler verildi. Artı proje ekibine zaten sertifikasyon eğitimleri verildi. Onun haricinde şuanda hala mesela 2. Ara denetimimizi atlattık, bir sonraki dönem belgelendirme denetimi olacak. Denetimimizi başarıyla tamamladık, hiçbir uygunsuzluğumuzda tespit edilmedi. Hatta denetçimizin yorumu da zamanla olumlu tespitler olumsuz tespitlerden daha fazla olmaya başlar, sizde de bu sene öyle oldu dedi. Bu bizim için çok gurur verici ama tabi iyileştirmeye hala devam edeceğiz. Zaten iyileştirme de standartın bir maddesi. Aynı zamanda risk yönetimine yönelik mesela şuan bir araç da bakıyoruz. Bu konuyu da aynı zamanda yönetimimiz bizleri destekliyor. Hem risk konusunda hem bilgi güvenliği yönetimi konusunda yönetimimiz bizi destekliyor.

Bir Sivil Havacılık kuruluşu olarak başka bir Sivil Havacılık kuruluşuna 27001 standartlarına uyum aşamasında herhangi bir danışmanlık firması ile çalışmasını önerebilir misiniz? Siz yaşadığınız tecrübeleri göz önünde bulundurarak.

Bu biraz kurumdaki know- How a bağlı aslında. Danışmanlık tabiiki önemli belli bir bilgi birikimi varsa ve kapsam çok geniş değilse belki danışmanlık alınmadan da ilerlenebilir. Ama sıfırdan başlanılacaksa bir yönlendirme ve bilgiye ihtiyaç varsa tabiki danışmanlık alınmasında fayda olacaktır. Bu biraz kurumun o anki bilgi birikimine ve kapsamına göre değişebilir aslında. Bu konu biraz kurumlara bağlı diyebiliriz aslında.

Siz çalışıyor musunuz bir danışmanlık firması ile şuanda?

Hayır, şuan çalışmıyoruz. Daha önce çalıştık ama biz danışmanlık firmalarının bilgi birikimi konusunda tecrübeli oluyorlar, yönlendirici oluyorlar ama sizin kendi kurumunuzu bilmedikleri için ister istemez bir yerden sonra tıkanıyor. Kitabi kalabilir bazı şeyler teorik kalabilir. Bu demek değildir ki alınmaması gerekir tabiiki sonsuz faydası var çünkü ekip aynı zamanda onlardan da besleniyor. Aslında karşılıklı bir beslenme söz konusu. Bir de mesela ISO 27001 kapsamına bakacak olursak yönetim sisteminin kurulması konusunda faydalı olabilir. Ama anlaşmanıza ve sözleşmenize bağlı olarak değişebilir bu söyleyeceğim. Bunun kurumlara, birimlere uygulanması,

yaygınlaştırılması, projenin implamantasyonu konusunda yine aslına bakarsanız danışmanlık alınsa bile iş eforu daha çok kuruma kalıyor.

Türk Hava Yolları ISO 27001 çalışmalarında diğer havacılık kurumlarından herhangi bir öneri herhangi bir yönlendirme ihtiyacı hissettiniz mi? Görüş alma vs.

Diğer projelerde oluyor. Havacılık sektörü olmasa da biz biraz IT tarafından sorumlu olduğumuz için IT ile ilgili bir proje olduğunda X bir firmaya bir ürünü kullanıyorlarsa onların yorum ve görüşlerini almak için ziyaretler yapabiliyoruz. Ancak 27001 kapsamında böyle bir ziyaretimiz olmadı. Aslında zaten THY öncülük yapıyor.

Diğer kurumlardan böyle bir ziyaret oldu mu THY'ye?

Hayır, olmadı.

ISO 27001 çalışmalarında çok fazla dökümantasyon ortaya çıkıyor ve onun haricinde risk analizi çalışması vs yapılırken bu çalışmaları nasıl yürüttünüz bu çalışmaları yaparken herhangi bir uygulama , araç kullandınız mı? İhtiyaç duydunuz mu?

Dökümantasyon ISO 27001' de evet zorunlu dökümanlar var. Eğer kurumunuzda olgun bir dökümantasyon yönetiminiz varsa ISO 9001 gibi bu sizin elinizi oldukça güçlendirecektir. Çünkü ISO 9001'den besleneceğiniz dökümanlar da var. Bilgi yönetim sistemlerinin yönetim sistemi tarafı genellikle hep aynı. Kapsam belirleme, kaynak belirleme, politikalar, 27001'in yönetim sistemi kampsamındaki farkı risk analizi ve varlık envanteridir. Onun haricinde hedefler, yönetim sisteminin performansı, aslına bakarsanız ISO 9001'de de vardır. İç tetkikler, yönetim gözden geçirme toplantıları, diğer standartlarda da vardır. Dolayısıyla oradaki ortak dokümantasyondan zaten faydalanacaksınız. Ama ISO 27001 ISO 9001 gibi, sanırım o da değişecek. İlla da şunu dökümente etmelisiniz mantığında değil. Süreci zaten biliyorsanız ve zorunlu dökümantasyon haricinde kalan bir konuysa dökümante etmek zorunluluğunuz yoksa çok fazla da karmaşık değil. Biz mesela şöyle ilerledik: Bilgi güvenliği politikaları var, bunları ayrı ayrı yapmak yerine bir el kitabı hazırladık. 27002'yi kılavuz alarak ilerledik. Ve tabi onun kurumumuza uyarlanmış halini kullandık. Ve bilgi güvenliği yönetimi konusunda bütün bilgi güvenliği politikalarının da olduğu kurum içerisinde kullandığımız prosedür ve talimatların da olduğu alt dökümanları da referans olarak ekledik. Ve bir el kitabı olarak çıkarttık. Ondan sonrası zaten sizin nasıl yönetmek istediğinize göre değişiyor. Biz ilk başta excel ile başladık, ama dünyanın en güzel toolunu getirin, süreç oturmamışsa o tool bir işe yaramaz. İlk

önce sürecin oturtulması lazım. Excelde de yapılabilir belki bir portalda da yapılabilir. Tabiiki excelleri yönetmek biraz karmaşık olabiliyor. Toolda yönetmek daha kolay olabiliyor, farklı avantajları var. Raporlama, karmaşıklık yok birbirini overright etmiyor. Ondan önce en önemlisi sürecin oturtulması ve olgunluk.

Peki 27001'in oluşturulması sürecinde ne gibi zorluklarla karşılaştınız? Sizi yoran problemler oldu mu?

Yine yönetim desteğinin faydasından bahsedeceğim karşılaştığımız zorluklar karşısında. Yine bir yönetim sistemi ve bir standarda uyumlu kalmaya çalışıyorsunuz ve bunun gereksinimleri var. En başından inşa ederken tabi birtakım zorlukları oluyor. Çünkü her şey ilk başta toz ve gaz bulutu oluyor. Siz bütün birimlerle, bütün müdürlüklerle varlık envanteri çalışması, risk analizi çalışması yapmanız gerekiyor. Zaten en çok kaynak ihtiyacının olduğu ve ekibin çok efor sarf ettiği alanlardan birisi bu. Ve ekipteki kişilerin gerçekten bu konuda hem çözüm odaklı olması, hem 27001 konusunda konuya tamamen hâkim olması gerekiyor. Burada ufak tefek dirençlerle karşılaştık tabiki çünkü siz bilgi güvenliği müdürlüğü olarak siz farkına varıyorsunuz ve ne yapmak istediğinizi biliyorsunuz ama iş birimlerinden bunu bilmeyen kişiler olabiliyor. Biz bu tarz durumları yönetim desteği ile aştık. Bu işin önemini anlatan farkındalık toplantıları düzenlendi ya da koordinasyon toplantılarında bahsedildi. En büyük zorluk bizim için sanırım bu uygulama kısmındaki direnç diyebiliriz. Çünkü ortada bir belirsizlik var daha ortaya çıkan somut bir şey olmadığı için, varlık envanteri, puanlamalar, risklerin sıfırdan belirlenmesi, bu da çok doğru. Çünkü bu kast daha gelişmemişti. Ama şimdi zamanla, uygulama yaptıkça, güncellemeler yapıldıkça artık kastlarımızı daha çok geliştirmeye başladık. Kurumda konu ne olursa olsun değişikliğe karşı her zaman bir direnç olur, bu sadece 27001 projesinde değil örneğin bir siem projesi yaparsınız, alışkanlıkların dışına çıktığınız zaman ister istemez insanlardan bir dirençle karşılaşıyorsunuz. Burada da yönetim desteğine hakikaten ihtiyaç duyuluyor.

9. TARTIŞMA VE SONUÇ

ISO/IEC 27001 standartının başlangıç aşaması olarak PUKÖ döngüsünün maddeleri özelinde bir çerçeve tanımlanmalıdır. Standartın gereklilikleri, iç ve dış konular ile ilgili tarafların bilgi güvenliği gereklilikleri de dahil, kuruluşu ve içeriğini anlamakla başlamaktadır. Üst yönetimin katılımı ve liderlik anahtardır ve yönetim uygun kaynakların mevcut olmasını sağlamalı, bireyleri BGYS'nin etkinliğine katkıda bulunmaları için yönlendirmeli ve desteklemelidir.

Riskleri ve fırsatları ele almak için süreçler belirlenmelidir. Bilgi güvenliği risk değerlendirmelerini yapmak, uygun bilgi güvenliği risk işleme seçeneklerini seçmek ve uygun bölüm ve seviyelerde bilgi güvenliği amaçlarını belirlemek için süreçler tanımlanmalıdır.Seçilen risk işleme seçeneğini uygulamak için kontroller belirlenmeli, hiçbir gerekli kontrolün atlanmadığından emin olmak için Ek A ile karşılaştırılmalıdır.

BGYS'nin oluşturulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için gerekli kaynaklar belirlenmelidir. Kuruluşun kontrolü altında bilgi güvenliği performansını etkileyecek işleri yapan tüm personel yetkin olmalı ve uygun iletişim kanalları ile bilgi güvenliği politikasından haberdar edilmelidir. BGYS standartın gerektirdiği dökümante edilmiş bilgiyi ve kuruluş tarafından gerekli olduğu belirlenen dökümante edilmiş bilgileri içermeli ve bunların tümü kontrollü olmalıdır.

Kuruluş bilgi güvenliği risk değerlendirmelerini yapmalı ve planlama aşamasında belirlenen kriterlere uygun olarak risk işleme planlarını uygulamalıdır.

Bilgi güvenliği performansı ve BGYS'nin etkinliği uygun izleme, ölçme, analiz ve değerlendirme yöntemleri ile değerlendirmelidir. BGYS'nin kuruluşun ve standartın gerekliliklerine uygunluğundan emin olmak için planlı aralıklarla iç tetkikler yapılmalıdır. Üst yönetim BGYS'yi uygunluk, yeterlilik ve etkinliğinin devam ettiğinden emin olmak için planlı aralıklarla gözden geçirmelidir.

Kuruluşların bir uygunsuzluk durumunda tepki verme, değerlendirme ve uygun düzeltici faaliyetleri uygulamalarını sağlamak için süreçler uygulanmalıdır. Kuruluşlar, BGYS'nin uygunluk, yeterlilik ve etkinliğini sürekli iyileştirmelidir.

Mülakat çalışmasınında gösterdiği bir sonuç olarak IEC/ISO 27001 standartının çerçevesi benimsenerek bir bilgi güvenliği yönetim sistemi oluşturulması sivil havacılık kuruluşların bilgi güvenliği performansını arttırmaktadır. Yönetim desteği alınarak oluşturulan bilgi güvenliği yönetim sistemi ile kuruluşlar bilgi güvenliği farkındalık düzeyini arttırmaktadır. Özellikle hassas verilere sahip olan sivil havacılık kuruluşları için bilgi güvenliği yönetim sisteminin oluşturulması siber tehditler sonucu oluşabilecek olumsuz sonuçları en aza indirilmesi açısından önemlidir. Kişisel veri, kredi kartı verisi gibi hassas verileri işleyen sivil havacılık kuruluşlarının regülasyonlara uyumlu olması gerektiğinden ve karşılabileceği cezalar açısından da bilgi güvenliği yönetim sistemi oluşturması gerekmektedir. Sivil Havacılık Genel Müdürlüğü tarafından zorunlu kılınan IEC/ISO 27001 standartının başarılı bir şekilde hayata geçirilmesi için yönetim desteğinin tam olması, proje elemanlarının yetkin olması, kapsam içerisinde bulunan birimlerden gereken desteğin alınması ve sürekli olarak iyileştirilmesi önemli unsurların başında gelmektedir. Çağımızın en değerli şeyi olan bilginin güvenliğinin sağlanması için bilgi güvenliği yönetim sistemi oluşturulması kaçınılmaz bir gereksinimdir.

10. KAYNAKÇA

Pfleeger, C.P. 1997. "The fundamentals of information security. Software", *IEEE* , 14(1,14)

Johnson, M. Eric & Goetz, Eric, "Embedding Information Security into the Organization", *IEEE,* Security & Privacy, May/June 2007, 16–24.

Thomson, Kerry-Lynn; Solms, Rossouw von & Louw, Lynette, "Cultivating an organizational information security culture", *Computer Fraud & Security*, 10, 2006, 7–11.

Siponen, Mikko T., "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*. 8/1, 2000, 31–41.

McCumber, J. (2005). Assessing and managing security risk in IT systems. Washington: CRC. Whitman, Michael E.; Mattord, Herbert J., "Principles of Information Security", *Introduction to Information Security*. 2011, 14-15

5651 sayılı kanun

TS ISO/IEC 27001:2013

Gürol CANBERK, Şeref SAĞIROĞLU. 2006 "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme" *Politeknik Dergisi Journal of Polytechnic Cilt: 9 Sayı: 3* s. 165-174, 2006

Shephard, B. 2002. "Information security-who cares?. Power System Management and Control," *Fifth International Conference on* (Conf. Publ. No. 488), 126s.

Oktal, Hakan & Oktal, Ozlem. (2009). "The use of information technologies and systems in airlines." *Proceedings of the European and Mediterranean Conference on Information Systems,* EMCIS 2009.

Yoon, M.G. et al. 2006. 'Impact of e-business on air travel markets: Distribution of airline tickets in Korea', *Journal of Air Transport Management* 12.

Duan, H., Wu, J. 1999. "Security management for large computer networks. Communications, APCC/OECC '99." *Fifth Asia-Pacific Conference on. and Fourth Optoelectronics and Communications Conference,* Volume 2, 1210s.

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

Guan, B., Lo, C., Wang, P., Hwang, J. 2003. "Evaluation of information security related risks of an organization: the application of the multicriteria decision-making method. Security Technology, Proceedings.",*IEEE 37th Annual International Carnahan Conference on,* 170s

Kaspersky, 2016. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within

https://www.kvkk.gov.tr/Icerik/5526/Kamuoyu-Duyurusu-Veri-Ihlali-Bildirimi-Turkiye-Is-Bankasi-A-S-

https://bilgiguvenligi.saglik.gov.tr/files/BGYS_Dokuman_Ornekleri/BG.PR...%20B%C4%B0LG%C4%B0%20G%C3%9CVENL%C4%B0%C4%9E%C4%B0%20%C4%B0HLAL%20OLAYLARI%20PROSED%C3%9CR%C3%9C.pdf

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-rising-tide-of-credential-phishing

https://www.antalyasm.gov.tr/DosyaIndir.ashx?Tip=4&Id=440&U=.docx&DosyaAd=BG.PR.04%20-%20%C4%B0HLAL%20B%C4%B0LD%C4%B0R%C4%B0M%20VE%20Y%C3%96NET%C4%B0M%C4%B0

http://www.iata.org/stbsupportportal

SAGE ACCPAC, 2006. ‘Sage Accpac Helps North American Airlines Soar to Great Heights’, Customer Success Story. http://www.careware.com.my/userfiles/file/naairlinesSS.pdf

https://www.sayistay.gov.tr/tr/Upload/95906369/files/yayinlar/RiskYonetimiRehberi.pdf
https://www.bankinfosecurity.com/airline-hack-was-denial-service-a-8342

http://web.shgm.gov.tr/documents/sivilhavacilik/files/mevzuat/sektorel/genelgeler/HGD-2015_1.pdf

http://www.yda.aero/wp-content/uploads/2018/05/PLT.01.pdf

https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf

https://eugdpr.org/the-regulation/

https://financial.ucsc.edu/Pages/Security_Penalties.aspx#non

https://www.kvkk.gov.tr/Icerik/5480/2019-144