YÖNETİMDE BİLGİ GÜVENLİK SİSTEMİNİN YAPISI İŞLEYİŞİ VE ASELSAN A.Ş.'DE UYGULAMASI

Sunay KAHRAMAN

YÜKSEK LİSANS TEZİ

İşletme Anabilim Dalı

Danışman: Prof. Dr. Mehmet ŞAHİN

Eskişehir

Anadolu Üniversitesi Sosyal Bilimler Enstitüsü

Ağustos 2006

YÜKSEK LİSANS TEZ ÖZÜ

YÖNETİMDE BİLGİ GÜVENLİK SİSTEMİNİN YAPISI İŞLEYİŞİ VE ASELSAN A.Ş.'DE UYGULAMASI

Sunay KAHRAMAN
İşletme Anabilim Dalı
Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Ağustos 2006
Danışman: Prof. Dr. Mehmet ŞAHİN

Giderek işletmeler ve sahip oldukları bilgi sistemleri ve ağları bilgisayar destekli sahtekarlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi çok geniş kaynaklardan gelen tehdit ve tehlikelerle karşı karşıyadırlar. Bilgisayar virüsleri, bilgisayar korsanları ve hizmet saldırıları gibi yıkıcı kaynaklar daha yaygın, daha hırslı ve daha karmaşık hale gelmeye başlamıştır.

Bilgi, diğer önemli ekonomik varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği bilgiyi, ekonomik sürekliliği sağlamak, ekonomik kayıpları en aza indirmek, fırsatların ve yatırımların dönüşünü en üst seviyeye çıkartmak için geniş tehlike ve tehdit alanlarından korur.

Bilgi güvenliği, politikalar, uygulamalar, yöntemler, örgütsel yapılar ve yazılım fonksiyonları gibi bir dizi uygun denetimi gerçekleştirme aracılığıyla sağlanır. Bu denetimler, işletmenin belirli güvenlik hedeflerinin karşılandığını garanti altına almak için kurulmalıdır. Etkin bir bilgi güvenlik yönetim sisteminin oluşturulması amacıyla, İngiltere Standartlar Enstitüsü (BSI) tarafından BS 7799 Bilgi Güvenliği Sistemi hazırlanmış ve ISO 17799/ISO 27001 adıyla uluslararası standartlar olarak geçerlilik kazanmıştır. ISO 17799/ISO 27001 standartları Türk Standardları Enstitüsü tarafından Türkçe'ye tercüme edilerek TS ISO/IEC 17799 ve TS ISO/IEC 27001 başlıkları altında Türk Standartları olarak yayınlanmıştır.

Bu tezde, işletmelerin TS ISO/IEC 17799 ve TS ISO/IEC 27001 standartlarında Bilgi Güvenlik Yönetim Sistemi kurmak için gereken bilgi risklerini belirleme yöntemleri vurgulanmakta ve bu risklerin giderilmesi için ihtiyaç duyulan temel safhalara ait teknoloji, politika ve prosedürler açıklanmaktadır. Bu standartlar kapsamında oluşturulan Bilgi Güvenlik Yönetim Sistemi sayesinde, işletmelerin bilgi varlıklarının güvenlik sürekliliği, yalnızca teknoloji ile değil aynı zamanda tüm şirket çalışanlarının da uyguladığı iş süreçleri ile sağlanabilecektir.

Anahtar Sözcükler: Bilgi, Bilgi Güvenliği, Bilgi Güvenlik Yönetim Sistemi, Risk Yönetimi, TS ISO/IEC 27001

ABSTRACT

Every other day the enterprises and the information systems and networks they posses are faced to threats and hazards that come from a variety of sources such as computer aided forgery, espionage, sabotage, destruction, fire and flood. Destructive sources such as computer viruses, computer piracy and denial of service attacks started to become more common, more ambitious and more complex.

Information, like other economic assets, is a precious asset for an enterprise so it must be properly protected. Information security protects information from a broad hazard and treats areas to assure economic continuity, to minimize economic loss and to maximize return of opportunities and investments.

Information security is provided by realizing a series of appropriate inspections such as policies, applications, methods, organizational structures and software functions. These inspections should be constructed to guarantee that the enterprise meets certain security goals. For an effective security management system BS 7799 Information Security system is prepared by BSI and it is used as international standards ISO 17799/ISO27001. The standards ISO 17799/ISO27001 are translated to Turkish by Turkish Standards Institute and published as Turkish Standard in the title TS ISO/IEC 17799 and TS ISO/IEC 27001.

In this thesis, the basic technology, policies and procedures required for the enterprises to establish an information security management system are explained in order to determine the real risks and eliminate them. By means of this the job processes, not only applied with technology but also with all enterprise workers, created as security management system the continuity will be provided robustly.

Key Words: Information, Information Security, Information Security Management System, Risk Management, ISO/IEC 27001

JÜRİ VE ENSTİTÜ ONAYI

Sunay KAHRAMAN'ın "Yönetimde Bilgi Güvenlik Sisteminin Yapısı, İşleyişi ve ASELSAN A.Ş.'de Uygulaması" başlıklı tezi ..... tarihinde, aşağıdaki jüri tarafından Lisansüstü Eğitim Öğretim ve Sınav Yönetmeliğinin ilgili maddeleri uyarınca, **İşletme (Yönetim ve Organizasyon)** Anabilim dalında Yüksek Lisans tezi olarak değerlendirilerek kabul edilmiştir.

İmza

Üye (Tez Danışmanı) : **Prof. Dr. Mehmet ŞAHİN** .....

Üye : .....

Üye : .....

Prof. Dr. Nurhan AYDAN
Anadolu Üniversitesi
Sosyal Bilimler Enstitüsü Müdürü

ÖNSÖZ

Mühendislik altyapısına yönelik eğitim almış bir kişi olarak, İşletme anabilim dalının Yönetim ve Organizasyon programını tamamlamış olmanın özellikle karmaşık teknik sistemlerin yönetimindeki katkılarının kaçınılmaz olacağına inanmaktayım. Başta AR-GE olmak üzere teknik organizasyonların yönetimine talip olmak isteyenlere bu programı tamamlamalarını tavsiye ediyorum. Bu program sırasında desteğini gördüğüm Sayın Prof. Dr. Mehmet ŞAHİN ve gerek ders gerekse tez hazırlıkları safhasında desteklerini esirgemeyen eşim İnci, kızlarım Mihriban ve Süeda'ya teşekkür ediyorum.

İÇİNDEKİLER

İKİNCİ BÖLÜM
BİLGİ GÜVENLİK SİSTEMİNDE RİSK YÖNETİMİ

ÜÇÜNCÜ BÖLÜM
BİLGİ GÜVENLİK YÖNETİM SİSTEMİ KURULUMU

DÖRDÜNCÜ BÖLÜM
ISO 27001 STANDARDINA GÖRE BİLGİ GÜVENLİK YÖNETİM SİSTEMİNİN ASELSAN'DA UYGULAMASI

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

GİRİŞ

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri "olmazsa olmaz" bir şekilde yer almaktadır. İletişim, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir. Bilişim sistemlerine ve bu sistemler tarafından işlenen verilere yönelik güvenlik ihlalleri inanılmaz bir hızla artmaktadır.

Bilgi güvenliği çoğu işletme için basta gelen sorunlarından biridir. "I-Love-You" virüsü bulaşmış bilgisayarlar, 11 Eylül terörist saldırıları ve Kuzey-doğu A.B.D'de 2003 yılında yaşanan elektrik kesintileriyle baltalama faaliyetleri, bilgi güvenliğinin bir ihtiyaç olduğunu kanıtlayan, çok iyi bilinen örneklerdir. Ne yazık ki işletmeler, bilgi güvenliğinin basit bir teknolojik olaydan daha fazlası olduğu gerçeğini çok çabuk unutuyorlar.

Bilgi, diğer önemli ekonomik varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği bilgiyi, ekonomik sürekliliği sağlamak, ekonomik kayıpları en aza indirmek ve fırsatların ve yatırımların dönüşünü en üst seviyeye çıkartmak için geniş tehlike ve tehdit alanlarından korur. Bilgi birçok biçimde bulunabilir. Kağıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkanlar kullanılarak gönderilebilir, filmlerde gösterilebilir veya karşılıklı konuşma sırasında sözlü olarak ifade edilebilir. Bilgi hangi biçimi alırsa alsın her zaman uygun bir şekilde korunmalıdır. Bilgi güvenliği genel olarak aşağıdakilerin sağlanması olarak tanımlanabilir:

a)Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmek;

b)Bütünlük: Bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etmek;

c) Elverişlilik: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etmek.

Bilgi güvenliği, politikalar, uygulamalar, yöntemler, örgütsel yapılar ve yazılım fonksiyonları gibi bir dizi uygun denetimi gerçekleştirme aracılığıyla sağlanır. Bu denetimler, işletmenin belirli güvenlik hedeflerinin karşılandığını garanti altına almak için kurulmalıdır.

Bilgi ve destek süreçleri, sistemler ve bilgisayar ağları önemli ekonomik varlıklardır. Bilginin gizliliği, güvenilirliği ve elverişliliği; rekabet gücünü, nakit akışını, karlılığı, yasal yükümlülükleri ve ekonomik imajı korumak ve sürdürmek için zorunlu ve gerekli olabilir.

Giderek işletmeler ve sahip oldukları bilgi sistemleri ve ağları bilgisayar destekli sahtekarlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi çok geniş kaynaklardan gelen tehdit ve tehlikelerle karşı karşıyadırlar. Bilgisayar virüsleri, bilgisayar korsanları ve hizmet saldırıları gibi yıkıcı kaynaklar daha yaygın, daha hırslı ve daha karmaşık hale gelmeye başlamıştır.

Bilgi sistemlerine ve hizmetlerine bağımlılık, işletmelerin güvenlik tehditlerine karşı daha savunmasız olduğu anlamına gelmektedir. Genel ve özel ağların birbiriyle bağlantısı ve bilgi kaynaklarının paylaşımı, erişim denetimini oluşturmadaki zorlukları arttırmaktadır.

Günümüzde, sadece çalışanlarıyla değil, müşterileri, iş ortakları ve hissedarlarıyla birlikte tanımlanan işletmelerde, bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine ilişkin güven ortamının yaratılması, stratejik bir önem taşımaktadır. Bilgi güvenliğini sağlamak, teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sisteminin kurulması ile mümkün olabilmektedir. Etkin bir bilgi güvenlik yönetim sisteminin oluşturulması amacıyla, İngiltere Standartlar Enstitüsü (BSI) tarafından BS 7799 Bilgi Güvenliği Sistemi hazırlanmış ve ISO 17799/ISO 27001 adıyla uluslararası bir standartlar olarak geçerlilik kazanmıştır. ISO 17799/ISO 27001 standartları Türk Standardları Enstitüsü tarafından Türkçe'ye tercüme edilerek TS ISO/IEC 17799 ve TS ISO/IEC 27001 başlıkları altında Türk standartları olarak yayınlanmıştır. Şirketler bilgi varlıklarını, TS ISO/IEC 17799 ve 27001 standartlarında belirtilen Bilgi Güvenliği Yönetim

Sistemini (BGYS) kurarak gerçek risklerini saptayabilir ve bu risklerin giderilmesi için gereken teknoloji, politika ve prosedürleri devreye alabilirler.

Bu tez kapsamında, birinci bölümde bilgi kavramı, bilgi güvenliği, işletmelerde BGYS kurulma gereği ve önemine değinilmiş, ikinci bölümde risk yönetimi, üçüncü bölümde TS ISO/IEC 27001/17799 standartlarına göre BGYS gerekleri, dördüncü bölümde ise TS ISO 27001 standardına uygun BGYS'nin ASELSAN firmasında uygulama şeklinin açıklanması amaçlanmıştır. Uygulama kapsamında;

– Korunacak bilgi kaynakları

– Risk yönetimine işletmenin yaklaşımı

– Kullanılan güvenlik kontrolleri ve hedefleri

– Risklere karşı gerek duyulan korunma düzeyi, belirlenecektir.

BGYS kurulum yöntem ve uygulamasından sonra işletmelerin elde edecekleri avantajların vurgulanacağı sonuç kısmı ile tamamlanacaktır.

BİRİNCİ BÖLÜM

İŞLETME YÖNETİMİNDE BİLGİ GÜVENLİĞİ KAVRAMI

1. BİLGİ

Çağımız toplumlarının en temel hedefi, bilgi toplumu düzeyine erişebilmektir. Bilgi toplumlarında, stratejik kaynak olarak kabul edilen bilgi, bilgi teknolojilerinin sağladığı imkanlarla üretilmekte, sınıflandırılmakta, erişilebilir kılınmakta ve toplumsal, kurumsal sorunlarımızın çözülmesinde kullanılabilmektedir. Günümüzde bilgi, bireylerin, organizasyonların ve devletlerin sahip olabilecekleri en stratejik kaynak durumuna gelmiştir.[1]

Bilginin tanımını farklı biçimde yapmak mümkündür. Belirli bir zümreye hitap eden bilgiden uzak durarak, bilgi mutlak olmamakla birlikte uyarlanabilir bir tanımını yapmak için bilginin kabul edilmiş tanımlarına bakacak olursak;

Webster's Sözlüğü aşağıdaki tanımları veriyor:

Bilgi: 1. Çalışma, araştırma, gözlem yada tecrübe sonunda elde edilen hakikat yada fikir. 2. İnsanın bildiği şeyler. 3. Okullarda, çoğunlukla da yüksek okullarda öğrenim yoluyla edinilen bilgiler. 4. Öğretici kitaplar.

Bu demektir ki bilgi; çoğunlukla eğitimi de kapsayan tecrübelerle edinilen hakikat ve fikirlerdir.

Roget's Thesaurus eşanlamlılar sözlüğüne bakıldığında;

Bilgi- başlığı altında 19 kelime yer alıyor. Bu eşanlamlılardan meydana gelen dizi, Webster'in hayli daraltılmış tanımlamasından çok daha geniş bir anlam taşıyor ve bilgi kavramına genişlik kazandırıyor. Buna göre bilgi; sezgi, anlama, beceri, idrak ve tahminin de eklenmesiyle derin bir anlam kazanıyor, zenginleşiyor.

Uzlaşmaya varmak için her biri çok değerli ancak ulaşılması imkansız olan Davenport ve Prusak'ın bilgi tanımlarını birleştirelim. Bilgi; deneyimler , değerler, uzmanlaşmış içerikler ve köklü sezgilerin akışkan bileşimidir. Öğrenenlerin akıllarından doğar ve gelişir. İşletmelerde yalnızca belge ve yayınlara yansımakla

[1] Şerif Şimşek, Yönetim ve Organizasyon, (Konya: Günay Ofset, 2002), s.410.

kalmaz aynı zamanda düzeni, kurallar, deneyimler ve uygulamaları ifade eder. Kısacası; buda bilginin doğru zamanda alınacak yerinde kararların, tahminlerin, tasarımların, planlamaların yükünü taşıyabilmesini mümkün kılar. Bilgi; bireysel ve ortak akıllar tarafından oluşturulur ve paylaşılır. Sadece veritabanlarından edinilmez; deneyimler, başarılar, başarısızlıklar ve öğrenimle zaman içinde kazanılır .[2]

Bilgi, mal ve hizmet üretimindeki, personel, malzeme, makine (tesis ve enerjiyi de içerir) ve para gibi temel girdilere ilave edilen belki de en pahalı ve önemli girdi olarak ifade edilmektedir.[3]

Bilgi, toplanmış, organize edilmiş, yorumlanmış ve belli bir yöntemle etkin karar vermeyi gerçekleştirmek amacıyla ilgili birime iletilmiş, belirli bir amaç doğrultusunda süreçlenen, yararlı biçime dönüştürülmüş ve kullanıcıya değer sağlayan verilerdir. Bilgi, çoğulculuğu, çeşitliliği, kurum içi etkileşimleri ve organizasyon faaliyetlerinin mantıksal arka planını oluşturmaktadır. Ünlü savaş uzmanı Napolyon'a göre, doğru bilgiyi doğru zamanda temin etmek savaşın onda dokuzunu kazanmak demektir.[4]

Bilgi bir üretim faktörüdür, diğer üretim faktörleri kullanıldıkça tüketilirken bilgi tüketilmemekte, transfer etmekle kaybolmamakta, bol fakat, kullanma yeteneği sınırlı olmaktadır. Ancak bilgi, organize bir düzen içinde gerçekleştirilmezse yaratılması güçleşmektedir.[5]

Özetle bilgi; verinin insanların yetenekleriyle, birikimleriyle, deneyimleriyle, fikirleriyle, düşünceleriyle, sezgileriyle, sorumluluklarıyla ve güdüleriyle bütünleşmiş biçimidir.[6]

Eflatun'un dan beri (M.Ö.400) batıda bilginin anlamı ve işlevi konusunda yalnızca iki teori söz konusudur. Doğuda'da aşağı yukarı aynı zaman süresi içinde yine iki teori gelişmiştir. Eflatun'un sözcüsü Sokrat, bilginin tek fonksiyonunun kendini bilme olduğuna, yani kişinin entelektüel, ahlaki ve ruhsal büyümesiyle ilgili olduğuna inanmaktadır. Onun en büyük hasmı, zeki ve bilgili

---

[2] Amrit TIWANA, Bilginin Yönetimi (Dışbank, 2003), s.76.
[3] Hadi Gökçen, Yönetim Bilgi Sistemleri (Ankara: EPİ yayıncılık, 2002), s.13.
[4] Şimşek, a.g.e., s.408.
[5] Famil Şamiloğlu, Entelektüel Sermaye (Ankara: Gazi Kitapevi,2002), s.18.
[6] Mehmet Şahin, Yönetim Bilgi Sistemi (Eskişehir: A.Ü.İkt. ve İda.Bil.Fak.Yayınları, 2003),s.485.

Protagoras ise, bilginin amacının, sahibine ne diyeceğini ve onu ne zaman diyeceğini bilme olanağı getirmekle onu etkin kılmak olduğu inancındadır. Protogoras'a göre bilgi, mantık, dilbilgisi ve konuşma sanatı demektir. Bunların üçü daha sonra "trivium" adıyla Ortaçağ'da eğitimin çekirdeğini oluşturmuştur. Bugün bile, "genel eğitim" dediğimiz zaman ifade edilmek istenen yukarıdaki kapsama girer. Almanlar da "Allgemeine Bildung" dedikleri zaman aynı ifadeyi kastetmektedirler.

Doğuda da bilgi konusunda aşağı yukarı aynı iki teori geçerlidir. Bilgi Konfiçyüsçüler açısından, ne diyeceğini ve onu nasıl diyeceğini bilmekti, dolayısıyla da ilerlemenin ve dünyasal başarıların yolunu ifade ediyordu. Taoistler ve Zen rahipleri için de bilgi kendini bilmekti, yani aydınlığa ve bilgeliğe açılan yol olarak biliniyordu. Ama taraflar bilginin anlamı konusunda böyle kesin görüş ayrılıklarına sahip olsalar bile, bilginin ne olmadığı konusunda tümü ile aynı görüşteydiler. Kesinlikle yapabilme yeteneği, işe yararlık olarak ifade edilmedi. İşe yararlık, bilgi olamaz, beceri olarak ifade edilirdi. Yunanca adı da "téchné" dir. Sokrat ve Protagoras için bile "téchné", saygın bir şey olmakla birlikte, yine de bilgi değildir. Ayrıca "téchné'yi" öğrenmenin tek yolu, çıraklık ve tecrübe olarak biliniyordu. Yazı ile de ifade edilmez ve ancak göstermek gerekirdi. 1700'den başlayarak inanılamayacak kadar kısa bir elli yıl içinde, teknoloji icat edildi. Kelimenin oluşturuluş biçimi bile, zaanat becerilerinin esrarengizliği olan "téchné" ile loji'yi, yani organize, sistematik, amaçlı bilgiyi birleştirdiğinin göstergesidir.[7]

Sonuç olarak, bugün en büyük güçlerden birisinin bilgi olduğu gerçeği kabul edilmiş ve dünya bu gerçek ışığında yapılanmış ve hatta içinde yaşadığımız çağa bilgi çağı denmeye başlanmıştır. Üstün teknolojinin sağladığı inanılmaz kolaylıklara sınırları ortadan kalkan ve biri birine yaklaşan devletler, kuruluşlar ve kişilerin yarattığı global dünya ile birlikte bilginin önemi daha da artmıştır. Bilgi ancak paylaşıldığı müddetçe bilgidir. Hali hazırda, teknolojik alandaki gelişmelere paralel olarak iletişim ve bilgisayar ortamlarındaki baş döndürücü ilerlemeler çok miktarda bilginin üretilmesine, depolanmasına, süratle iletilmesine ve kullanımına

[7] Peter F.Drucker, Kapitalist Ötesi Toplum (İstanbul: İnkilap Kitapevi,1993), s. 43-44.

imkan sağlamaktadır. Bu ise toplumun her kesimine bilginin etkin kullanımı açısından büyük faydalar sağlamakta ve bu kesimlerin her seviyesinde büyük çapta bilgi alış verişi olabilmektedir. Bugün, buna gösterilebilecek en güzel örnek 'INTERNET' tir.

1.1. Veriden Bilgiye

Veri, gerçeklik üzerinde yapılan gözlemlerin soncu ve bu anlamda bilginin üretildiği hammaddedir. Başka bir ifadeyle veri, kullanıcılar için herhangi bir anlam ifade etmeyen olgular ve şekillerdir. Verilerin sadece sayısal değerler olmaları gerekmez. Deneylerle elde edilen yada gözlemlerin sonucu olan, sayısal olmayan değerler da veri olarak değerlendirilir. [8]

Bir markette duyduğunuz her bip sesi, kasiyerin marketin veritabanına yeni bir para eklediğinin işaretidir. Kasanın yazdığı fişte ne aldığınız, saat kaçta aldığınız ve ne kadar aldığınızı görebilirsiniz. Ama fişte bu ürünü neden aldığınız, neden özellikle o markayı aldığınız, neden o saatte ve neden o miktarda aldığınıza dair bir bilgi yoktur.

Market açısından veri; bir olay hakkında bir dizi özel ve objektif açıklamalar ile yapılmış bir alışverişin yapısal kayıtlarından ibaret bir olaydır. Olay sizin favori biranızı almanız da olabilir, yaşam boyu biriktirdiğiniz tüm paranızı borsada kaybetmeniz de. Çünkü rakamlar, tek başlarına bakıldıklarında hiçbir anlam ifade etmezler. Örneğin, aldığınız marka biranın, bugün ülke çapında daha fazla sattığı, dünkü satışlarının ne olduğu ve yarın ne satacağını rakamlardan anlayamazsınız. Aynı şekilde, hisse senetlerine bakarak, biranızın dünkü, bugünkü ve yarınki kalitesi hakkında bilgi edinilemez. Rakamlar ve veriler, ancak bilgiye dönüştürüldüklerinde bir anlam kazanacaklardır. Diğer bir deyişle, bilginin hammaddeleridir.[9]

Düzenlenmiş olmayan bilgi hala veridir. Bir anlam ifade etmesi için bilginin düzenlenmiş olması gerekir. Bununla birlikte, kişinin kendi işi için belirli tür bilgilerin ne şekilde ve ne özellikle nasıl bir düzenlenmeyle bir anlam ifade ettiği hiç de açık değildir. Aynı bilginin farklı amaçlar için farklı biçimlerde

[8] Gökçen, a.g.e., s.14.
[9] TIWANA, a.g.e., s.76.

düzenlenmesi gerekebilir. Örnek vermek gerekirse, Jack Welch 1981'de icra kurulu başkanı pozisyonuna gelmesinden sonra "General Electric Company" (GE) dünyadaki diğer her şirketten daha fazla servet yarattı. Bu başarıdaki en önemli faktörlerden biri, GE'nin birimlerindeki herkesin performansı hakkındaki aynı bilgiyi farklı amaçlar için düzenlemesi olarak değerlendirilmektedir.[10]

Bilgi bir organizasyonun içinde her zaman vardır. Günümüz dünyasının yığınla verisi ve her şeyin iç yüzünü çabuk kavrama ve hızlı kararlar alma zorunluluğu, bilgiyi ona ihtiyaç duyan herkes için anahtar konuma getirmiştir.[11]

1.2. Bilginin Sınıflandırılması

Bilgi, bilgi felsefesi açısından örtük ve açık bilgi olarak iki ayrı sınıfta incelenmektedir;

Örtülü bilgi: Yüksek derecede kişisel olan bir bilgi türüdür. Bu tür bilgiyi formülleştirmek ve bu nedenle başkalarına iletmek güçtür. Örneğin zanaatkarlıkta kullanılan bilgi yada tencerenin dibini tutturmadan sütlaç yapmak için kullanılan bilgi, örtülü bilgidir. Örtülü bilgi, yetenek, deneyim ve becerilerin yanında Senge'nin "5 nci Disiplin" de üzerinde durduğu "zihni modeller" i ve değerleri de içerir. Örtülü bilgi; bilişsel boyutta öznel, teknik uzmanlık boyutta ise deneyseldir.[12]

Bilgi yaratma süreci sübjektif örtük bilginin (deneyime dayalı) dönüşüm geçirerek objektif açık bilgi haline gelmesi çevresinde gelişir ve dışsallaştırma olarak adlandırılır. Bu süreç içinde yaşanan sorun, deneyime dayalı örtük bilginin bütünleştirilmesi, düzenlenmesi, deşifre edilmesinde karşılaşılan zorluklardır. Örneğin kent içine girdiğinizde trafik ışıklarına, yayalara, hız limitlerine, trafik kurallarına uymak gibi bir çok eylemi çok kısa bir anda karar verip yapmak zorundasınızdır. Deneyiminizi kullanarak bilinçaltı bir dürtüyle kazaya yol

---

[10] Peter F. Drucker, 21. Yüzyıl İçin Yönetim Tartışmaları (İstanbul: Epsilon Yayıncılık, 2000), s.141-142.
[11] Şamiloğlu, a.g.e., s.26.
[12] Umut Koç, 3.Ulusal Bilgi, Ekonomi ve Yönetim Kongresi (Osmangazi Üniversitesi yayınları, 2004), s.419.

açmadan bunu başarırsınız. Adeta kodlanmışınızdır. Ama bunları başkasına anlatmak ya da aktarmak son derece zordur.[13]

Açık bilgi: Bilimsel ve sistematiktir. Bu yüzden de başkalarına kolaylıkla iletilebilir ve yine başkalarıyla kolaylıkla paylaşılabilir. "Deniz seviyesinde saf su, 100 °C' de kaynar" ifadesi açık bir bilgiyi göstermektedir. Açık bilgi; nesnel ve formüle edilebilmektedir.[14]

Kolay ulaşılabilme, saklanabilme ve kişiler arasında paylaştırılabilme özelliğine sahip olan açık bilgi; kontrol edilmesi, yönetilmesi ve en önemlisi de işlenmesi en kolay olan bilgi türünü oluşturmaktadır. Organizasyonlarda açık bilgiye örnek olarak dokümanlar, veri tabanları, prosedürler, üretim sürecine ait teknik bilgiler, kılavuzlar, formüller, organizasyon şemaları gösterilebilir.[15]

1.3. Bilginin Özellikleri

Bilgiyi daha iyi kavramak için bilginin bazı temel özelliklerini incelemek gereklidir. Bunlar beş grupta toplanabilir.

Bilgi Dağınıktır: İşletmelerde bilginin her boyutu çevresindeki her unsurla bağlantılıdır. Bilgiyi çevresindeki bu unsurlardan ayırt etmek oldukça zordur. Bilgiyi oluşturan ve etkileyen faktörler karmaşık ve düzensiz bir yapıya sahiptir. Kurumsal bilgi, sosyal yapı, kültür, teknoloji, örgütlenme yapısı ve bireylerin şahsiyet yapıları ve becerileri ile doğrudan veya dolaylı olarak bağlantılıdır. Bilgiyi bütün çevresinden tamamen saf olarak izole edip çalışmak mümkün değildir. Bu bağlamda, bilgi üretimi için gerekli ortam oluşturulurken, onun uygun çevre şartlarını da hazırlamak gereklidir.

Bilgi Kendini Düzenleyebilen Bir Yapıya Sahiptir: Bilgi gerçekte kendi kendini örgütleyebilen bir kimliğe sahiptir. Bilgiyi düzenleyen ve yönlendiren bu yapı ise, işletmenin veya grubun kimliği, vizyonu ve misyonu çok net olarak tanımlanmış ve her bir fert tarafından ortak bir değer olarak paylaşılmamışsa, katma değeri yüksek bir bilginin üretilebilmesi mümkün olmayacaktır.

---

[13] TIWANA, a.g.e., s.87.
[14] Koç, a.g.e., s.419.
[15] S. Thomas, The Wealth of Knowledge (2001), s.124.

Bilgi Bir Topluluk veya Grubu Arama Özelliğine Sahiptir: Bilgi var olmak, gelişmek ve topluluk oluşturmak özelliğine sahiptir. Bunun en güzel örneği internet üzerindeki bilgi kümeleridir. Bilgi toplulukları o kadar güçlü bir yayılma dinamizmine sahiptir ki küresel çapta değiş tokuş yapmaları için insanlar arasında iletişimi teşvik eder.

Bilgi Bir Dili Kullanarak Dolaşımını Gerçekleştirir: Bilginin her bir çeşidi farklı bir terminoloji setiyle farklı bir iletişim dilinde dolaşır. Bunun için, edinilmek istenilen bilgi çeşidine göre terminolojileri anlamak ve ilişkilendirmek gereklidir. Bu bağlamda zengin bilgi ve terminolojiye sahip olmak belli bilgi boyutlarını anlayabilmek için gerekli ön şarttır.

Bilgi Kontrol Edilmesi Zor Kaygan Bir Yapıya Sahiptir: Bilgi ne kadar bir noktada toplanılmaya çalışılırsa çalışılsın o oranda kendini dağıtacaktır. Günümüzde büyük bir güç üretme aracı olan bilgi, şifrelenmiş doküman, veri tabanı, patent ve zihin mülkiyeti hakları gibi yollarla kontrol altına alınmaya çalışılmaktadır. Ancak bilgin çok fazla baskı ve kontrol altında tutularak dolaşımının engellenmesi, yeni bilgi üretimini ve geliştirmeyi olumsuz yönde etkileyecektir. Bu açıdan bilgi, çok fazla kontrol ve baskı altında tutulduğu taktirde yok olma ve işlevini kaybetme tehlikesiyle karşı karşıya kalacaktır. Bu nedenle bilginin sürekli devinim içerisinde, değişime ve paylaşıma açık olması, değerini koruyabilmesi ve artırabilmesi açısından gereklidir.[16]

1.4. Bilgi Kaynakları

Bilgi yönetim sisteminin ana besin kaynakları Tablo 1'de kısmi olsa da, bilginin çoğunun açıklanabileceği, sisteme adapte edilebileceği ve yeniden kullanılabileceği görülebilmektedir.

[16] Nazik Nazan ÖRNEK PINAR, İşletmelerde Bilgi Yönetimi ve ARÇELİK A.Ş.de Bilgi Yönetimi Sürecine İlişkin Uygulama Çalışması (Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, 2002), s.11.

Tablo 1. Bilgi Yönetim Sistemini Besleyen Bilgi Kaynakları

Kaynak	Açık/Kodlanabilir	Örtük/Açıklama Gerektirir
Çalışanların bilgisi, yetenekleri ve uzmanlık alanları	+	+
Deneysel bilgi	+	+
Takım temelli işbirliği yeteneği		+
Samimi bilgi paylaşımı	+	+
Değerler		+
Normlar		+
İnançlar	+	+
Görev temelli bilgi	+	+
Fiziksel sistemle edinilen bilgi	+	+
İnsan sermayesi		+
İç yapıyla edinilen bilgi		+
Dış yapıyla elde edinilen bilgi	+	+
Müşteri sermayesi	+	+
Çalışanların deneyimi	+	+
Müşteri ilişkileri	+	+

TIWANA, s.97.

1.5. Bilgi Üretimi

İşletme açısından bilgi üretimi beş temel aşamadan oluşmaktadır. Bunlar; saklı bilginin paylaşılması, kavramların üretilmesi, kavramların gerekçelendirilmesi, bir prototip üretilmesi ve bilginin yayılması safhalarıdır.

Saklı bilginin paylaşılması: Saklı bilginin paylaşılabilmesi için güven düzeyinin yüksek olduğu bir atmosfere gerek vardır. Üyeler zengin bir etkileşim zemini oluşturabilmek için düşüncelerini, hatta bunun yanında beden dillerini de paylaşmalı ve bunları eşzamanlı olarak ortaya koyabilmelidirler. Bilgi üretiminin bu aşamasının özelliği, konuların bolluğu ve iletişimin zenginliğidir.

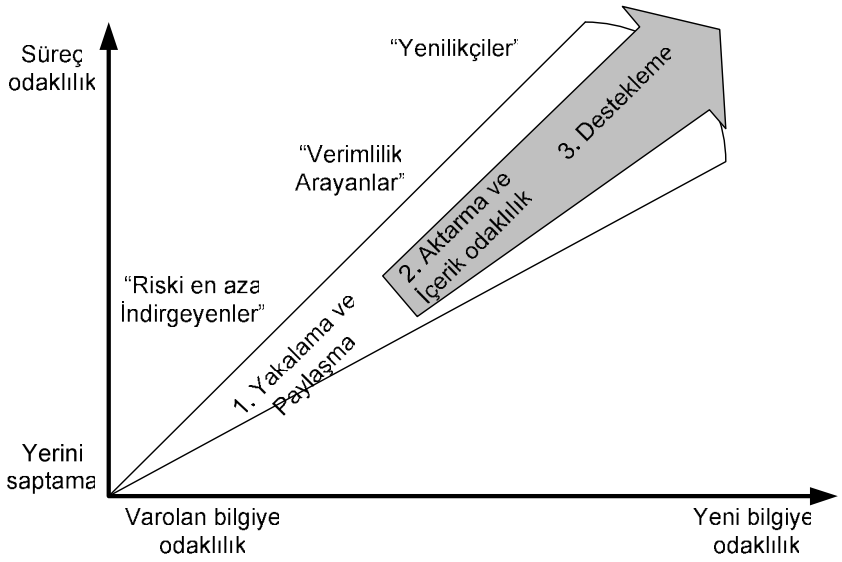
Kavramların üretilmesi: Kişilerin birbirlerine güvenmeyi öğrendikleri ve aralarında bir özen ortamı oluşturdukları bu tür açık uçlu konuşmalara dayalı etkileşim sürecinde yeni kavramlar ortaya çıkmaya başlar. Yaratıcı bir konuşma kişilerin kendi düşüncelerini ve bilgilerini tümdengelim, tümevarım ve sözcük oyunları gibi çeşitli mantık yürütme yöntemleri ile ortaya koyabilmelerine

yardımcı olur. Böylece grubun eline, yeni terimler, anahtar sözcükler, tanımlar ve anlamlar verecektir.

Kavramların gerekçelendirilmesi: Yeni kavramların işletme değerleri, bilgi vizyonu, iş stratejisi, maliyetler, yatırım getirileri vb. unsurlar çerçevesinde gerekçelendirilmesi gerekecektir. Bu süreç, kabul edilmeyecek ve beğenilmeyecek kavramların elenmesini sağlar.

Bir prototip üretilmesi: Katılımcılar teknik çözümler önerir ve bunlar üzerinde dikkatle tartışırlar. Bu noktada bilginin teyidine yönelik konuşmalar giderek daha önemli bir rol oynamaya başlar.

Bilginin yayılması: Açık bilginin ve kavramların şirket genelinde paylaşılmasını içerir.



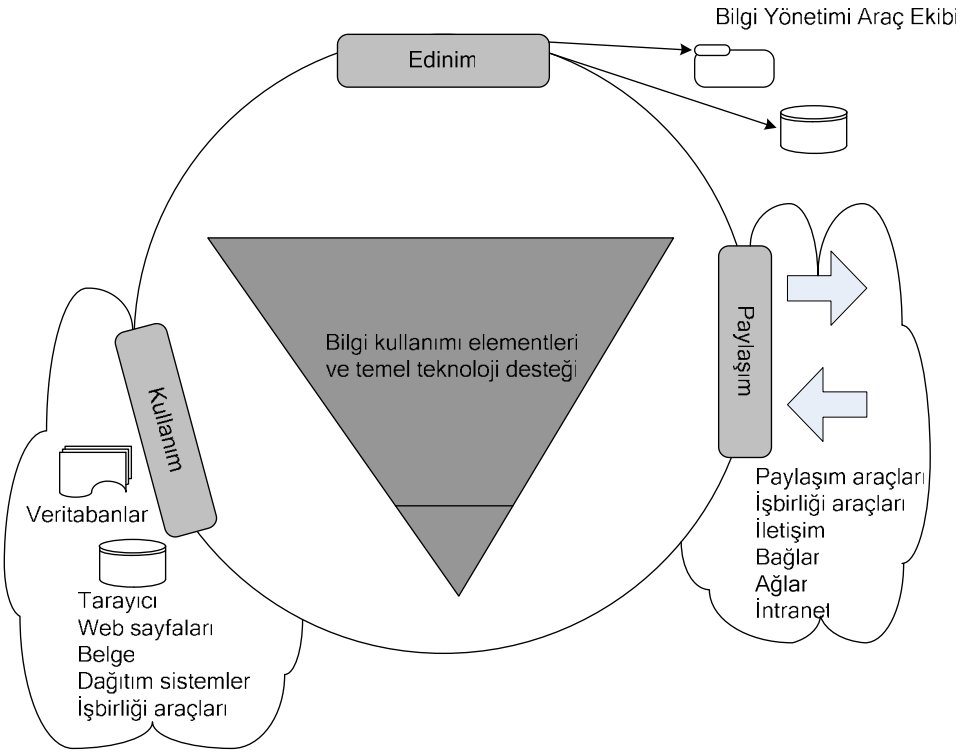
Şekil 1. Şirkette Bilgi Üretiminin Gelişmesi
TIWANA, 2003, s.97.

Şekil 1'de bilgi girişimlerinin uygulamada gözlemlediğimiz şekliyle gelişmesi gösterilmektedir. Şirketlerin bilgi girişimlerini başlatmak için birbirlerinden farklı pek çok gerekçeleri olabilir. Şirket yöneticileri, bilgi girişimlerinde genellikle riski en aza indirgeyenler, verimlilik arayanlar ve yenilikçiler olarak üç genel grupta toplanır. Bilgi üretimini destekleme yolunda en ileride olanlar yenilikçilerdir. Yöneticilerin çoğu önce diğer aşamalardan geçerler ve böyle olmasının da birtakım çok mantıklı ve anlaşılır nedenleri vardır. Böyle bir yenilik

yaparak ön sıralara geçmiş her başarılı girişimciye karşılık hiçbir yere varamamış yüz girişimci bulunur.[17]

1.6. Bilgi Edinimi Kullanımı ve Paylaşımı

Bilgi kullanımının temel elemanları ve hangi tür teknolojinin bu adımları sağlamlaştırdığı Şekil 2'den görülebilir. Bilgi kullanımı; bilginin edinilmesi, bilginin paylaşımı ve bilginin kullanımı safhalarından oluşmaktadır.



Şekil 2. Bilgi Kullanımının Temel Elemanları
TIWANA, 2003, s.110.

Bilginin Edinilmesi: Sezgilerin, becerilerin ve ilişkilerin yaratılıp geliştirilmesini kapsayan bir sürecin sonucudur. Örneğin, uzmanlaşmış bir borsacı, daha bilgisayarına göz atar atmaz, borsadaki trendin ne olduğunu, hangi hisse senedinin yükseleceği ve hangisisin düşeceğini söyleyebilir. Bu onun deneyimleri sonucunda kazandığı bir sezgi ya da bilgidir. İşte bu tür bilgi, kendisini kuşatan bilgi teknolojisiyle birlikte bir bütün oluşturur. Süzgeçten geçmiş beceri, veri

[17] George Von KROGH, Kazuo ICHIJO, Ikujro NONAKA, Bilgin Üretimi (Dışbank, 2002), s.297-298.

yakalayıcı araçlarla, akıllı veri tabanlarıyla, tarayıcılarla, "CrossPad" tipi not yakalayıcılarıyla bilgiyi destekleyecek bilgi teknolojisinin parçalarıdır.

Bilgi Paylaşımı: Şekil 2.'den anlaşılacağı gibi, bilinen konuları erişilebilir hale getirmeyi amaçlar. Bir teknik destekleme grubu, başı sıkışıp yardım isteyen kişilere istenen bilgiyi paylaşıp onların sorunlarının giderilmesini sağlayabilir. Microsoft şirketinin Internet üzerinden ürünlerine teknik destek uygulamaları bilgi paylaşımına iyi bir örnektir.[18]

Ayrıca gelecek, hem bilgi değiş tokuşu hemde bilgi paylaşımındadır. Bilgi Yönetimi Enstitüsü'nden Larry Prusak, "Daha verimli bilgi pazarları yaratmaya yönelik piyasa mekanizmaları geliştirmenin çok karlı bir iş olduğunu" söylüyor. "Bu pazarlar, bilgi alıcıları ile satıcılarına sahip oldukları malları pazarın belirlediği fiyattan alıp satma olanağı verir." Bunlar borsanın üçüncü kuşağını oluşturacaktır. Birinci kuşak yüzlerce yıl önce kurulan hammadde borsası, yüzyıl kadar önce ortaya çıkan finansal borsa ve şimdi ortaya çıkacak üçüncü kuşak borsa, bilgi borsasıdır.[19]

Bilgi Kullanımı; Erişilebilir hale gelmiş olan bilgiler de genel kullanıma açılır ve yeni durumlar karşısında kullanılırlar. Paylaşım ve kullanım birbirlerini izleyen iki halkadır. Bilgisayar destekli herhangi bir sistem bu fonksiyonların hayata geçirilmelerin ve bir bütün halinde çalışmalarını sağlamak için yeterlidir.[20]

1.7. İşletme Yönetiminde Bilgi

Bilgi organizasyonlar için yaşamsal bir unsurdur. Örgütsel planlama ve kontrol için vazgeçilmez bir kaynaktır. Örgütsel planlama ile örgütsel etkinlik arasında doğrusal bir ilişki olduğu gerçeği ışığında bilgi ile örgütsel etkinlik arasında pozitif bir korelasyon olduğu ileri sürülebilir. Başka bir deyişle, etkin

[18] TIWANA, a.g.e., s.92-96.
[19] Leif Edvinsson, Şirket Boylamı (İstanbul: Türk Henkel Dergisi yayınları, 2002), s.51.
[20] TIWANA, a.g.e., s.92-96.

bilgi temini ve yönetiminin, etkin bir örgütsel işleyiş için vazgeçilmez ön koşul olduğu iddia edilebilir.[21]

Şekil 3'te 1950'lerden 2000'lere ulaşan dönemde, yöneticilerin başvurduğu gözde araçların evrimi gösterilmektedir. Bu araçların kimi modanın oluşumuna katkıda bulundu, kimi ise günümüzde hala ayakta. Bu süreç günümüzde bilgi yönetimi diye adlandırdığımız gelişme ile noktalandı.

Günümüzde işletmeler (kar amaçlı olsun olmasın) mal ve/veya hizmet üreten kurumlar değil, "değer merkezleridir". Mal ve hizmetler, değerlerin somutlaşmış halidir. Ekonomik faaliyetlerin temeli olan "değer yaratma" ve "değişim", fiziki olarak değer yaratma (üretim) ve yaratılan ürünün fiziksel olarak el değiştirmesi faaliyetleri yanında, iletişim ve bilgisayar teknolojilerini kullanarak ve yenilikler yaparak, değer olarak bilgi yaratmak, bilgiyi kullanarak fiziksel akımları (hammadde-imalat-satış) yönlendirmek ön plana geçmiştir. Artık, "bilgi" en fazla değeri olan çıktı olmuştur.[22]

IBM firması deneyimlerine göre:

-Bilgi yönetimi her şeyden önce bir işletme konusudur ve teknoloji de onun bir yardımcısıdır.

-Bilgi yönetimi işletme için merkezi bir öneme sahiptir ve işletmenin dokusunun bir parçasıdır.

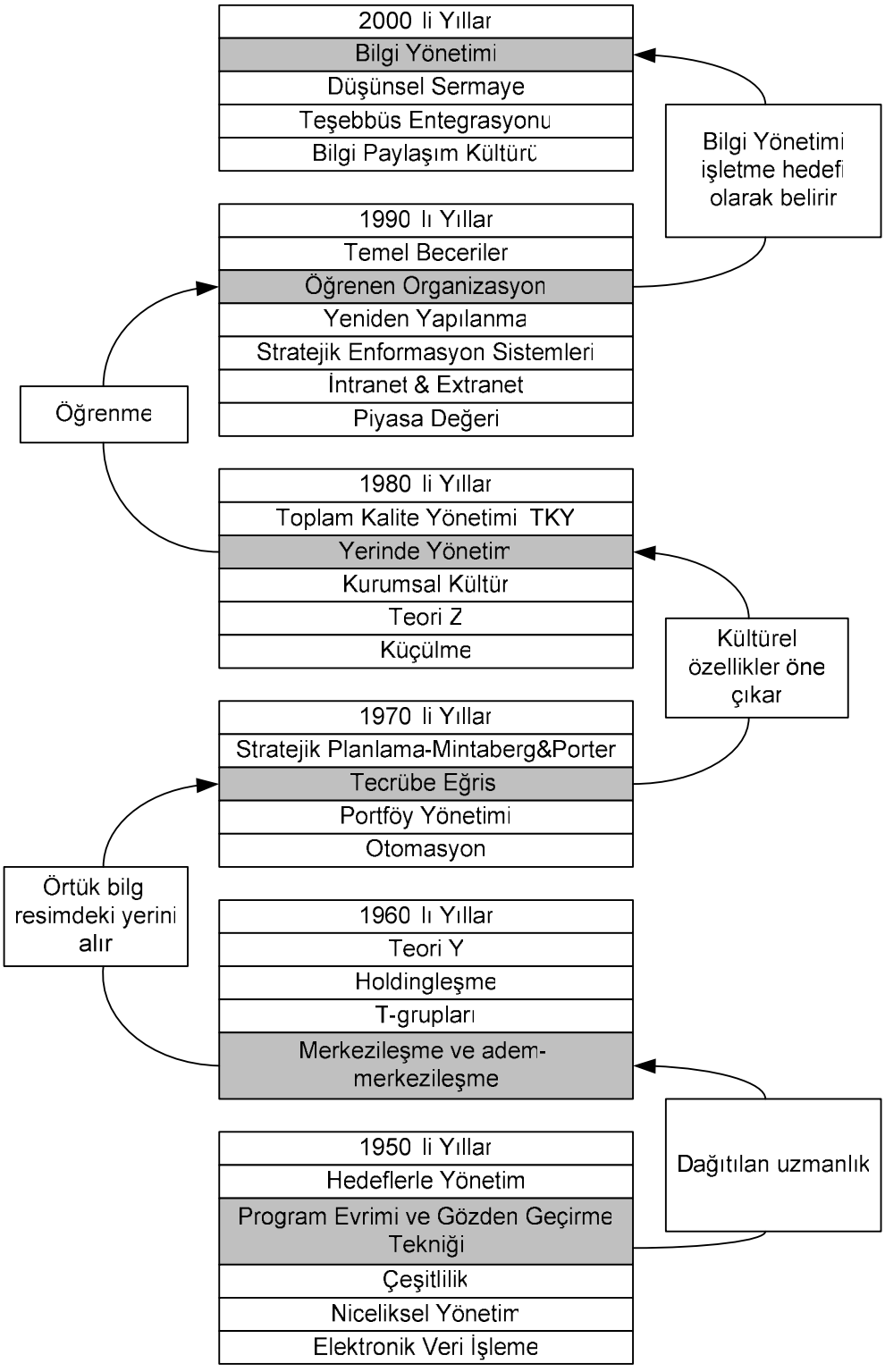
-Bilgi yönetimi insan davranışını kapsamaktadır.

-Bilgi yönetiminden faydalanabilmek için, yatırım yapılması gerekmektedir.

-Başarılı bilgi yönetimi bir sistem yaklaşımını gerektirmektedir.[23]

---

[21] Şimşek, a.g.e., s.410.
[22] Koç, a.g.e., s.419.
[23] Şamiloğlu, a.g.e., s.15.



Şekil 3. Bilgi Yönetiminin 1950'lerden Günümüze Gelişimi
TIWANA, 2003, s.110.

İkinci Dünya Savaşının sonunda 1970'li yılların ortalarına kadar 30 yıl boyunca, gelişmiş ülkelerin hepsinde, yüksek ücretli işler vasıfsız beden işlerinde yoğunlaşmıştı. Şimdi yüksek ücretli yeni işlerin çoğunluğu bilgi işlerindedir: teknisyenler,profesyoneller, çeşitli alanlardaki uzmanlar, yöneticiler gibi. 20 yıl önceki yüksek ücretli işler için sendikadan alınan bir kart çalışmak için yeterli görülüyordu. Şimdi yeterlilik denince örgün eğitim anlaşılmakta. Çalışan insanın sayı olarak, sosyal statü olarak, gelir olarak uzun süren müthiş yükselişi bir gece içinde hızlı bir gerilemeye dönüşüvermiştir. Bu dönüşümün sebebi üretimdeki düşüş değildir. ABD'nin imalat sanayii üretimi düzenli olarak yaygınlaşmaktadır. Büyüme hızı gayrı safi milli hasılaya eşit hatta ondan biraz daha yüksektir. Beden işçisinin gerileyişi ne bir rekabet gücü meselesi, ne hükümet politikaları, ne iş hayatının bir dönemi, hatta ne de ithalat meselesidir. Gerileme yapısaldır, geri dönüşü de yoktur. Bunun sebebinin biriside, düzenli olarak emek yoğun sanayilerden bilgi yoğun sanayilere geçiştir. Bu duruma yüksek kazanlardan dökülen çeliğin azalışı, ilaç yapımının ise devamlı artışı örnek olarak gösterebiliriz. Son yirmi yıl içinde, ABD imalat sanayii üretimindeki artışın tamamı bilgi yoğun sanayilerde meydana gelmiş ve hemen hemen iki katına çıkmıştır. Geleneksel kaynakların yani emeğin, toprağın ve sermayenin getirisi giderek azalmış, servet kazanan kaynaklar olarak bilgi ortaya çıkmıştır.[24]

Bilgi ucuza elde edilemez. Bütün gelişmiş ülkeler, Gayri Safi Milli Hasılalarının yaklaşık beşte birini bilginin üretimine ve dağıtımına harcamaktadırlar. Zorunlu okul eğitimi, yani kişilerin işgücüne katılmadan önce aldıkları eğitim, Gayri Safi Milli Hasılanın yaklaşık onda birini götürmektedir. (Birinci Dünya Savaşından bu yana bu oran %2'den yükselerek bu duruma gelmiştir.) İstihdam veren kuruluşlar da elemanlarının sürekli eğitimini sağlamak için Gayri Safi Milli Hasılanın %5'ini daha harcamaktadırlar. Bu rakam daha da yüksek olabilir. Bunlardan ayrı olarak, Gayri Safi Milli Hasılanın %3-5 arasındaki bir oranı da araştırma-geliştirmeye harcanmakta, yani yeni bilgilerin üretilmesine gitmektedir.[25]

---

[24] Drucker, 1993, a.g.e., s.151.

[25] Drucker, 1993, a.g.e., s.259-260.

En büyük değişiklik, bilgide olacaktır. Bu değişiklik, bilginin biçiminde ve içeriğinde, anlamında, sorumluluğunda ve eğitimli insan için taşıdığı anlamda kendini gösterecektir.[26]

2. BİLGİ GÜVENLİĞİ

Günümüzde internetin yaygınlığının ve kullanımının artması, gittikçe üzerinden daha fazla kritik veri dolaşması, kurumların iş süreçlerini elektronik ortama taşıyarak kurumsal kaynak planlama (ERP) ile e-iş fonksiyonlarını birleştirme çabaları, bunun sonucunda daha hızlı işlem yapmaları ve dolayısıyla ürün ve hizmetlerine rekabet üstü değerler kazandırmaları git gide tüm bu unsurlara temel teşkil eden güvenlik teknolojilerinin önemini arttırmaktadır. Veri güvenliği, ortam güvenliği, kullanıcı tanıma, e-ticaret gibi kavramlar giderek artan oranlarda kullanılmaktadır.

Bugünün "dijital ekonomi" dünyasında, bilgiye sürekli erişimi sağlamak ve bu bilginin son kullanıcıya kadar bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden güvenli bir şekilde sunulması giderek bir seçim değil zorunluluk haline gelmektedir.[27]

Bilgi diğer iş varlıkları kadar değerli bir servettir. Bilgi organizasyon için oldukça değerlidir ve bu nedenle en uygun biçimde korunması gerekmektedir. Bilgi güvenliği, şirketin bilgilerini çok çeşitli tehditlerden koruyarak şirketin iş devamlılığına olanak tanır, iş kaybını düşürür ve yatırımların iş imkanları olarak dönüşünü artırır.

Bilgi birçok biçimde bulunabilir. Kağıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkanlar kullanılarak gönderilebilir, filmlerde gösterilebilir veya karşılıklı konuşma sırasında sözlü olarak ifade edilebilir. Bilgi hangi biçimi alırsa alsın veya paylaşıldığı veya toplandığı hangi anlama gelirse gelsin her zaman uygun bir şekilde korunmalıdır.

---

[26] Drucker, 1993, a.g.e., s.303.
[27] ISO17799 Danışmanlığı, (Şubat 2006), http://www.innova.com.tr/04Hizmetler/detayli_bilgi02.htm,

2.1. Bilgi Güvenliği Tanımı

Bilgi Güvenliği, bilginin gizliliğinin, bütünlüğünün ve elverişliliğinin korunması olarak ifade edilmektedir. Burada;

Gizlilik: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi,

Bütünlük: Blginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesi,

Elverişlilik: Yetkilendirilmiş kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin, garanti edilmesidir.[28]

Kısaca, gizlilik; önemli, hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmemesini, bütünlük; bilginin bozuk, çarpık ve eksik olmamasını, elverişlilik ise bilgi veya bilgi sistemlerinin kullanıma hazır veya çalışır durumda olmasını hedefler.

İşte bilginin bu şekilde değerlenmesi, kurumların ürün ve hizmet bilgilerinin yanı sıra, stratejik, finansal, pazar bilgilerinin rakiplerden ve yetkisiz erişimlerden korunması, süreçlerin hızlı ve kusursuz bir yapıda işlerliği, tüm bunlara hizmet veren bilgi teknolojilerinin alt yapısı, işletim yazılımları, iletişim ağları, bilgi yönetimi vb unsurların bir sistem dahilinde düzenlenmesini ve ele alınması gereğini ortaya çıkarmıştır.

Sadece teknolojik önlemlerle (virüs koruma, güvenlik duvarı sistemleri, şifreleme vb.) iş süreçlerinde bilgi güvenliğini sağlama olanağı yoktur. Bilgi güvenliği, süreçlerin bir parçası olmalı ve bu bakımdan bir iş anlayışı, yönetim ve kültür sorunu olarak ele alınmalıdır. Her kurum mutlaka bireysel olarak ve kurum bazında bir güvenlik politikası oluşturmak, bunu yazılı olarak dokümante etmek ve çalışanlarına, iş ortaklarına, paydaşlarına aktarmak zorundadır. Tüm çalışanlar bilgi güvenliği konusunda bilinçli olmalı, erişebildikleri bilgiye sahip çıkmalı, özenli davranmalı, üst yönetim tarafından yayınlanan "BG politikası" şirket açısından bilgi güvenliğinin önemini ortaya koymalı, sorumlulukları belirlemeli, çalışanlarını bilgilendirmeli ve BG sistemi, iş ortaklarını (müşteri, tedarikçi, taşeron, ortak firma vb.) da kapsamalıdır.

---

[28] TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, (Ankara: Türk Standardları Enstitüsü, 2002), s.1.

Tüm bunlardan çıkan sonuç; Bilgi Güvenliği'nin bir teknoloji sorunu olmadığı, bunun bir iş yönetimi (sistem) sorunu olduğudur. Bu nedenle günümüzün rekabet ortamında küresel ekonominin içinde varolmak için bilgi varlıklarımızı koruma ve güvence altına alma, bunu bir yönetim sistemi yaklaşımı içinde kurumsal düzeyde yaygınlaştırma mecburiyeti kurumları Bilgi Güvenliği Yönetim Sistemi kurmaya ve kullanmaya zorlayacaktır.[29]

2.2. Bilgi Güvenlik Tehditleri

Bilgi güvenlik tehdidi, bir kişi, bir organizasyon veya o şirketin bilgi kaynaklarına zarar verebilecek potansiyele sahip bir faaliyet olabilir. Bilgi güvenlik tehditleri kasıtlı oluşturulabileceği gibi, bilinçsizlik nedeni ile kaza sonucu, hem şirket içinden hem de şirket dışından kişi veya gruplar tarafından oluşturulabilmektedir.[30]

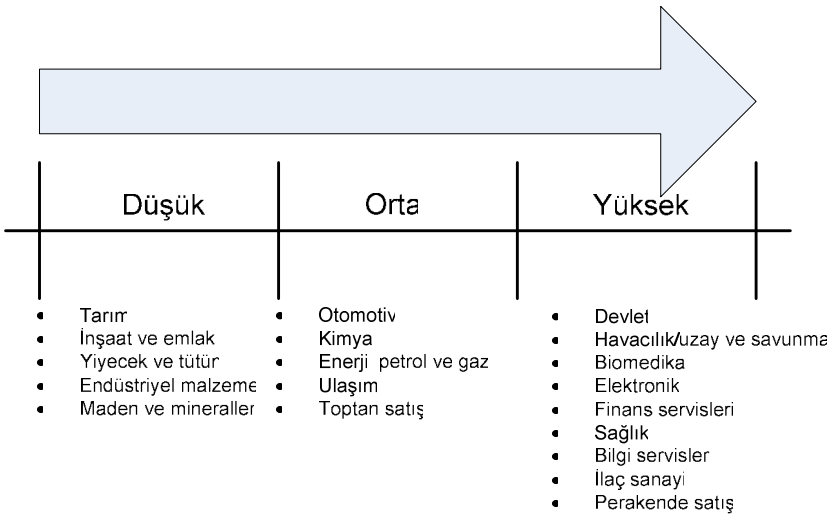
Şirketlerin çalıştıkları sektörlere bağlı olarak bilgi sistemlerinin zayıflık seviyeleri Şekil 4'te verilmiştir. Buna göre özellikle devlet, havacılık sektörlerinde zafiyet seviyesi yüksek iken tarım kısmında bu oran düşük kalmaktadır.[31]

---

[29] ISO17799 Danışmanlığı, (Şubat 2006), http://www.innova.com.tr/04Hizmetler/detayli_bilgi02.htm,

[30] McLeod Jr.Raymond, George Schell, Management Information System (Person Education, 2004), s.208-222.

[31] Bisson Jacquelin, René Saint-Germain, The BS 7799 / ISO 17799 Standard, White Paper, (Şubat 2006), https://www.callio.com/files/wp_iso_en.pdf

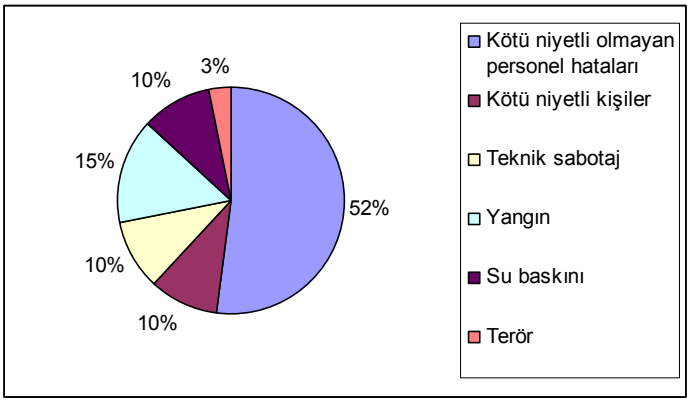


Şekil 4. Şirketlerin Sektör Seviyede Bilgi Sistem Zayıflık Seviyeleri

Jacquelin, a.g.e., https://www.callio.com/files/wp_iso_en.pdf Şubat 2006.

2.2.1. İç ve Dış Tehditler

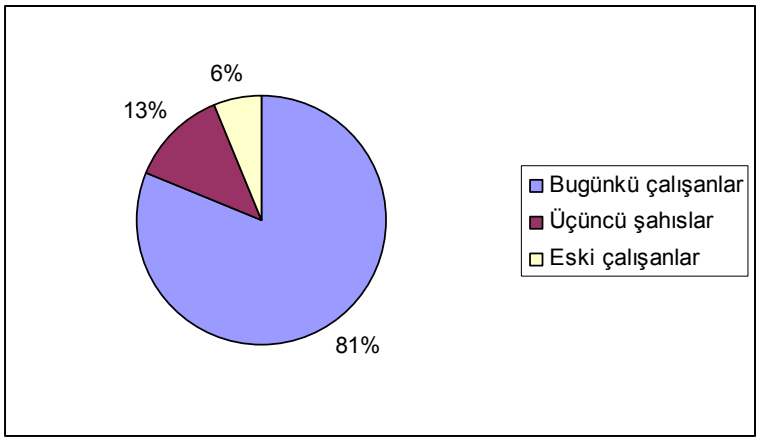
Şirket içi bilgi tehditleri, şirketin kendi personeline ilave olarak geçici çalışanlar, danışmanlar, alt yüklenicilerin personeli ve hatta ortak çalıştıkları şirketin çalışanları tarafından yaratılabilir. Gartner Datapro Research şirketi tarafından yapılan araştırmanın sonuçları kurumsal bilgilerinizin nasıl, kimler tarafından tehdit edilebileceği ve zarar verilebileceği hakkında ilginç sonuçlar vermektedir. Bu araştırmanın sonuçlarına göre Bilişim Teknolojilerinde meydana gelen zararların genel sebepleri Şekil 5'te gösterilmiştir.



Şekil 5. Güvenlik Saldırılarının Nedenleri

Türkiye Bilişim Derneği, Haziran 2003, s.10.

Saldırıların kimler tarafından yapıldığı da aynı çalışmada Şekil 6'da olduğu gibi sıralanmıştır. İşletme personelinin bilgisayar suçlarına karışma oranı %81'e kadar çıkmaktadır.[32] Bu nedenle iç tehdit, dış tehdide göre iç tehditte bulunan personelin sistem konusunda kişisel bilgiye sahip olunmasından dolayı daha ciddi sorunlara neden olabileceği değerlendirilmektedir.



Şekil 6. Güvenlik Saldırılarını Gerçekleştirenler

Türkiye Bilişim Derneği, Haziran 2003, s.10.

Güvenliğe yönelik dış tehditlere karşı kontrol mekanizması kullanılır. Kontrol aynı zamanda güvenlik tehditlerini planlayan iç tehditlerin tahmin edilmeleri amacı ile de kullanılır.[33]

2.2.2. Rastlantısal ve Kasıtlı Tehditler

Tehditler sadece zarar vermeyi amaçlayan kasıtlı eylemlerden oluşmaz. Bazıları rastlantısal olarak iç ve dış personel tarafından kaynaklanır. Bilgi güvenlik sistemi kasıtlı tehditlere karşı koruyacak önlemler içereceği gibi rastlantısal tehditleri de azaltacak şekilde olmalıdır.

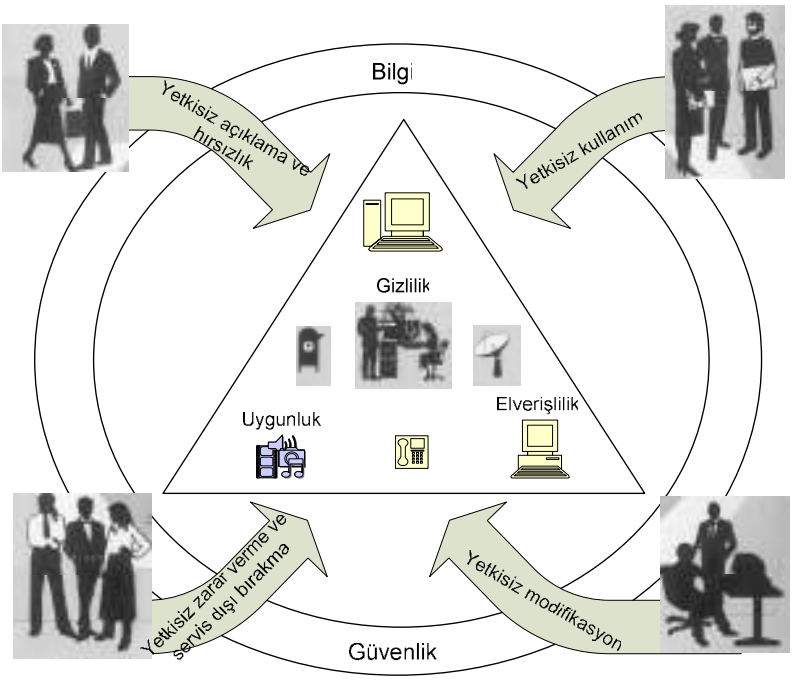
---

[32] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği,Haziran 2003), s.9

[33] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği,Haziran 2003), s.9-10

2.3. Bilgi Güvenlik Riskleri

Bilgi güvenlik ihlalleri sonucunda ortaya çıkan istenmeyen potansiyel sonuca, bilgi güvenlik riski olarak adlandırılır. Yetkisiz eylem olarak adlandırılabilecek bu riskler 4 gruba ayrılır. Şekil 7'de bilgi güvenlik sistemi amacı ve dört tip risk şekilsel olarak verilmiştir. Bunlar; yetkisiz açıklama ve hırsızlık, kullanma, zarar verme, hizmet dışı bırakmak ve modifikasyonlardır.



Şekil 7. Bilgi Güvenlik Sistemi Amacı ve Dört Tip Risk
Raymond, a.g.e. s.212.

2.3.1. Yetkisiz Açıklama ve Hırsızlık

Bir işletmede yetki verilmemiş personel, yazılım kütüphanesi, ya da veritabanına ulaşabildiğinde bilgi ve para kaybına neden olabilir. Örnek olarak endüstri casusları rekabet edebilecek bir bilgiyi ele geçirebilir, bilgisayar suçluları şirketin parasını çalabilir.

2.3.2. Yetkisiz Kullanım

Yasal olarak kullanım yetkisi verilmeyen kişilerin şirketin kaynaklarını kullanmaya başladığı durumda ortaya çıkar. Bu tip bilgisayar suçlarına bilgisayar korsanı örnek olarak verilebilir. Bu tür yetkisiz kullanımlar genellikle şirketin bilgi güvenlik sistemini bir meydan okuma gibi görmelerinden ileri gelmektedir. Bilgisayar korsanları bir şirketin bilgisayar ağına girebilir, telefon sistemini kontrol edebilir ve uzun mesafeli telefon görüşmeleri yapabilir.

2.3.3. Zarar Verme ve Hizmet Dışı Bırakma

Her personel bir şirketin bilgisayar sisteminin donanım ve yazılımına zarar verip yok edebilir. Hatta bilgisayar korsanın aynı bina içinde olmasına da gerek yoktur. Bunlar uzak terminallerden bağlantı yaparak, ekran, disklere fiziksel hasar verdirip yazıcıları karıştırıp klavyeleri kullanılmaz hale getirebilirler.

2.3.4. Yetkisiz Modifikasyonlar

Şirketin verilerinde, bilgilerinde ve yazılımlarında değişiklik yapabilirler. Bu değişiklikler duyurulmadan yürürlüğe girerek sistem kullanıcıları tarafından hatalı kararlar alınmasına neden olabilir.[34]

2.4. Kontroller

Kontroller, bilgi güvenlik risklerini yok etmek veya azaltmak için kurulan mekanizma olarak isimlendirilir. Kontroller teknik, resmi ve resmi olmayan olmak üzere üç gruba ayrılır.

2.4.1. Teknik Kontroller

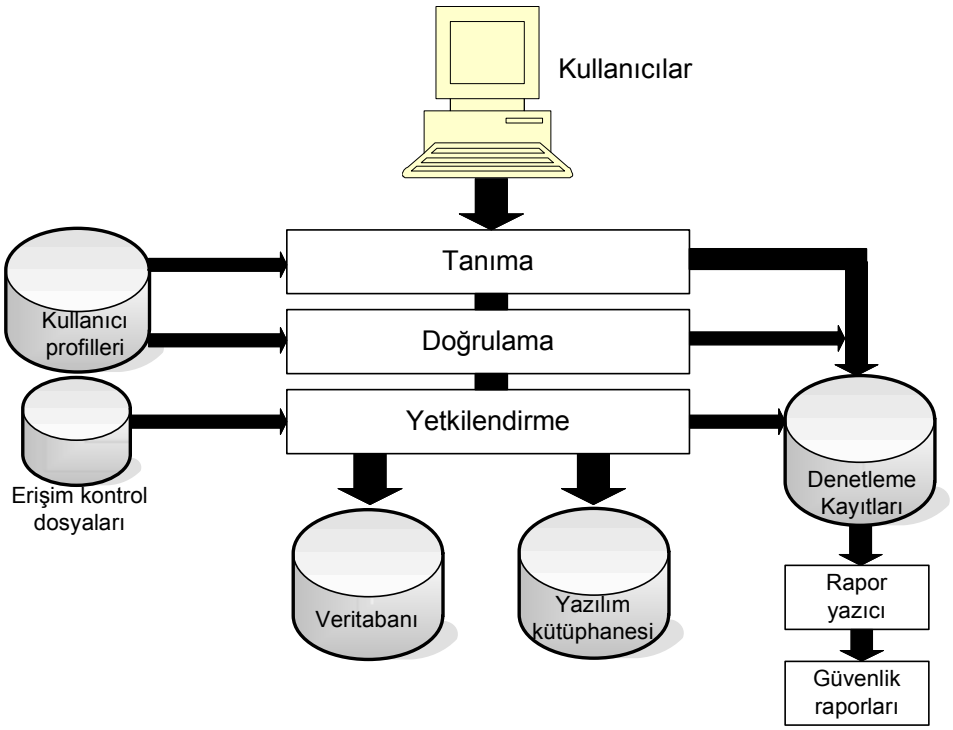
Sistem geliştirilmesi aşamasında, geliştiriciler tarafından sisteme sokulan kontrolleri teknik kontroller olarak adlandırabiliriz. Proje ekibi içinde bir denetçi olması sağlanarak bu gibi kontrollerin sistem tasarımında yer alıp almadığını kontrol edebiliriz. Güvenlik kontrollerinin çoğunluğunun temeli donanım ve yazılım teknolojisine bağlıdır. En yaygın olarak kullanılan yöntemler

[34] Raymond ve diğerleri, a.g.e., s.208-222.

aşağıda sunulmuştur. Bu üç tip kontrol biçiminin de maliyeti vardır. Risk maliyetinize uygun olmayacak bir biçimde kontrole para harcamak iyi bir uygulama olmadığından uygun bir güvenlik seviyesi sağlanması gereklidir. Genelde maliyet ile karşılaştırma yapılırken bazı alanlarda başka kavramlar da devreye girer. Örneğin, bankacılıkta ATM'lerin risk yönetiminde kontroller sistemi güvenli kılmalı ancak bu müşteri memnuniyetini olumsuz yönde etkilememelidir. Diğer bir örnekte, sağlık sektöründeki kontrol mekanizmaları hasta sağlığını ve hasta haklarını gözetmelidir. Ayrıca, sistem hasta bilgilerini hastaya bakan hastanenin ve hastanın doktorunun ulaşabileceği yapıda olmalıdır.

2.4.1.1. Erişim Kontrolü

Yetkisiz personel tehditlerine karşı güvenlik, erişim kontrolü yöntemi ile sağlanabilir. Eğer yetkisiz kişi bilgi kaynaklarına ulaşamaz ise zarar da veremez. Erişim kontrolü üç safhada gerçekleşir. Bu safhalar Şekil 8'de sunulmuştur.



Şekil 8. Erişim Kontrol Fonksiyonları
TIWANA, 2003, s.118.

Kullanıcının Kimlik Tespiti: Kullanıcılar önce, şifre gibi kendi bildikleri bir bilgi ile, kimliklerini göstermek zorundadırlar. Kimlik tespiti işlemi, kişinin yer bilgisinin telefon numarası veya ağ bağlantı noktası da içermelidir.

Kullanıcı Doğrulama : İlk kimlik tanıtma işlemi tamamlandıktan sonar, kullanıcı sahip olduğu bir bilgi ile akıllı kart veya kimlik çipi gibi giriş haklarının doğrulamasını yapar. Kullanıcı doğrulama, kullanıcının kendinin olduğu bir bilgi, imza, ses veya konuşma örneği ile tamamlanabilir.

Kullanıcı Yetkilendirme : İlk iki basamak geçildikten sonra kişi ancak kendi seviyesine veya kullanım derecesine göre yetkilendirilir. Örneğin, bir kişi bir dosyayı sadece okuma hakkına sahip iken başka bir kullanıcının o dosya üzerinde değişiklik yapma hakkına sahip olması gereklidir.

2.4.1.2. Sızma Tespit Sistemleri

Sızma tespit sistemlerinin altında yatan mantık güvenlik ihlali için yapılan bir denemeyi zarar vermeye fırsat bulmadan algılamaktır. Bu sistemlere iyi bir örnek e-posta kanalı ile taşınan virüslere karşı etkili virüs koruma programlarıdır. Yazılım, virüs taşıyan mesajları tespit eder ve kullanıcıyı uyarır. Yazılımın yeni virüslere karşı etkili olabilmesi için sürekli olarak güncelleştirilmesi gerekmektedir.

Sızma tespitine başka bir örnek de potansiyel sızma girişimlerini algılayan yazılımlardır. İç tehdit önleme araçları kişinin işletmedeki pozisyonunu, hassas veriye ulaşımını, donanım değişikliği yapma yeteneği, kullanılan yazılım tipleri, sahiplenilen belgeler ve kullanılan ağ protokolleri gibi karakteristikleri göz önünde tutarak profiller çıkartırlar. Bu profil yazılımlarının çıktıları, bazıları sayısal olmak üzere, iç tehditleri kasıtlı tehditler potansiyel kazalar, şüpheli durumlar ve zararsız durumlar gibi kategoriler altında sınıflayabilirler.

2.4.1.3. Güvenlik Duvarları

Bilgisayar kaynakları ağa bağlandıkları surece risk altındadırlar. Ağın tipi, ağ kanalıyla bilgisayara ulaşabilecek kişi sayısı riski belirler. Bir

yaklaşım firmanın Web sitesini hassas bilgiler içeren iç ağından fiziksel olarak ayırmaktır. Diğer bir yaklaşım, iş ortaklarının şifre ile Internet üzerinden iç ağa ulaşımını sağlamaktır. Üçüncü bir yaklaşım ise koruyucu bir güvenlik duvarı kurmaktır.

Güvenlik duvarı içeri ve dışarı veri akışını kısıtlayan bir filtre ve bariyer rolü oynar. Güvenlik duvarının arkasındaki kavram firmanın ağa bağlı bütün bilgisayarlarını bir bütün halinde korumaktır, her bilgisayar için ayrı bir koruma gerekmemektedir.

2.4.1.4. Şifreleme Kontrolleri

Depolanan ve iletilen veri ve bilgiler istenmeyen kişilere karşı şifreleme, matematiksel süreçlerle oluşturulan kodlar kullanılması ile de korunabilir. Şifreleme işlemi sayesinde bilgiler anlamsızlaştırılarak, yetkisiz bir kişinin bu dosyalara erişim sağlaması durumunda dahi, anlaşılmasını ve kullanılmasını engeller.

Şifrelemenin öneminin artmasının sebebi, e-ticaret artmakta ve özel protokoller geliştirilmektedir. İmzalar e-ticaret'e taraf olan iki taraf için de yayınlanır. Kredi kartı numaraları yerine çift imza kullanılır.

Şifrelemenin suç veya terörist eylemlerin gizlenmesinde kullanılmasından çekinen hükümetler konu üzerine ilgileri toplamaktadır. Şu anda şifreleme yazılımlarının ithalinde sınırlamalar olmasa da ihracında sınırlamalar bulunmaktadır. Amerika Birleşik Devletleri, Küba, Irak, İran, Libya, Kuzey Kore, Sudan ve Suriye'ye şifreleme teknolojisinde ihraç yasağı uygulamaktadır. Şifrelemeye olan ilginin artması, e-ticaretin ve teknolojinin ilerlemesi ile birlikte hükümet kısıtlamalarının artması beklenmektedir.

2.4.1.5. Fiziksel Kontroller

İstenmeyen kişilere karşı yapılan ilk koruma metodu bilgisayarın bulunduğu odanın kapısını kapamaktı. Bu konudaki gelişmeler daha gelişmiş kilit yapılarının, ses veya avuç izleri ile açılan, güvenlik kameraları ve korumalar gibi araçların da kullanılabileceğini göstermektedir. İşletmeler, bilgi işlem merkezlerini şehrin uzağına ve doğal afetlere karşı güvenli yerlere taşıyabilirler.

2.4.2. Resmi Kontroller

Resmi kontroller yönetim kurallarının sağlanması, beklenen prosedürler ve durumların dokümantasyonu ve sağlanan yönetmeliklerin dışında olan davranışların belirlenmesi ve önlenmesini içerir. Kontroller resmi, yazılı olarak belgelenmiş ve uzun vadede etkili olmalıdır. Bu kontrol sisteminin etkili olabilmesi için üst yönetimin de aktif olarak sisteme katılmalarını gerektirmektedir.

2.4.3. Resmi Olmayan Kontroller

Bu kontrol biçimi firmanın çalışanlarının etik anlayışını, firmanın amacının anlaşılmasını, eğitim programlarını içerir. Bu kontroller işletme çalışanlarınca güvenlik programının anlaşılıp, çalışanlar tarafından destek verilmesini amaçlamaktadır.[35]

2.5. Bilgi Güvenlik Yönetim Sistemi ve Tarihçesi

Bilgi ve iletişimin büyük bir önem kazandığı dünyada şirketlerin verimliliklerini artırabilmeleri, pazarda etkin rol oynamaları, müşteri ve pazar paylarını artırmaları ve rekabet üstünlüğü sağlayabilmeleri için bilgi edinme ve bilgileri işleme konusunda gerekli teknolojileri kullanmaları, süreçlerini bilgi yönetimine göre şekillendirmeleri ve insan kaynaklarını bu yönde yetiştirmeleri gerekmektedir.

Geleneksel iş dünyasında bilişim sistemlerine gittikçe artan bağımlılık, bilişim dünyasının sunduğu olanaklar ve tüm bunların getirdiği iş fırsatları ve riskler ister istemez "bilgi" kavramının da yönetimsel bir yaklaşımla stratejik seviyede ele alınmasına ve kurumları bu alanda sistem yaklaşımları kurmaya zorlamıştır.

İşte 1990'lı yılların ortalarına doğru İngiltere'de bazı endüstriyel kuruluşların talepleri ve BSI (İngiliz Standartlar Enstitüsü) girişimleri ile temelleri atılan Bilgi Güvenliği Standartları BS7799 altında ortaya çıkmıştır. 1995 yılında

---

[35] TIWANA, a.g.e., s.115-120.

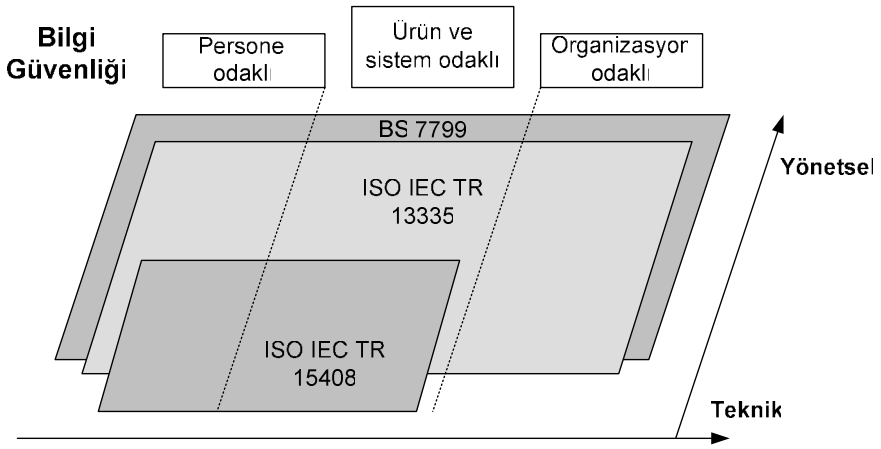
BS7799 olarak yayınlanan standart daha sonra iki kısma ayrılarak BS7799-2:1998 ve BS7799-1:1999 olarak yayınlanmıştır.

Uluslararası Standartlar Komitesi (ISO:International Organization for Standardization) ise Bilgi Güvenliği ile ilgili standardın birinci bölümünü 2000 yılında ISO 17799 olarak yayınlamıştır. Bununla birlikte ISO tarafından IT Güvenlik standartları ile ilgili çalışmalar JTC 1(Joint Technical Committee) Bilişim Teknolojileri komitesine bağlı SC 27: Bilişim Güvenlik Teknikleri alt komisyonunda ele alınmaktadır. Bu komisyon içinde üç ayrı çalışma grubu (Working Group) bulunmakta ve her biri farklı konularda standartlar hazırlamaktadır. Bu çalışma grupları ve konuları aşağıda verilmektedir:

- WG1:Güvenlik Yönetimi (Security Management)
- WG2:Şifreleme Teknikleri (Cryptograhic Techniques)
- WG3:Bilişim Ürünleri ve sistemleri için güvenlik değerlendirmesi (Security Evaluation of IT Products and Systems)

SC27'ye bağlı çalışma gruplarından WG1, ISO/IEC 17799 ile ilgili çalışmaları yürütmektedir. "Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri"ni içeren standardın son gözden geçirmeleri (FDIS) 2004 Ekim'de tamamlanmış ve yeni versiyonun 2005 yılının ortalarına doğru yayınlanması planlanmaktadır. Türk Standartları Enstitüsü tarafından TS ISO/IEC 17799 Kasım 2002'de yayınlanmış olup, tetkiklerde kullanılan BS7799-2 standardının karşılığı olan TS 17799-2 "Bilgi Güvenliği Yönetim Sistemleri-Özellikler ve Kullanım Kılavuzu" Şubat 2005'de yayınlanmıştır.

Temel olarak endüstri, devlet ve ekonomik kuruluşlar tarafından ortak bir güvenlik modeli oluşturulmasına yönelik talepler doğrultusunda geliştirilen BS7799 Bilgi Güvenliği standardı ISO/IEC TR 13335 (IT Güvenliği Yönetimi için kılavuz) ve ISO/IEC 15408 (IT Güvenliği için Değerlendirme Kriterleri) temel alınarak hazırlanmıştır. Standartlar arası etkileşim Şekil 9'da verilmiştir.



Şekil 9. Bilgi Güvenlik Standartlarının Kapsamı

http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=583, Şubat 2006,

Sertifikasyona esas kurallar standardın ikinci kısmında bulunduğu için halen sadece BS 7799-2 sertifikası verilmektedir. ISO 17799 bir referans standardı olarak kullanılmaktadır. ISO 17799-2 standardı ile ilgili çalışmalar halen yürütülmektedir. Sertifikaya temel teşkil eden BS 7799-2:2002 standardının Ek-A bölümünde 10 ana başlık altında 36 konu ve toplam 127 güvenlik kriteri sorgulanmaktadır. Ek-B bölümünde Standard için kullanma kılavuzu, Ek-C bölümünde ise, ISO9001, ISO14001 ve BS 7799-2 başlıklarının karşılaştırması verilmiştir.

2002 yılında değişikliğe uğrayan BS7799-2'de en göze çarpan özellik diğer yönetim sistemi standartlarında (ISO 9001, ISO14001) olduğu gibi "Planla - Uygula - Kontrol et - Önlem al" PUKÖ döngüsünün (PDCA Model: Plan-Do-Check-Act) sisteme entegre edilmiş olmasıdır. Şirketlerde Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulmasına yönelik olarak dört temel özelliği içeren bu tür bir yönetim sisteminin temel adımları aşağıda sıralanmıştır:

Planlama kapsamında :

- BGYS kapsamının belirlenmesi,
- BGYS politikasının belirlenmesi,
- Risklerin azaltılması için gerekli kontrollerin belirlenmesi,
- Uygunluk beyanının (Statement of Applicability) hazırlanması,

Uygulama safhasında :

- Risk azaltma planının oluşturulması,
- Riskleri azaltıcı çalışmaların başlatılması,
- Hedeflere ulaşmak için belirlenmiş kontrollerin yapılması,

Kontrol kapsamında :

- BGYS etkinliğinin periyodik olarak gözden geçirilmesi,
- Artık ve kabul edilebilir risk seviyelerinin gözden geçirilmesi,
- Planlanan periyotlarda dahili BGYS denetimlerinin yürütülmesi,

Önlem alma safhasında :

- Belirlenen geliştirmelerin uygulanması,
- Uygun düzeltici ve önleyici çalışmaların yapılması,
- Kontrol sonuçlarını ve düzeltici faaliyetleri tüm ilgili taraflara bildirilmesi,
- Sürekli gelişmenin sağlanması,[36]

gerekmektedir.

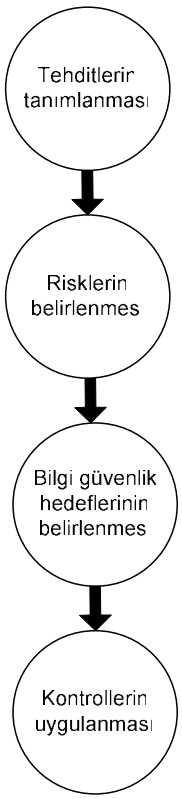
2.6. İşletmede Bilgi Güvenlik Yönetim Sistemi Süreci

Temel olarak, Bilgi Güvenlik Yönetim Sistemi dört aşamadan oluşmaktadır. Bu süreç şirket bilgi kaynaklarına saldırıda bulunabilecek tehditlerin belirlenmesi, tehditlerin yükleyebileceği risklerin belirlenmesi, bilgi güvenlik hedeflerinin oluşturulması ve risklere karşı kontrollerin uygulamasını kapsar. Tehditler mutlaka kontrol edilmesi gerekli riskleri ortaya çıkarır. Bu riskler şirketin bilgi kaynaklarına zarar vermeden ortadan kaldırılması yada azaltılmasına yönelik risk yönetimi uygulanmasını gerektirir. Bilgi Güvenlik Yönetim Sistemi kurulumuna yönelik süreçler Şekil 10'da sıralanmıştır.[37]

---

[36] Altay Onur, Bilgi Güvenliği Yönetim Sistemleri Standartları, (Şubat 2006), http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=583

[37] Raymond ve diğerleri, a.g.e., s.208-222.



Şekil 10. Bilgi Güvenlik Yönetim Sistemi Süreci
Reymond ve diğerleri, s.212.

Kurumsal ölçekte bilişim güvenliğinin sağlanması, teknik bir problem olmanın yanında, yönetimsel bir problemdir. Bilişim güvenliğini sağlamaya yönelik tedbirler, teknolojiler, bunların kurum içinde kullanımı, işletilecek süreçler ve bunların sahipleri gibi pek çok konuda kalıcı ve etkin kararların verilmesi, bu karar ve bilgilerin belgelerle desteklenmesi ve konunun bir yaşam döngüsü bakış açısıyla canlı tutulması gereklidir. Bu amaçla çeşitli standartların oluşturulması ve uygulanması bir yöntem olarak benimsenmiştir.[38]

2.7. ISO 17799 Standardı

ISO 17799 ve buna bağlı BS7799 hiçbir zaman ISO 15408 (Common Criteria) veya CASPR (Commnonly Accepted Security Practices) gibi teknik bir standart olarak tasarlanmamış , her sektördeki şirketin kolayca uygulayabileceği

[38] Bilişim Güvenliği (Oracle Türkiye: Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.48.

bilginin korunması için gerekli esnek ve genel prensipleri oluşturmak amacı ile geliştirilmiştir.

ISO 17799 standardı bilgi güvenlik yönetiminin verimli gerçekleştirilmesi için yayınlanmıştır. Teknik bir standart olmamasına rağmen, ISO17799 bir şirketin güvenlik gereksinimlerini tanımlar ancak gerçekleştirme şeklini şirketlere bırakmaktadır. Diğer bir deyimle, şirket içi ve dışı yanlış ve kötü amaçlı kullanımına karşı bilginin korunması için gerekli beklentileri ve işlemleri tanımlamaktadır.

ISO 17799 standardında aşağıda genel kapsamı verilen 10 alan kapsanmaktadır. Bunlar, güvenlik politikası, organizasyon güvenliği, varlıkların sınıflandırılması/denetimi, personel güvenliği, fiziksel/çevresel güvenlik, iletişim yönetimi, erişim kontrol, sistem geliştirme, iş süreklilik yönetimi ve uyumluluk olarak sıralanabilir.

2.7.1. Güvenlik Politikası

Güvenlik politikası, şirket yönetimin destek ve katkıları ile güvenlik beklentilerinin karşılaması için gerekli güvenlik işlemlerini içeren, uyarlanmış kurallardır.

2.7.2. Organizasyon Güvenliği

Organizasyon güvenliği, güvenliğin koordine edilmesi, güvenlik yönetim sorumlulukların atanması ve güvenlik tehlikesi olaylarında takip edilecek işlemleri de kapsamak üzere bir güvenlik yönetim alt yapısının oluşturulmasıdır.

2.7.3. Varlıkların Sınıflandırılması ve Denetimi

Varlıkların sınıflandırılması ve denetimi, şirkete ait detaylı bilgi alt yapı envanterinin çıkarılıp değerlendirilmesi ve bilgi varlıklarının en uygun güvenlik sınıfına atanması işlemleridir.

2.7.4. Personel Güvenliği

Personel güvenliği, insan kaynakları ve iş süreçleri açısından güvenliğin önemli bir bileşen olarak ele alınmasıdır. Şirket çalışanlarının (Bilişim elemanları ve son kullanıcılar da dahil) görevlerine güvenlik beklentilerinin tanımlanması, işe alınmadan önceki personel araştırmaları, güvenlik kritik işlemlerde gizlilik anlaşmalarının devreye alınması, güvenlik olaylarının personel tarafından raporlanması gibi bir dizi konu içerir.

2.7.5. Fiziksel ve Çevresel Güvenlik

Fiziksel ve çevresel güvenlik, bilişim alt yapısı, bina ve çalışanların korunmasını sağlayan güvenlik politikasının tanımlanmasıdır. Kapsamında, binaya giriş, yedekli güç kaynağına sahip olma, periyodik bilgisayar bakımı ve bina dışında bilişim kaynaklarının barındırılması gibi konular vardır.

2.7.6. İletişim ve Operasyon Yönetimi

İletişim ve operasyon yönetimi, güvenlik olaylarının önlenmesini sağlayan anti virüs koruma, günlük alma ve izlenmesi, güvenli uzaktan erişim, güvenlik olay takip sistemin devreye alınması gibi güvenlik önlemlerini içerir.

2.7.7. Erişim Kontrol

Erişim kontrolü, parola yönetimi, kimlik denetimi, günlük alma yöntemleri ile ağ ve uygulama kaynaklarına olabilecek iç ve dış saldırılara karşı korunma beklentilerini kapsar.

2.7.8. Sistem Geliştirme ve Bakım

Sistem geliştirme ve bakım faaliyetleri, yazılım geliştirme ve bakım süreçlerinde güvenliğin ele alınması ve mevcut uygulamaların güvenli olarak bakımının sağlanması beklentilerini içerir.

2.7.9. İş Süreklilik Yönetimi

İş süreklilik yönetimi, doğal veya insan temelli felaketlerde şirket operasyonlarının sürekliliğinin sağlanması için gerekli planların yapılması faaliyetlerini içerir.

2.7.10. Uyumluluk

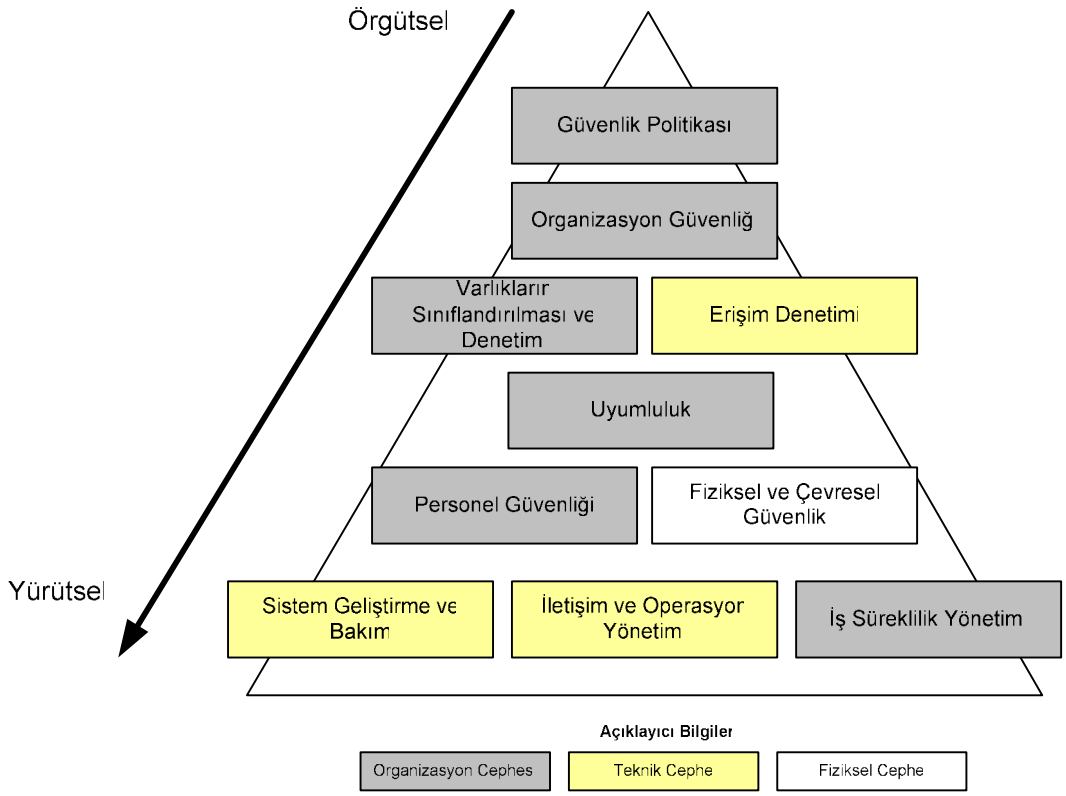
Uyumluluk, şirketin bağlı olduğu güvenlikle ilgili kanun ve yönetmeliklere uyumlu olması için gerekli kontrolleri kapsar.[39]

Şekil 11'de bu 10 alanın standart yapılanması görülmektedir. Her bir alan, yukarıdan aşağıya, ayrı başlıklar altında, yönetsel, teknik ve fiziksel önlemler ile ilgili bilgiler içerir. Başka bir deyişle, yönetsel seviyeden yürütsel seviyeye kadar faaliyetleri kapsar.[40]

---

[39] ISO17799 Güvenlik Danışmanlığı, (Şubat 2006), http://www.innova.com.tr/04Hizmetler/detayli_bilgi02.htm,

[40] Bisson Jacquelin, René Saint-Germain, The BS 7799 / ISO 17799 Standard, White Paper, (Şubat 2006), https://www.callio.com/files/wp_iso_en.pdf



Şekil 11. ISO 17799 Standardının Kapsamı

https://www.callio.com/files/wp_iso_en.pdf , Şubat 2006

17 Ocak 2006 tarihi itibarı ile halen dünyada 2017 adet işletme ISO 17799-2 standardına (ISO 27001) göre başarıyla tetkikten geçerek akredite edilmiş kurumlarca sertifikalandırılmıştır. Bunların ülkelere göre dağılımı Tablo 2'de sunulmuştur.[41]

[41] ISMS Journal (Issue 6, The ISMS International User Group: Jan 2006)

Tablo 2. ISO 17799-2 Sertifikasyonu Alan İşletme Sayılarının Ülkelere Göre Dağılımı (17 Ocak 2006 tarihli)

Japonya	1190	Çek Cumhuriyeti	6	Bahreyn	1
İngiltere	219	Brezilya	5	Şili	1
Hindistan	139	Yunanistan	5	Mısır	1
Tayvan	69	İspanya	5	Fransa	1
Almanya	51	Türkiye	5	Lübnan	1
İtalya	41	Hırvatistan	4	Litnanya	1
Kore	35	İzlanda	4	Lüksemburg	1
ABD	31	Filipinler	4	Macau	1
Macaristan	24	Suudi Arabistan	4	Makedonya	1
Hollanda	22	Arjantin	3	Fas	1
Çin	21	Kuveyt	3	Yeni Zelanda	1
Hong Kong	20	Meksika	3	Katar	1
Avusturalya	18	BAE	3	Romanya	1
Finlandiya	15	Belçika	2	Rusya	1
İsviçre	13	Kanada	2	Slovenya	1
İrlanda	11	Kolombiya	2	Tayland	1
Norveç	11	Danimarka	2	Sırbistan	1
Singapur	11	Isla of Man	2		
Avusturya	9	Malezya	2		
Polonya	7	Slovakya	2		
İsveç	7	Güney Afrika	2		

Humphreys, Jan 2006, s.18.

İKİNCİ BÖLÜM

BİLGİ GÜVENLİK SİSTEMİNDE RİSK YÖNETİMİ

1. RİSK YÖNETİM KAVRAMLARI VE BİLGİ GÜVENLİK YÖNETİM SİSTEMİ İLE İLİŞKİSİ

Günümüz toplumlarının günlük yaşamlarında vazgeçilmez bir unsur olmaya başlayan bilişim teknolojileri, yeni ekonomi ve yönetim modellerinin önemli işlem araçları olmuştur. Bilgi ve iletişim teknolojileri alanındaki gelişmeler ile çeşitlenmeler her geçen gün konunun önemini daha da artırmakta, daha kaliteli, sürekli ve güvenilir hizmetlerin sağlanmasını gerektirmektedir.

Kaliteli, sürekli ve güvenilir hizmetlerin sağlanması için amaca yönelik stratejik hedeflerin belirlenmesi bu hedeflere göre de süreçlerin iyi yönetilmesi kaçınılmaz hale gelmektedir. Kurumların temel stratejilerini gerçekleştirebilmesi için bilgi işlem sistemleri ile bilgi işlem çalışanlarının rolleri son derece kritik bir hale gelmiş, kurumların bilgi işlem platformlarının çalışabilirliği ("availability"), platformlar üzerinde işlenen bilginin doğruluğu ("accuracy"), bütünlüğü ("integrity") ve sürekliliği ("continuity") gittikçe önem kazanmaktadır.

Bu nedenle küreselleşen dünyada, bilişim teknolojileri gittikçe önemli hale gelerek, paylaşılan doğru bilgi bir "değer" ve gelişim için kullanılan en önemli "meta" haline gelmiştir. Kurumların bu alanda çalışabilirliğini etkileyecek, hizmetlerini aksatacak ve güvenilirliğini zedeleyecek faktörlerin belirlenerek, yönetilmesi de kaçınılmaz olmuştur. Bu yaklaşım sonucunda da "Risk Yönetimi" kavramı ortaya çıkmıştır.[42]

Risk yönetimi uygulamalarının etkin ve verimli sonuçlanması için öncelikle risk yönetiminin genel yapısının ve kavramlarının incelenmesi ve Bilgi Güvenlik Yönetim Sistemi ile ilişkisinin ortaya konması gerekmektedir. Bu nedenle risk yönetim modelinin incelenmesinden önce risk yönetiminin genel yapısı, kavramlar ve BGYS ile ilişkisi açıklanmıştır.

---

[42] M. Okay, A.Pekel, O.Yaman, D. Soyar , N. Kuleyın, A. Mete, Bilişim Teknolojilerinde Risk Yönetimi, Kamu Bilişim Platformu, (20 Mart 2006), http://kamubib.tbd.org.tr/dokumanlar/cg2.doc

1.1. Risk Yönetiminin Konusu

Bütün girişimler çeşitli riskler taşır. Örneğin, dünyayı büyük oranda etkileyen güncel risklerden bazıları şu şekilde sıralanabilir:

-Teknolojik riske örnek olarak Çernobil reaktör patlaması,

-Ulaşım riskine örnek olarak Challenger mekiğinin düşüşü,

-Ekonomik riske örnek olarak New York Borsası çöküşü,

-Sağlık riskine örnek olarak AIDS veya sıtma,

-Ekolojik riske örnek olarak Aral gölünün kuruması, Exxon Valdez, Tropik ormanların yok oluşu, ozon tabakasının delinmesi, sera etkisi,

-Doğal risklere örnek olarak depremler, yanardağ patlamaları, hortumlar, vs.

Bu tür olaylar giderek daha sık gerçekleşmekte ve gerçekleştiklerinde de sonuçları az veya çok felaket olmaktadır. Bu durum doğal olarak riski iki boyutlu bir büyüklük (olasılık ve sonuçlar) şeklinde dikkate almaya yönlendirmektedir.[43]

Günlük yaşantımızda ve işimizde verdiğimiz kararların çoğu risk içerir. Örneğin, bir iş seyahatine havayolu ya da karayolu ile gitme kararını verirken, zaman ve maliyet faktörleri kolaylıkla değerlendirilebilir, ancak emniyet faktörü ve toplantıya zamanında yetişebilme olasılığı çok daha karmaşık olabilir. Hangi ulaşım şeklinin daha emniyetli olduğunun değerlendirilmesinde, elde edilebiliyorsa geçmiş istatistiksel veriler incelenir (örneğin, 1000 km başına kaza sayısı). Toplantıya zamanında ulaşılabilirlik için, havayolu ve karayolu koşulları değerlendirilmelidir. Riskin incelendiği durum karmaşıklaştıkça, kriterler arttıkça, karar verme karmaşıklaşır. Örnekte, toplantıya geç kalmak kabul edilemez bir risk iken, fiyatın yüksek olması kabul edilebilir bir risktir. Emniyet riski de, kabul edilemez bir risktir.

İşletmelerin başarıları, problemleri oluşmadan önleyebilmeleri ile doğrudan ilişkilidir. Problemlerin, oluşmadan önce çok daha erken aşamalarda, öngörülerek ortadan kaldırılması gerekir. Öngörülebilen potansiyel problemler ya da riskler, mercek altına alınarak, kuruluşun ya da programın başarısına olumsuz etkileri en aza indirgenmelidir. Risklerin öngörülmesi ve azaltılması çalışmaları, yalnızca problemlerin oluşmadan önlenmesini sağlamakla kalmayıp, önemli fırsatları da yakalama olanağı sunacaktır. Risk yönetimi ile iki önemli fayda elde edilecektir. Birinci fayda,

[43] A.Leroy , J.Pierre Sıgnoret, Teknolojik Risk (İletişim Yayınları,1994), s.16.

problemleri oluşmadan önleyerek ya da sonuca olumsuz etkilerini en aza indirgeyerek performans ve maliyet hedeflerine ulaşmaktır. İkincisi ise, büyük risklerin temel nedenleri belirlenerek önleme çalışmaları ile yüksek kazançlara ulaşmaktır. Örneğin, yeni teknoloji kullanılması kararı önemli ölçüde risk almayı gerektirirken, rekabetçi bir ürünle pazara hakim olmayı ve büyük fırsatları da getirecektir. Yüksek riskli kararlar, risklerin iyi yönetilmemesi durumunda önemli kayıplara neden olabilecektir. Bu yol, keskin bir bıçak sırtı gibidir.

Riskin incelendiği durum karmaşıklaştıkça, kriterler arttıkça, karar verme daha da güçleşir. Karar verme mekanizmalarının çoğu, karar verme sürecinde başlangıç noktası olarak sezgi ve yargılarını kullanırlar; önemli riskleri içeren kararlarda, yargı yada sezginin ötesine gidebilmek, ancak risk yönetiminin sistematik olarak uygulanması ile mümkündür. Riskin kritiklik derecesi ve sonuca etkisi belirlenmelidir. Risk tüm işin aksamasına neden olacaksa, kabul edilmemeli ve riskleri zararsız hale getirecek ya da tamamı ile ortadan kaldıracak risk azaltma planları ya da önlem planları geliştirilmelidir.

Yaşamın ve evrenin doğasında, bilinmeyenlerden kaynaklanan riskler her zaman olacaktır. Önemli olan bu risklerin olabileceğini görmek, kabullenmek ve olumsuz etkilere karşı önlemler geliştirmektir. Bilinmeyen her zaman bizi gelecekte olumsuz bir yöne doğru götürmeyecektir, diğer bir deyişle fırsatlara da gebedir. Riskin olumsuz yanına, gereğinden fazla odaklanmak, moral ve motivasyonu olumsuz yönde etkileyerek, cesaret kırıcı ve karar vermekten kaçınmak gibi istenmeyen davranış biçimlerine neden olabilecektir. Risk yönetim felsefesi, risklerden korkmak ve kaçmaktan çok, risklerin bilinçli bir şekilde alınması ve etkin bir şekilde yönetilmesi yönünde geliştirilmelidir.[44]

1.2. Risk Yönetimi Kavramları

Geleceğe ilişkin olaylar hakkında yeterli bilgiye sahip olmadan karar vermek zordur. Karar verilse dahi, o kararın yanlış olma olasılığı yüksektir. O açıdan karar noktasındaki birey veya bireylerin, zaman içinde şartların değişebileceğinin sonuçlarının da buna bağlı olarak farklı durumlar olabileceğinin bilincine varması

[44] Meryem Fıkırkoca, Bütünsel Risk Yönetimi (Ankara: Pozatif Matbaacılık, 2003), s.13-24.

gerekir. Karar organları gelecekle ilgili kararları verirken, karar sürecinde önemli bir yere sahip olan risk ve belirsizlik faktörleri ile karşı karşıya kalırlar. Bu faktörler, kısa dönem kararlarında olduğu gibi uzun dönemde de etkilidir. Risk ve belirsizlik, gelecekteki olayların nasıl gelişeceğini ifade etmekteyse de, risk durumunda gelecekteki olayların ortaya çıkma olasılıkları gerçeğe yakın olarak tahmin edilebilirken, belirsizlik durumunda hiçbir şekilde tahmin edilememektedir.[45]

Risk yönetim faaliyetlerinin, etkin bir şekilde yürütülebilmesi için de risk yönetimi ile ilişkili kavramların iyi anlaşılması gerekir. Bu nedenle aşağıda risk yönetimi ile ilgili bazı önemli kavramlara kısaca değinmekte yarar vardır:

Risk Kavramı: Risk, bir olay ve onun sonuçlarına ilişkin olasılıklar kombinasyonu olarak tanımlanmaktadır. Genellikle risk terimi sadece en az bir olumsuz sonuç ihtimali bulunduğu bir durumda kullanılmaktadır. Bazı durumlarda "risk" beklenen sonuçtan veya olaylardan sapma olasılığından kaynaklanmaktadır.[46]

İtalyanca'sı "risco" Almanca'sı "risiko", İngilizce'si "risk"olan bu kavram dilimiz de önceleri riziko olarak kullanılmış daha sonra risk olarak yerleşmiştir. Zarar veya kayıp durumuna yol açabilecek bir olayın ortaya çıkma olasılığı anlamına gelmektedir. Tehlike ile eş anlamlı ve ileride ortaya çıkması beklenen ama meydana gelip gelmeyeceği kesin olarak bilinmeyen olaylar için kullanılmaktadır. Ayrıca gelecek ile ilgili bir kavram, çünkü gelecek belirsizlik ifade etmektedir. [47]

Risk, en basit koşullarda bazı uygun olan ve uygun olmayan olayların meydana gelme şansı olarak da tanımlanmaktadır. Burada üzerinde durulması gereken nokta, çok sayıda gözleme dayanarak örgüt açısından ortaya çıkabilecek kayıpların belirlenmesidir. Riskler, daha çok örgüt çevresinden kaynaklanmaktadır. Bazen çevrede değişimler ve işletme yöneticisinin deneyim ve düşünceleri arasında farklılıklar olabilir. Bu farkın derecesi önemlidir. Çünkü bazen öyle olur ki insanlar doğru bildikleri şekilde hareket etmelerinden dolayı işletmeyi zarara uğratabilirler. Bunun için yönetici, olabilecek risklere karşı kendi düşüncelerini doğru yönde kullanmalıdır.[48]

---

[45] Cevat Elma, Kamile Demir,Yönetimde Çağdaş Yaklaşımlar (Ankara: Anı Yayıncılık, 2000), s.243.
[46] TS ISO/IEC GUIDE 73, Risk Yönetimi- Terim ve Tarifler (Ankara: Türk Standardları Enstitüsü, 2005)
[47] Atilla Filiz, Risk Yönetimi, (05 Mart 2006), http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=638
[48] Cevat Elma, Kamile Demir,Yönetimde Çağdaş Yaklaşımlar (Ankara: Anı Yayıncılık, 2000),, s.243.

Riskin iki temel bileşeni vardır:

- Belirli bir sonuca ulaşamama olasılığı ya da istenmeyen bir olayın oluşma olasılığı (olasılık)
- Sonuca ulaşamama olasılığı ya da riskin oluşması durumunda sonuca etkisi (etki)

Riskin matematik ifadesi ise:

$$Risk = f(olasılık, etki)$$[49]

Risklerin bir kısmı ölçülebilmekte ve dolayısı ile sigorta edilebilmektedir. Yangın, sel, hırsızlık ve kazalar, ölüm gibi durumlar birer risk örneğidir. Bu tür durumlara karşı yönetici önceden gerekli tedbirleri almalıdır.[50]

Ancak riski uygun ölçemeyen şirketler, korumacı ve emniyet marjı ile hareket etmeye başlarlar. Aşağıda verilen Şekil 12 risk ölçümünün önemini vurgulamak üzerine gösterilmiş olup, buzdağlarının yapısı örneğinde olduğu gibi sadece suyun üzerindeki görünen yüzeye bakarak buzdağının geneli hakkında karar verilmemesi, suyun altında kalan kısmının da incelenmesi gereklidir.

Şekil 12. Risk Ölçümünün Önemi

Uz, 2004, s.24.

Sonuç: Sonuç, bir olayın neticesi olarak tanımlanmaktadır. Bir olaydan birden fazla sonuç çıkabilir. Sonuçlar nitel veya nicel olarak ifade edilebileceği gibi, olumludan olumsuza doğru sıralanabilir. Ancak, sonuçlar güvenlik yönünden daima olumsuzdur.

---

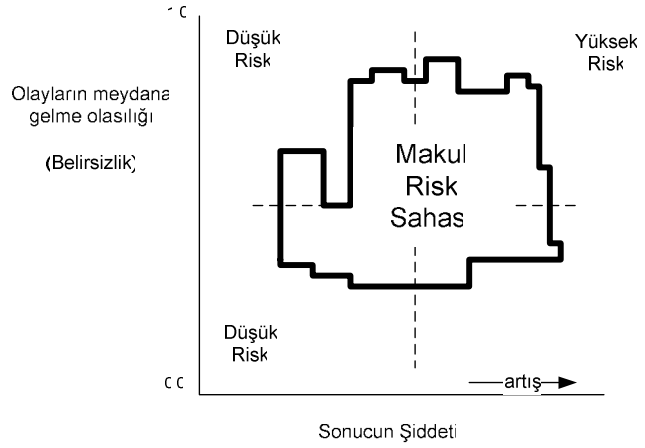
[49] Fıkırkoca, a.g.e., s.25.
[50] Cevat ve diğerleri, a.g.e., s.244.

Olasılık (Belirsizlik): Olasılık, bir olayın oluşma ihtimali olarak tarif edilmektedir. Olasılık, matematiksel olarak 0 - 1 aralığında rasgele olayın oluşumuyla ilişkilendirilen pozitif bir sayıdır. Olasılık, meydana gelecek bir olaya inanma derecesi ya da çok sayıda tekrarlanan olaylarda, olayın göreceli oluşma sıklığı olarak ifade edilebilir. Yüksek derecede inanma durumunda olasılık 1'e yaklaşır.[51]

Olasılık geleceğin neler getireceğinin bilinmemesi anlamına da gelmektedir. Kısaca olasılık, önceden kestirilemeyen olaylar olarak tanımlanabilir. Meydana gelebilecek olaylar hakkında bir olasılığın saptanamaması, olasılığı riskten ayırtan önemli bir faktördür.[52]

Risk ve olasılık çoğunlukla birbirinin yerine, yerleri değiştirilerek kullanılır. Fakat risk ve olasılık aynı şey değildir. Bu yüzden riskli parçanın doğru olarak anlaşılıp anlaşılmadığı, olayın meydana gelme veya meydana gelmemesinin sonuçlarının potansiyel etkilerinin anlaşılması şarttır. Şekil 13'te bu kavram gösterilmiştir.[53]

Riski tanımlamada olasılıktan daha çok sıklık kullanılabilir. Olasılığa inanma dereceleri aşağıdaki gibi ifade edilmektedir: Nadiren / beklenmeyen /orta dereceli / beklenen / hemen hemen kesin / İnanılmaz / ihtimal dışı / çok uzak / ara sıra olan / muhtemel / sık sık.[54]



Şekil 13. Olayların Meydana Gelme Olasılığı

Yılmaz, 2003, s.56

[51] TS ISO/IEC GUIDE 73, Risk Yönetimi- Terim ve Tarifler (Ankara: Türk Standardları Enstitüsü, 2005)
[52] Cevat ve diğerleri, a.g.e., s.248.
[53] Ayşe Küçük Yılmaz, Havacılıkta Emniyet Açısından Risk Yönetimi ve Havacılık Örgütlerinden Uygulama Örnekleri, (Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, 2003), s.55.
[54] TS ISO/IEC GUIDE 73, Risk Yönetimi- Terim ve Tarifler (Ankara: Türk Standardları Enstitüsü, 2005)

Şiddet: Riskin verebileceği zarar derecesidir.

Tehlike: Tehlike ise, kurum yada insanların yaralanması, hastalanması, zarar görmesi veya bunların bileşimi olabilecek zarar potansiyeli olan durumdur.[55] Bunlar, maddeler veya makineler, çalışma metotları, iş organizasyonunun diğer konuları olabilirler. [56]

Risk Kriterleri: Riskin önemini değerlendirme kuralları olarak ifade edilmektedir. Risk kriterleri, ilgili fayda ve maliyetleri, yasal ve hukuki gerekleri, sosyo-ekonomik ve çevre boyutunu, çıkar grupları kaygılarını, değerlendirilecek öncelikleri ve diğer girdileri içermektedir.[57]

Risk Yönetimi: Risk yönetimi, kuruluşun kayıplarını en aza indirebilmesini ve fırsatların en üst düzeyde değerlendirebilmesini mümkün kılacak ve en maliyet etkin biçimde risklerin içeriğini ve etkilerini belirleyen, tanımlayan, analiz eden, değerlendiren, muamele eden, izleyen ve iletişimini yapan görevlere yönetim politikalarının, prosedürlerin ve yaklaşımların sistematik biçimde uygulanmasıdır.[58]

Çıkar Grupları: Riski etkileyen, riskten etkilenen veya kendini etkilenmiş gibi algılayan kişi, grup veya kuruluş.

İlgili Taraf: Bir kuruluşun başarısından veya performansından fayda sağlayan kişi ya da grup "ilgili taraf" olarak tanımlanır. Örnek olarak, müşteriler, kuruluşun sahipleri, kuruluştaki kişiler, tedarikçiler, bankacılar, sendikalar, ortaklar veya toplum sayılabilir. Ayrıca bir grup, bir kuruluştan, kuruluşun bir parçasından veya birden fazla kuruluştan oluşabilir.

Risk Algılama: Bir çıkar grubunun değer ve kaygı temeline dayalı olarak bir riske bakış şekli olarak ifade edilmektedir. Risk algılama, çıkar grubunun ihtiyaçlarına, bilgisine ve risk konularına bağlı olduğu gibi objektif verilere göre değişebilmektedir.

---

[55] Atilla Filiz, Risk Yönetimi, (05 Mart 2006), http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=638
[56] http://isggm.calisma.gov.tr/docs/sunumlar/18.hafta/6May2004/8, (27 Ocak 2006)
[57] TS ISO/IEC GUIDE 73, Risk Yönetimi- Terim ve Tarifler (Ankara: Türk Standardları Enstitüsü, 2005)
[58] TS IEC 62198, Proje Risk Yönetimi (Ankara: Türk Standardları Enstitüsü, 2003)

Risk İletişimi: Riske ilişkin bilgilerin karar verici ve diğer çıkar grupları arasında değişimi veya paylaşımı, risk iletişimi olarak adlandırılır. Söz konusu bilgiler, riskin mevcudiyeti, yapısı, şekli, olasılığı, şiddeti, kabul edilebilirliği, risk muamelesi ve diğer boyutlarıyla ilgili olabilmektedir.

Arta Kalan Risk: Güvenlik önlemlerini uyguladıktan sonra kalan riskler olarak ifade edilmektedir.[59]

1.3. Risk Gruplandırma

Belirsizlik ve karmaşıklığın arttığı pazar koşullarında, kuruluşların rekabet edebilirliğinin ve sürekliliğinin sağlamasında önemli riskler vardır. Proje yönetimlerinin, bir ürünü belirlenmiş bir performans, maliyet ve zamanda teslim edebilmesinde her zaman riskler içerir. Teknolojik yenilik politikalarında rakibinden geri kalan bir kuruluş, her zaman pazarı ve işini kaybetme riski ile karşı karşıyadır. Bir ürünün performansı, hedeflenen değerlere ulaşamayabilir, gerçekleşen maliyet planlanandan yüksek olabilir ya da ürün müşteriye zamanında teslim edilemeyebilir.

Riskler yönetilebilir parçalara ayrılmalıdır. Riskler kaynağına bağlı olarak başlıca üç alanda gruplandırılır:

-Teknik

-Takvim

-Maliyet

Risk alanları, birbiri ile etkileşim içerisindedir. Bu etkileşim çoğu zaman kuvvetlidir. Risk alanları arasındaki etkileşim ve bu etkileşimin düzeyi, risk analizlerinde incelenmesi gereken kritik konulardandır. Risk alanları arasındaki etkileşim, risk olaylarını daha karmaşık hale getireceğinden, risklerin yönetimini daha önemli kılar.

---

[59]Gürsoy DURMUŞ, Risk Analizi (Mart 2006), http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/Riskanal.pdf

1.3.1. Teknik Risk

Teknik riskler hedeflenen performans değerine ulaşamamanın bir ölçüsüdür. Teknolojinin çok hızlı ilerlemesi ile, kuruluşların ürünlerini sürekli iyileştirmeleri, yenilikçi ve buluş niteliğinde ürünler ortaya çıkarabilmeleri daha önemli hale gelirken, teknik riskler de artmıştır. Teknik risk, yeni tasarımda, ARGE ve geliştirme projelerinde daha çok önem kazanır. Yeni bir tasarımla önceki performansın üzerine çıkmak konusunda, çok sayıda kısıtla karşılaşılabilir. Teknik riskler, teknolojik, performans, tasarım, idame konulardaki riskleri içerir.[60]

Teknik riskleri dikkate almak başlıca şu yararları sağlar:[61]

-Teknoloji, önerilen programın tüm amaçlarını karşılayabilecek seviyede olup olmadığını,

-Performans, program kapsamındaki her bir ihtiyacın veya temel ihtiyaçların, ürünün testi sonunda karşılanıp karşılanmadığını,

-Tasarım, program mühendislik amaçlarına mevcut teknoloji, tasarım araçları ve tasarım olgunluğu ile ulaşıp ulaşamadığını,

-İdame, program lojistik amaçlarının sistem tasarım ve bakım ihtiyaçları doğrultusunda giderilip giderilmediğini.

1.3.2. Takvim Riski

Takvim riski, çizelgelenen sürelerin aşılma olasılığının bir ölçüsüdür. Çizelgeleme sürecinde, bir işin ne zaman bitirileceğine ilişkin zaman tahminlerinin doğru yapılabilmesi için, bu işle ilgili ölçümlerin olması gerekir. Ölçümlere dayalı olmayan, öznel yönü ağır basan tahminler, çoğu zaman yetersiz olacaktır. Takvim risklerinin yönetilmesinde temel alınan tahminlerin doğruluğu, risk yönetiminin etkinliğini doğrudan etkileyecektir. Tahminlerdeki belirsizliğin fazla olması, tahminlerin elverişli olmaması projenin yanlış yönlendirilmesi sonucuna götürecektir. Bir iş için tahmin edilen bitirme süresinin gereğinden uzun olması, fazla kaynak ayrılmasına, kaynak israfına neden olacaktır.

---

[60] Fıkırkoca, a.g.e., s.40.
[61] Edmund H. Conrow, Effective Risk Management (AIAA, 2003), s.23.

1.3.3. Maliyet Riski

Maliyet riski, planlanan maliyetin aşılmasının bir ölçüsünü verir. Ekonomik güçlükler, kuruluşun yönetiminde kaos ve belirsizliği arttırır. Ekonomik koşullardaki belirsizlikler, yöneticilerin baş etmesi gereken önemli risk kaynaklarındandır. Maliyet riski, tahmin edilenle, gerçekleşen maliyet değerleri arasındaki değişkenliğin ölçüsü ile belirlenir. Ekonomik belirsizlikler, maliyet değişkenliğini ve riskleri artırır. Maliyet riskleri şu nedenlerle oluşur:

-Maliyet tahminindeki yetersizlikler

-Programın maliyet hedefini karşılayacak şekilde yönetilmemesi

-Teknik, takvim, destek ve programla ilgili risklerin etkin bir şekilde çözümlenmemesi.

Maliyet tahminleri yapılırken, ürünün yaşam çevrim maliyeti dikkate alınmalıdır. Yöneticiler, aldıkları kararların çoğunda, belli ölçüde risk üstlenirler, alınan kararla ilgili olarak, ilerleyen aşamalarda problem çıkması durumunda, sorunu ortadan kaldırmak için yönetim rezervi ayrılmalıdır. Ölçülemeyen hata maliyetleri için, bütçeleme sırasında belli bir pay ayrılmalıdır.[62]

1.4. Risk Yönetiminin Bilgi Güvenlik Sisteminde Uygulanma Gereksinimi

Bilgi sistemleri güvenliğinin önem kazanmaya başladığı günlerde, tüm açıklıkların kapatılması güvenlik programlarının ana hedefi idi. Tüm açıklıkları kapatmanın mümkün olmadığı ve alınan güvenlik önlemlerinin ciddi maliyetleri olduğu fark edildikçe bu yaklaşımdan vazgeçildi. Üzerinde çalışılacak olan açıklıklarının önceliklerinin belirlenmesi, eldeki kaynakların verimli kullanılması ve güvenlik maliyetlerinin dengelenmesi amacıyla risk yönetimi anlayışı benimsenmiştir.[63]

Teknolojinin hızlı gelişmesi, ürün ve hizmetlerdeki çeşitliliğin artması, iş süreçlerinin buna bağlı olarak karmaşıklaşması sistem ya da sistemler üzerindeki kontrolü zorlaştırmaktadır. Bunun sonucunda hata ve dolandırıcılığa karşı tedbirlerin önceden alınması zorunlu hale gelmektedir. O nedenle, kurum ve kuruluşlar olası bir zarara karşı gerekli altyapı yatırımlarını önceden yapmış olmalıdır.

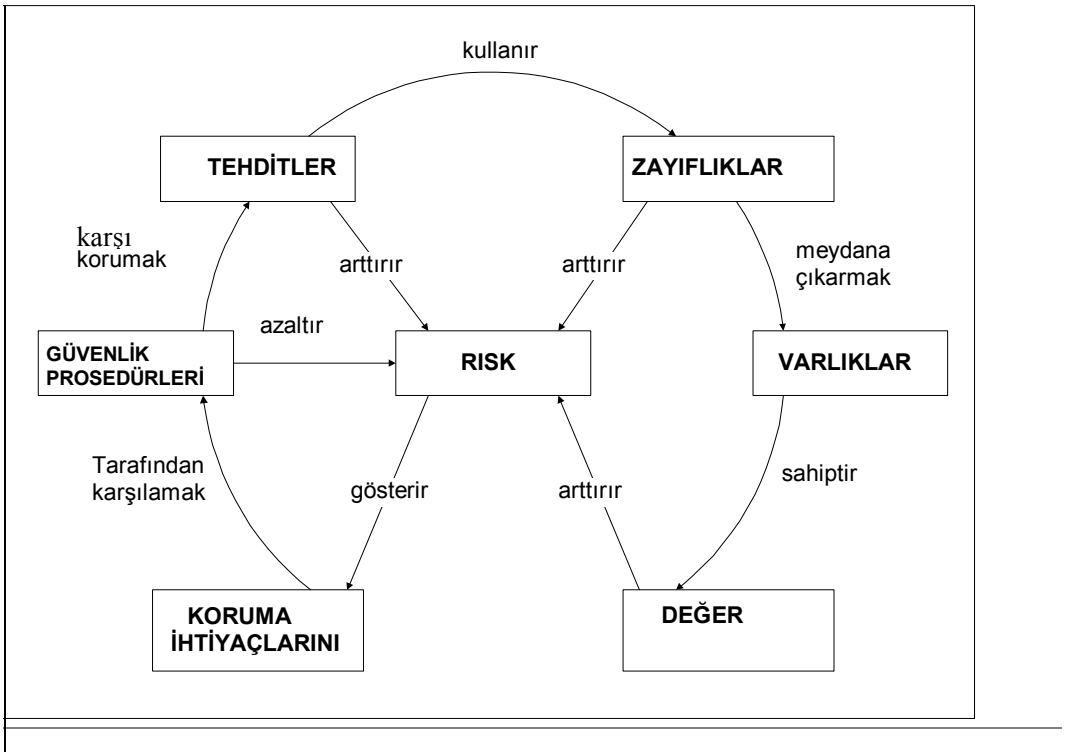
---

[62] Fıkırkoca, a.g.e., s.41-43.

[63] http://www.uekae.tubitak.gov.tr/OKTEMWeb/Baglantilar/2-RiskYonetimi.htm

Bugün Bilişim Teknolojilerine dayalı süreçler, artık kurum ve kuruluşlar için, varlıklarını devam ettirebilmeleri açısından vazgeçilmezler arasında önemli bir yer tutmaktadır. Bilişim Teknolojilerine dayalı iş süreçlerinin herhangi bir sebeple olumsuz yönde etkilenmesi aynı zamanda kurum ya da kuruluşların asli fonksiyonlarını devam ettirememesi anlamına gelmektedir.[64]

Şekil 14'te bilgi güvenlik ile risk yönetimi arasındaki ilişkiler gösterilmiştir. Örnek verecek olursak, tehditler riski arttırırken, güvenlik prosedürleri riski azaltır.



Şekil 14. Bilgi Güvenlik ile Risk Yönetimi Arasındaki İlişkiler

ISO/IEC TR 13335-1, Part 1, 1996

[64] M. Okay, A.Pekel, O.Yaman, D. Soyar , N. Kuleyın, A. Mete, Bilişim Teknolojilerinde Risk Yönetimi, Kamu Bilişim Platformu, (20 Mart 2006), http://kamubib.tbd.org.tr/dokumanlar/cg2.doc

2. RİSK YÖNETİM MODELİ

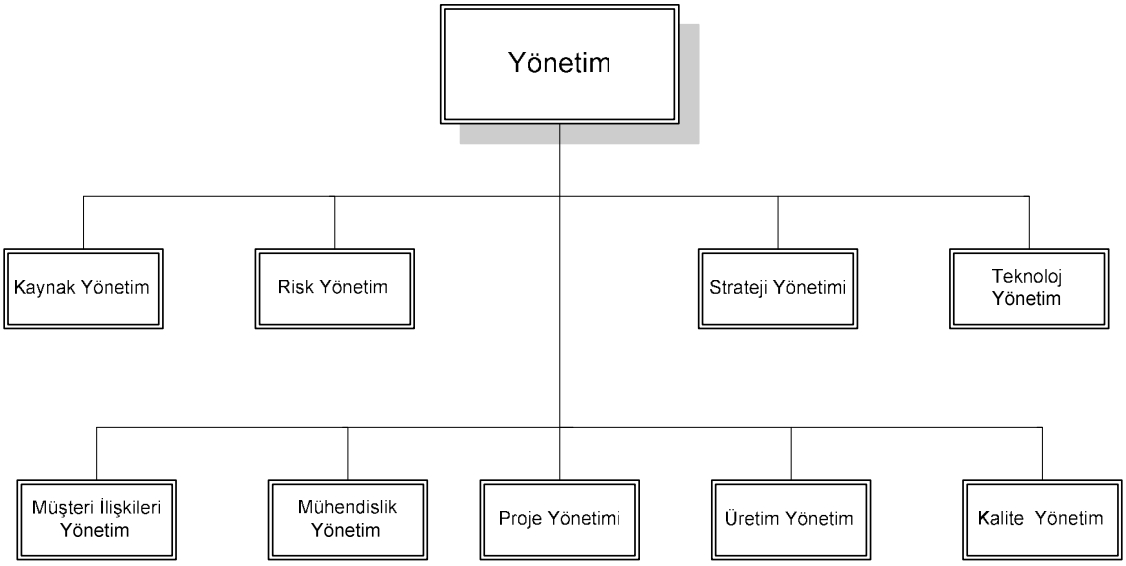
Risk yönetimi, işi başında ve ilk seferde doğru yapmak ilkesinin yaşama geçirilmesini sağlayan kritik bir disiplindir. Risklerin problem olarak karşımıza çıkmasını önlemenin maliyeti, problem haline dönüştükten sonraki düzeltme maliyetinden çok daha düşük olacaktır. Riski önlemenin maliyeti performans, maliyet ve zaman olarak çok daha fazlası ile geri dönecektir. Risk yönetim disiplini, işin başında, sürekli olarak uygulandığında program kaynaklarının etkin bir şekilde kullanılması için uygun bir ortam sağlayacaktır.

Risk yönetiminin, kuruluşun işleyen yönetim sistemi içine enjekte edilmesi zor bir faaliyettir; çünkü çoğu zaman kültür ve çalışma şeklinin değiştirilmesini gerektirir. Risk yönetim yaklaşımları, kuruluş yönetim yaklaşımına ileri, geniş ve önleyici bir yaklaşımı enjekte edecektir. Performans mükemmelliği yolunda, kaçınılmaz bir disiplin olan risk yönetimi, yalnızca müşteriye sunulan ürünle ilgili risklerin en aza indirgenmesi yaklaşımı ile değil, kuruluşun performans göstergelerinin de olumlu yönde gelişmesini sağlayacak şekilde uygulanmalıdır. Bu da risk yönetiminin kuruluş ya da projedeki tüm yönetim disiplinleri ile entegre olarak ele alınması gerekliliğini açığa çıkarır.

2.1. Risk Yönetim Yaklaşımı

Risk yönetimi başlı başına bir yönetim disiplinidir. Risk yönetimi, ne kalite yönetiminin ne de proje yönetiminin faaliyetlerinden biridir. Risk yönetimi ayrı bir disiplindir, ancak tüm yönetim disiplinlerinde olduğu gibi, tek başına ve bağımsız olarak uygulanması da pek mümkün değildir. Risk yönetimine, proje yönetiminde kullanılan bir teknik olarak bakılması risk yönetimi ile sağlanacak kazançları azaltacaktır. Risk yönetiminin başlı başına bir disiplin olarak ele alınması, risk kültürünün, stratejisinin, prosedürlerinin, planlarının geliştirilmesini, sorumlulukların, yetkilerin ve nasıl bir organizasyonla yürütüleceğinin, süreçlerin net bir şekilde tanımlanmasını sağlayacaktır. Diğer ilişkili yönetim disiplinlerle bir bütün olarak uygulanması sonucunda, tekrarlayan faaliyet ve süreçlerin ortadan kaldırılması sağlanarak, yönetimin etkinliğini arttırılır. İşletmelerdeki yönetim süreçleri Şekil 15'te sunulmuş olup, buradan da anlaşılacağı gibi, risk yönetim süreci, işletmenin diğer

süreçleri ile bir bütün olarak tanımlanmalı, yöntem ve sorumluluklar belirlenmeli, prosedür haline getirilmelidir.



Şekil 15. Yönetim Süreçleri

Fıkırkoca, 2003, s.142.

2.1.1. Risk Kültürü

Etkin bir risk yönetimi için çok boyutlu düşünme kültürü geliştirilmeli, farklılıklar ve riskler fırsata dönüştürülmelidir.

Kuruluşlarda, her düzeydeki çalışan, verdiği kararlarda, değişen belirsizlik ölçüsünde risk alır. Verilen her kararda, alınan riskler, yeni fırsatlar da içerir. Karar verirken, riskleri ve yaratılabilecek fırsatları öngörebilmek gerekir. Risk almamak, fırsatları da kaçırmayı beraberinde getirecektir.

Kurum kültürü ve risk kültürü birbirini desteklemelidir. Risk alma konusunda, teşvik edici bir ortam oluşturulmalıdır. Alınan risklerin büyüklüğü karar verme düzeyine bağlı olarak değişir. Riskler bilinçli, verilere dayalı ve riskle baş edebilme yeteneği ölçüsünde alınmalıdır. Risk yönetimi, korkuya dayalı olmayan, motive edici, teşvik edici bir çalışma ortamı gerektirir. Riskler açık bir şekilde tartışılabilmeli ve riskleri azaltıcı yaratıcı düşünceleri harekete geçiren bir ortam yaratılmalıdır.

Risk kültürü, pozitif ve öncel bir yaklaşıma dayalı olmalıdır. Riskin olumsuz yönüne gereğinden fazla odaklanılmamalıdır. Riskler öncel olarak; olumsuz etkisini en

aza indirgemeye, yeni fırsatları yaratabilmeye izin veren en erken aşamada belirlenerek yönetilmelidir.[65]

2.1.2. Risk Stratejisi

Risk yönetiminin etkinliği, üst yönetim tarafından taahhüt edilen, tanımlı, prosedür halini almış bir risk stratejisinin varlığı ve bu stratejinin, kuruluştaki tüm faaliyetlere indirgenmesi ile doğrudan ilişkilidir. Risk yönetim stratejisinin önemli bir özelliği, risk yönetimi ve diğer faaliyetler arasındaki ilişkilerin kurulmasının bir yolunu oluşturmasıdır. Projenin başında oluşturulmalıdır ve her temel karar noktasında gözden geçirilmelidir.

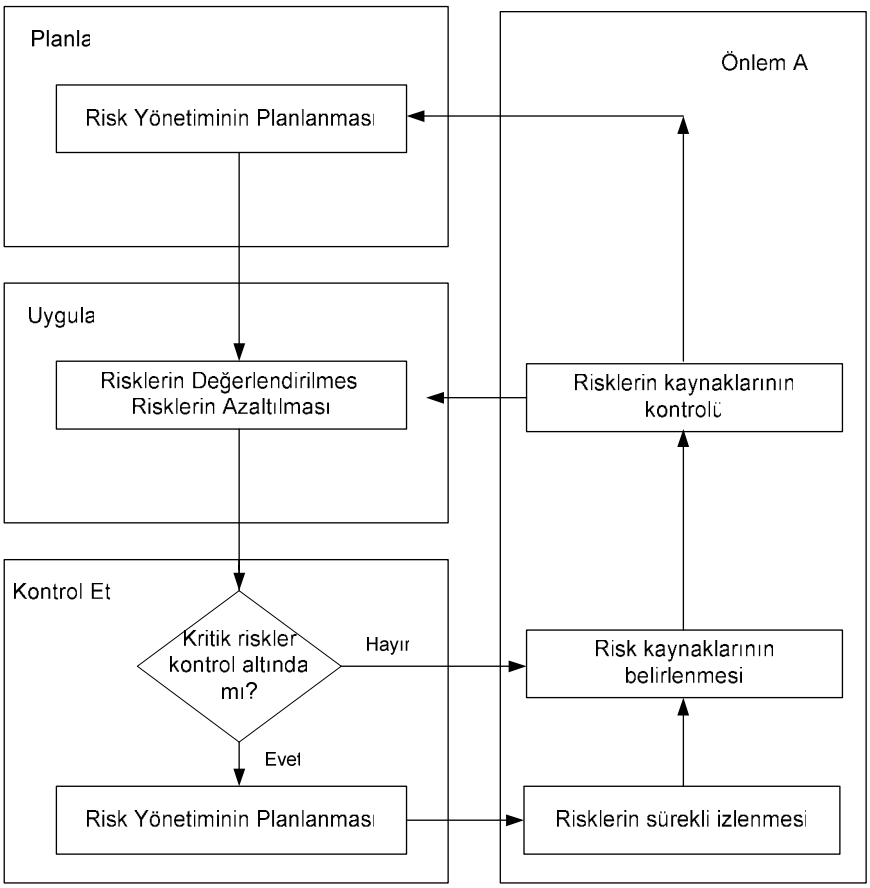
Organizasyon düzeyinde geliştirilen ve prosedür halini almış risk stratejisi, proje düzeyindeki risk stratejilerinin belirlenmesinde temel oluşturur. Risk stratejisi, risk süreçlerinin organizasyon düzeyinde tanımlanması, proje yönetimlerine uyarlanması için bir temel sağlar ve yön verir. İlk olarak, konsept geliştirme aşamasında belirlenen risk yönetim stratejisi, program tedarik stratejisi, kuruluş stratejisi ile tutarlı olmalıdır. Strateji geliştirilirken, gerek ve tehditler, sistem ve projenin özellikleri göz önünde bulundurulur. Risk stratejisi, projelere ve kuruluştaki tüm süreçlere uyarlanmalı ve konuşlandırılmalıdır.

2.1.3. Risk Yönetim İlkeleri

Risk yönetiminin etkin bir şekilde uygulanması ve kuruluşun rekabet üstünlüğüne olumlu yönde katkılar sağlaması için aşağıdaki ilkeler temel alınmalıdır:

Sürekli yönetim: Risk yönetimi, yalnızca belirli zaman aralıklarında ya da programın belirli aşamalarında uygulanan bir disiplin değildir. Yaşam çevrimi boyunca sürekli bir şekilde uygulanmalıdır.

[65] Fıkırkoca, a.g.e., s.46.



Şekil 16. Risk Yönetiminde PUKÖ Çevrimi

Fıkırkoca, 2003, s.59.

Risklerin etkin bir şekilde en aza indirgenebilmesi için PUKÖ (Planla-Uygula-Kontrol et-Önlem al) yaklaşımı kullanılmalıdır. Bu çevrimde risk yönetim faaliyetlerinin uyarlanması Şekil 16'da sunulmuş olup buna göre; "Planlama" safhasında, risk yönetim faaliyetlerinin planlaması, "Uygulama" kısmında, risklerin değerlendirmesi ve azaltılması faaliyetleri, "Kontrol Et" safhasında risk azaltma faaliyetlerinin etkinliğinin izlenmesi, "Önlem Al" bölümünde ise sürekli bir faaliyet olarak risk azaltma faaliyetlerinin etkinliğini arttıracak önlemler alınır.

Entegre Yaklaşım: Risk yönetimi, tek başına uygulanacak bir disiplin değildir. Risk yönetimi, kuruluştaki tüm süreçlere, disiplinlere entegre olarak uygulanmalıdır. Tüm süreç ve faaliyetlere entegre edilen risk yönetim süreç ve faaliyetleri tanımlanmış,

görünür, yönetilebilir ve etkinliği izlenebilir olmalıdır. Risk yönetimi planlama, organizasyon, kontrol, koordinasyon ve yönlendirme fonksiyonlarının doğal bir parçası olmalıdır. Başka bir deyişle, risk yönetimi iyi yönetimin ayrılmaz bir parçasıdır.

Süreç Yaklaşımı: Risk yönetimi, riskleri sistematik olarak belirleyen, değerlendiren, azaltan ve izleyen, yapılandırılmış bir dizi süreçle yürütülmelidir.

Yapılandırılmış bir süreç, programın karmaşıklığını ve belirsizliğini azaltacaktır, risklerin daha iyi yönetilmesini sağlayacaktır. Kaynaklar ve faaliyetler, bir süreç olarak yönetildiğinde, risk yönetiminden beklenen sonuçlar, daha etkin olarak elde edilebilecektir. Süreç yaklaşımı sonucunda aşağıdaki faaliyetler belirlenir:

-İstenilen sonuca ulaşmak için süreçler tanımlanır,

-Süreçlerin girdi ve çıktıları belirlenir ve ölçülür,

-Kuruluşun işlevlerinin süreçler ile arayüzleri belirlenir,

-Müşteri, donatıcı ve diğer süreç paydaşları ile birlikte süreçlerin olası riskleri, sonuçları ve etkileri değerlendirilir,

-Süreçlerin yönetimi için yetki ve sorumlulukları net olarak tanımlanır,

-Süreçlerin iç ve dış müşterileri, donatıcıları,

-Diğer paydaşları belirlenir.

Sistem Yaklaşımı: Sistem yaklaşımında bileşenlerden, parçalardan çok, onlar arasındaki ilişkiye odaklanılır. Parçalar arasındaki ilişkilerin anlaşılması ile bütünü bir arada görebilme yeteneği kazanılır. Sistem yaklaşımında, bir sistem kendisini meydana getiren parçaların toplamından daha büyüktür. Sisteme, özelliklerini, parçalardan çok, parçalar arasındaki ilişki kazandırır. Bu ilişkilerdeki basit bir değişiklik bile, sonuçlarda önemli değişikliklere neden olabilir. Risk yönetiminin sistem yaklaşımı ile ele alınması, bu ilişkilerdeki risklerin belirlenmesini önemli kılar.

Etkin bir risk yönetiminde sistem yaklaşımı, birbiriyle ilişkili risk yönetim süreçlerinin oluşturduğu sistemin tanımlanması, anlaşılması ve yönetilmesi olarak tanımlanır.

Son yıllarda, süreç yaklaşımının önem kazanması ile sistem yaklaşımında aksaklıklar olmaktadır. Süreçlerin önemli olduğu bir gerçektir, ancak süreçler arasındaki ilişki üzerinde duran sistem yaklaşımı da süreç yaklaşımını bütünleyen bir düşüncedir.[66]

2.2. Risk Yönetim Süreçleri

Günümüz yönetim disiplinleri, süreç ve sistem yaklaşımı ile ele alınır. Etkin bir risk yönetiminin de sistem ve süreçlere dayalı bir yaklaşımla yürütülmesi gerekir. Risk yönetiminin süreçlere dayalı bir yaklaşım ile uygulanabilmesi için, süreçler tanımlı hale getirilmeli ve yapılandırılmalıdır. Risk yönetim süreçleri arasındaki etkileşimin tanımlanması, görünür kılınması, geribildirim mekanizmalarının kurulması ile risk yönetiminde sistem yaklaşımı gerçekleştirilecektir.

Ürün yaşam çevrimi boyunca uygulanacak olan risk yönetim süreçlerinin, işletmedeki tüm ürün yaşam çevrim süreçleri ile bir bütün olarak tanımlanması gerekir. Günümüz yönetim yaklaşımlarında, süreçlere odaklanmanın yeterli olmadığı, süreçlerle birlikte, süreçler arasındaki etkileşimlere de önem vermek gerektiği anlaşılmıştır. Bu nedenle, etkin bir risk yönetim sistemi için, süreçlerin tanımlanması ile birlikte, risk yönetim süreçlerinin kendi içerisinde ve diğer süreçlerle ilişkisinin net olarak anlaşılması, tanımlanması ve prosedür haline gelmesi gerekmektedir.[67]

İşletilebilir bir risk yönetim modelinin Şekil 17'deki yapıyı içermesi gerekmektedir. Bu modelde risk yönetimi dört temel süreçten oluşmaktadır:

-Risk planlama,

-Risk değerlendirme,

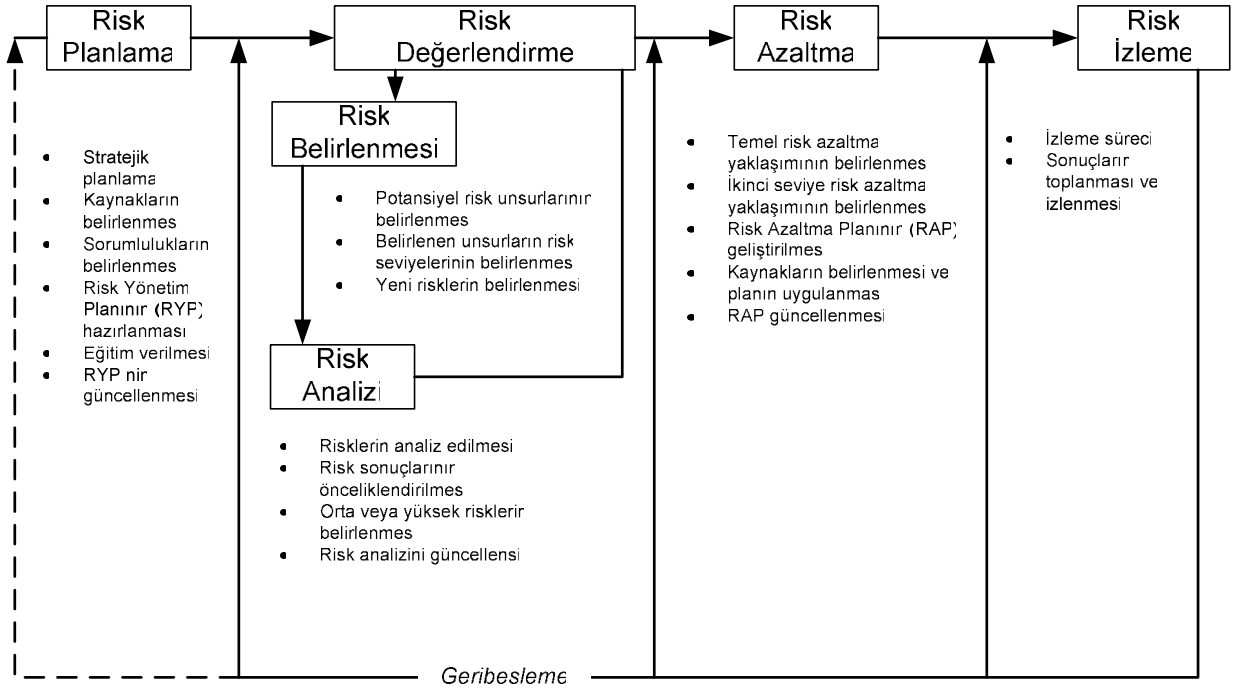
-Risk azaltma,

-Risk izleme.

---

[66] Fıkırkoca, a.g.e., s.50-54.

[67] Fıkırkoca, a.g.e., s.139.



Şekil 17. Risk Yönetim Süreci

Conrow, 2003, s.44.

Risk yönetim süreci, risk yönetim planının hazırlanması ile başlar, risklerin belirlenmesi, analizi, önceliklendirmesi, azaltılması ve izlenmesi faaliyetleri ile devam eder. Risk yönetim faaliyetlerinin akış şeması Şekil 16.'da sunulmuştur.

Risk planlama sürecinin çıktısı olarak doküman haline getirilecek planlar, en tehlikeli risklere öncelik verilerek, riskli durumları kabul edilebilir bir düzeye indirgeyecek faaliyetleri içerir. Planlarda risk azaltma hedefleri verilir. Risklerin, risk yönetim faaliyetleri yürütülmesine karşın problem olarak ortaya çıkma olasılığına karşı önlem planları geliştirilir.

Risk izleme sürecinde risk verileri toplanır, risk azaltma ve yönetim faaliyetlerinin etkinliği değerlendirilir, belirlenmiş zamanlarda risk durum raporları hazırlanır. Her risk için durum raporu analiz edilerek, yürütülen risk azaltma faaliyetinin etkinliği değerlendirilir. Bu değerlendirme sonucunda aşağıdaki kararlar verilir:

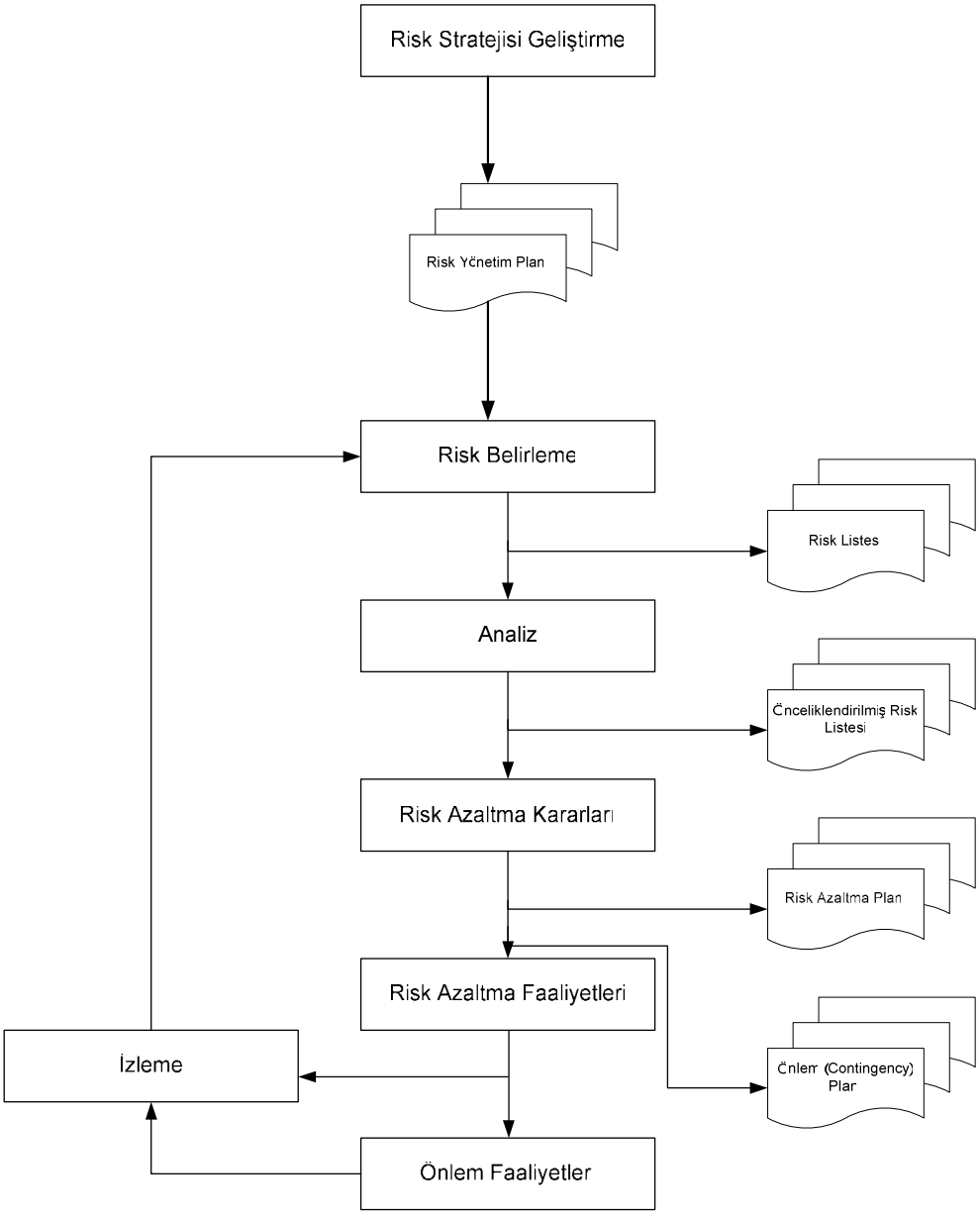
-Yeniden planlama,

-Riski kapatma,

-Önlem planının devreye alınması,

-Yürürlükteki planın uygulanması ve izlenmesi.

Risk yönetim süreci, proje yönetim sürecinin bir parçası olmalıdır. Geri bildirim mekanizması kurulmalı, proje risk listesi ve risk yönetim planı yaşayan bir doküman olarak tutulmalıdır. [68]



Şekil 18. Risk Yönetim Akış Şeması

Fıkırkoca, 2003, s.148.

[68] Fıkırkoca, a.g.e., s.147.

2.2.1. Risk Planlama

Bir organizasyonda risk yönetim disiplini kapsamında dört temel düzeyde planlama yapılır;

- Organizasyon düzeyinde
- Program düzeyi
- İş düzeyi
- Faaliyet düzeyi

Organizasyon düzeyinde planlama için en kritik olan stratejik planlamadır. Kuruluşun stratejilerinin belirlenmesi ve planlanmasında, risk yönetim disiplininden elde edilen veriler çok önemlidir. Bu nedenle, planlama bir program yöneticisinin birinci ve en kritik görevidir. Risk planlama süreci de, program yönetim fonksiyonlarından biri olan risk yönetiminin sistematik ve disiplinli bir şekilde uygulanmasında temel bir süreçtir.

Planlama faaliyeti, süreç odaklı yürütülmeli ve planlama süreci iği izlenmeli ve sürekli iyileştirilmelidir. Planlamanın başarısı, planlama sürecinin etkin olarak işletilmesine bağlıdır.

Program risk planlama ile organizasyon düzeyindeki risk yönetim süreçleri, program risk stratejisini yansıtacak şekilde, programın gereklerine uygun olarak programa uyarlanır.

Risk planlama sürecinin temel hedefi, risklerin sonuç üzerinde yaratabileceği tehlike düzeyine bağlı olarak, risk azaltma hedeflerinin ve faaliyetlerinin belirlenmesidir. Riskin problem haline dönüşme olasılığı hesaplanmalı yada problem oluştuğunda yürütülecek önlem faaliyetleri belirlenmelidir. Risk yönetim sürecinin etkinliğinin izlenebilmesi için verilerin nasıl toplanacağı, nasıl değerlendirileceği, geri bildirimin nasıl yapılacağı planlama sürecinde belirlenmesi gereken temel faaliyetlerdendir.

Risk yönetiminin nasıl, ne zaman ve kimler tarafından yönetileceği planlarda anlatılır. Risk planlama sürecinin çıktısı olarak, risk planları hazırlanır. Programın karmaşıklığına, kapsamına ve içerdiği risklere bağlı olarak planlama süreci ve çıktıları tanımlanır. Risk planlama süreci çıktıları, program boyunca risklerin nasıl yönetileceğini anlatan "Risk Yönetim Planı", risk azaltma kararı verildiğinde azaltma

faaliyetlerinin nasıl yönetileceğini anlatan “Risk Azaltma Planları” ve risklerin problem haline dönüşmesi durumunda neler yapılacağını anlatan “Önlem Plan”dır.

Planlar, program risk stratejisi doğrultusunda, risklerin belirlenmesini, nicelenmesini, önceliklendirilmesini, önceliklere bağlı olarak kaynakların planlanmasını, risk kararlarının alınmasını, risk azaltma faaliyetlerinin nasıl yürütüleceğini, risk yönetiminin etkinliğinin nasıl izleneceğini ve geri bildirim mekanizmalarını anlatır. Bu faaliyetlerinin en etkin bir şekilde planlanması, risk yönetiminin etkinliğini belirleyen faktörlerden biridir.

Planlama sürecinin etkinliği, planların tam, doğru ve erken bir zamanda yapılmasının yanı sıra, planlara uygun çalışılmasına bağlıdır. Program yönetimi boyunca, planların yaşayan ve uygulanan dokümanlar olmasının sağlanması kritiktir. Çalışmanın bu aşamasında risk planlama süreci ve risk yönetim planlarına kısaca değinilecektir.

2.2.1.1. Risk Planlama Süreci

Risk planlama sürecinde, tedarik stratejisinin anlaşılması ile işe başlanır, tedarik stratejisi ve program yönetim planı ile tutarlı bir risk stratejisi geliştirilir.

Risk planlama süreci, konsept geliştirme ile başlar ve programın ilerleyen aşamalarında, tüm risk faaliyetlerinde risk yönetim planı temel olarak alınır, plan gözden geçirilir ve güncellenir.

Risk yönetiminden sorumlu kişi, program düzeyi bir risk yönetim ekibi ile koordineli olarak, Proje Yönetim Kılavuzuna dayanarak, risk yönetim planını geliştirir. Risk planlama sürecinin sahibi risk koordinatörü, program yöneticisi ya da program risk yönetim ekibi olabilir. Etkin olmak için, risk yönetimi program yönetiminin önemli bir fonksiyonu olarak ele alınmalı ve risk yönetim planı çalışmalarına program yöneticisi aktif olarak katılmalıdır. Planlama esasen, tüm program yönetim ofisinin ve yüklenici ekibinin aktif katılımını gerektirir.

Planlama süreci, risk yönetim stratejisinin geliştirilmesi ve dokümantasyonu ile başlar. Hedef ve amaçlar, belirli alanlardaki sorumluluklar, teknik uzmanlık gereksinimleri belirlenir; incelenecek alanlar ve değerlendirme süreci anlatılır. Risk azaltma seçeneklerini inceleme yöntemleri, risk derecelendirme şeması oluşturulur.

Raporlama ve dokümantasyon yöntemi, izleme metrikleri belirlenir. Risk planlama sürecinin çıktısı risk yönetim planı, risk azaltma planı ve önlem planıdır.

2.2.1.2. Risk Yönetim Planları

Risk planlama sürecinin çıktısı olarak üç tür plan hazırlanır:

-Risk Yönetim Planı

-Risk Azaltma Planları

-Önlem Planları

Risk yönetiminde hazırlanan planlar, tedarikçi ve yükleniciye risklerin en aza indirgenmesinde bir yol haritası oluşturur. İyi hazırlanmış planlar, program ekibinin riskleri yönetmek için gereksinim duyduğu, tüm bilgileri içerir.

2.2.1.2.1. Risk Yönetim Planı

Risk yönetim planında, risk yönetimi yaklaşım ve süreçleri, proje gereksinimlerine uygun olarak, projenin diğer planlan ile uyumlu olacak şekilde tanımlanır. Projenin boyutuna, karmaşıklığına ve risklerin düzeyine bağlı olarak, proje yönetim planının bir parçası olarak ya da aynı bir plan olarak hazırlanabilir. Risk yönetim planı, projenin ömrü boyunca, riskin nasıl yönetileceğini detaylı olarak anlatmalıdır. Risk yönetim planı, üst yönetim tarafından onaylanan resmi bir dokümandır. Yeni bir durum ya da bilgi edinildiğinde, risk yönetim planlan güncellenir. İzleme sonucunda, yeni riskler belirlenebilir ya da riskler kapatılabilir. Buna göre risk yönetim planı güncellenir. Risk yönetim planının etkin bir şekilde uygulanabilmesi ilgili kişilerin yeterli bilgi, beceri ve eğitilmiş olmalarına bağlıdır.

2.2.1.2.2. Risk Azaltma Planı

Risk azaltma planında, risklerin tanımlanması, oluşma olasılığı ve sonuca etkilerini en az indirgemek amacıyla yürütülmesi gereken faaliyetler, bu faaliyetlerin ne zaman ve kimler tarafından yürütüleceği, risk azaltma planının kapatma yöntemi anlatılır.

Risk azaltma planlarında seçilen her faaliyet, programdaki sorumlulukları, işleri, takvimi etkileyeceğinden, program planları ile uyumlu hale getirilmelidir. Risk azaltma faaliyetleri, maliyet tahminleri ile entegre edilmelidir. Proje çizelgeleri, risk azaltma

planlarına göre güncellenmelidir. Örneğin, yeni geliştirilen bir sistemde, bir risk azaltma önlemi olarak, prototip oluşturmaya karar verilebilir. Bu yeni işin proje planlarına, takvimlere, maliyet tahminlerine yansıtılması gerekir.

2.2.1.2.3. Risk Önlem Planına

Risk azaltma faaliyeti hemen yürütülemiyorsa ya da bu faaliyetler riski azaltıyor, ancak tamamen ortadan kaldırmıyorsa, risk önlem planı geliştirilir. Önlem planı, yalnızca risk probleme dönüştüğü zaman uygulanır. Önlem plan örnekleri, felaket iyileştirme planları, personel elverişli değilse, danışman ya da dış uzmanlara başvurma ya da alternatif bir tasarım yaklaşımının seçimini içerebilir.

Önlem planı olan her risk, ayrıca bir de tetikleyiciye sahiptir. Tetikleyici, gelecekte riskin probleme dönüşmesinin en erken aşamadaki göstergesidir. Örneğin, risk kritik bir personelin elverişliliği ile ilgili ise, gerçekleşen ve planlanan beceri düzeyi arasındaki değişkenliğin %l0'dan fazla olması bir tetikleyicidir. Öncelikli riskler için belirlenen tetikleyiciler, risk göstergeleri olarak göz önüne alınmalıdır. Öncelikli olmayan riskler için tetikleyici belirlenmesine gerek olmayabilir, ancak öncelikli riskler için tetikleyicilerin belirlenerek, riskin erken aşamada tespit edilmesi gerekir.[69]

2.2.2. Risk Değerlendirme

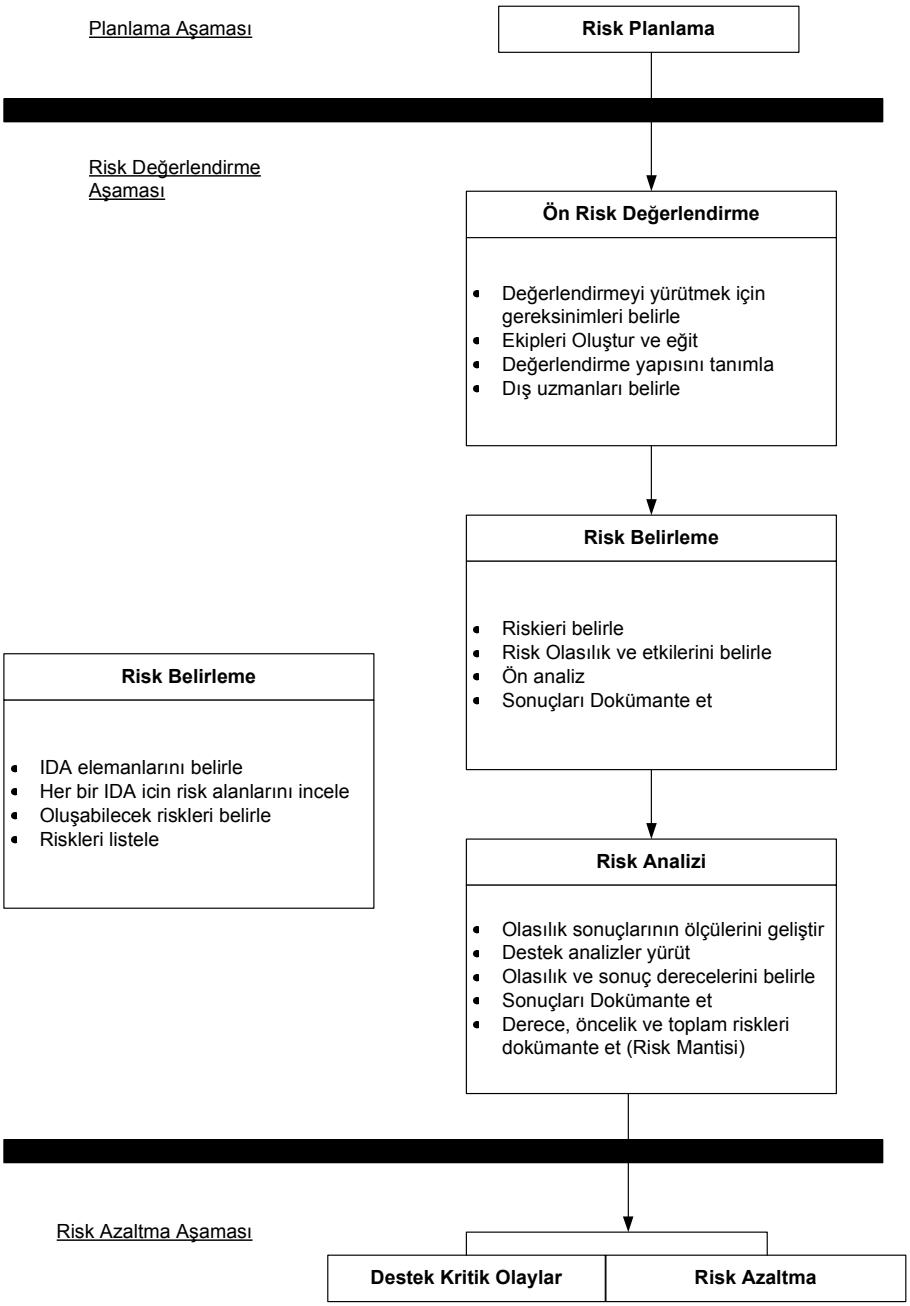
Risk değerlendirme, risk yönetiminin en önem1i ve karmaşık faaliyetlerini içerir. Risk değerlendirme yeteneği, organizasyon ya da program yönetiminin başarısında kritiktir.

Risk değerlendirmenin esas amacı, risklerin en kritik olanlarını öncelikle kontrol altına alabilmek için riskleri ve büyüklüklerini belirlemektir. Etkin bir risk yönetiminde, yalnızca oluşabilecek risklerin belirlenerek, sonuca etkilerinin en aza indirgenmeye ça1ışılması yeterli değildir. Belirlenen risklerin oluşma olasılığının ve projenin başarısını ne derece etkileyebileceğinin yapılan analizlerle ortaya konulması gerekmektedir. Bu analizler sonucunda, risklerin kritiklik derecesi hesaplanarak, öncelikle en kritik olanların azaltılması planlanmalıdır. Kritik risklerin doğru belirlenmesi, etkin bir risk yönetiminin can damarıdır. Değerlendirme sonuçları maliyet,

[69] Fıkırkoca, a.g.e., s.161-170.

takvim, performans hedeflerinin kurulmasında göz önüne alınan faktörlerdir; çünkü onlar istenilen çıktılara ulaşma olasılığının göstergeleridir. Hedef değerler belirlenirken, onlara ulaşma konusundaki riskler göz önüne alınmalıdır. Risklerin gerçeğe yakın olarak belirlenmesi, hedeflerin doğru belirlenmesini etkileyen önemli bir faktördür.

Riskleri değerlendirmek için, her programa ya da kuruluşa uyan standart bir süreç yoktur; kullanılan tekniğe, program aşamasına ve programın yapısına göre değişik yöntemler uygulanabilir. Bununla birlikte temel faaliyetler, bütün risk değerlendirme yaklaşımlarında ortaktır. Risk değerlendirmenin yürütülmesinde, genel bir yaklaşım Şekil 19'da gösterilmiştir.



Şekil 19. Risk Değerlendirme Süreci

Fıkırkoca, 2003, s.185.

Programın herhangi bir aşamasında karşı1aşı1acak tüm riskler ayrıştırılarak ayrıntılı bir şekilde analiz edilir. Program riskleri maliyet, takvim ve teknik olarak ayrıştırılır. Değerlendirme sonucunda, bulunan tüm riskler toplanarak program riskleri bulunur.

Ayrıştırma ile, riskler kapsamlı ve ayrıntılı bir şekilde belirlenirken, aralarındaki etkileşim de görünür hale getirilir. Risklerin doğru ve ayrıntılı belirlenmesi, aralarındaki etkileşimin net bir şekilde resmedilmesi, riskleri doğurabilecek temel nedenlerin belirlenmesine, ortadan kaldırılmasına olanak sağlayacaktır.

Risk değerlendirme sürecinde, İş Dağı1ım Ağacını (İDA) temel olarak almak en uygun yaklaşımdır. Programla ilgili riskler, İDA temel alınarak belirlenir. İDA 'daki her ürün ve işle ilgili olası riskler öngörülür. İDA 'daki her ürün ve süreç bileşeni için risk alanları ya da risk kaynakları incelenerek riskli durumlar belirlenir. Her bir İDA bileşeni için belirlenen risklerin oluşma olası1ığı ve sonuca etkisinin büyüklüğü belirlenir. Her bir İDA bileşeni için risk derecesi belirlenir. İDA bileşenleri için belirlenen riskler toplanarak program toplam riski bulunur.

Risk değerlendirme araçlarından/tekniklerinden hiçbiri, her organizasyon, program ya da proje için tam olarak uygun değildir. Uygun araçlar/teknikler kullanılmadığında, risk değerlendirmeden beklenen sonuçlar elde edilemeyecektir. Örneğin, yeterli bilgi birikimi ve deneyime sahip olmayan bir uzman tarafından risklerin değerlendirilmesi sonucunda, belirlenen riskler, tahmin edilen önem dereceleri doğru olamayabilecektir. Buda yanlış konular üzerinde, zaman ve kaynak harcanması sonucuna götürecektir. Yeterli bilgi ve deneyime sahip uzmanların bulunamadığı bir durumda, uzman görüşmesi tekniği uygun değildir. Organizasyon yapısına en uygun risk değerlendirme teknikleri belirlenerek ku1lanılmalıdır. Risklerin değerlendirilmesinde ku1lanılacak tekniklerden bazıları aşağıda verilmiştir:

-Karar matrisleri

-Karar ağaçları

-Risk haritaları

-Risk grafikleri

-FMECA (Hata Türü Etkileri,Kritikliği ve Analizi), FTA (Hata Ağacı Analizi)

-Monte Carlo Simülasyonu

-AHP (Analytic Hierarchy Process)

-SMART (Simple Multi Attribute Rating Technique)

Risk değerlendirme, konsept geliştirme aşamasının son yarısında başlar ve izleyen program aşamaları boyunca sürer. Program yönetimi boyunca, sürekli olarak programın ilerlemesi ile artan bilgi ve detay düzeyine bağlı olarak riskler yeniden

değerlendirilir. Bununla birlikte, olayların gerektirdiği zamanlarda, yeni risk değerlendirmeleri yapılmalıdır (örneğin, tedarik stratejisinde önemli değişiklikler olduğunda, kritik süreçlerde değişiklik olduğunda, ekonomik koşullarda beklenmeyen yönde bir değişme olduğunda v.b.). Program riskleri, belirlenmiş kilometre taşlarında değerlendirilir.[70]

Risk değerlendirmesi, risk seviyesinin kabul edilebilirlik kriteri ile karşılaştırılmasını ve risklerin iyileştirilmesi önceliklerinin tayinini içerir.[71]

2.2.2.1. Risk Değerlendirme Teknikleri

Risk değerlendirme tekniğinin seçiminde şu iki sorunun yanıtı araştırılır:

-Risk değerlendirme nicel (sayısal) mi, yoksa nitel (yüksek, orta, düşük gibi derecelendirme) mi olmalıdır?

-Otomatik gereçler kullanılmalı mıdır?

Nitel risk değerlendirme tekniklerinde, istenmeyen olayların oluşma olasılığı ve sonuca etkileri yüksek, orta ve düşük gibi derecelerle sınıflandırılır. Sonuç üzerinde en fazla etkiye sahip risk senaryolarının geliştirilmesinde kullanılır. Nitel teknikler, elde anlamlı veriler bulunmadığı ve düşük riskli durumlarda kullanışlıdır.

Risk değerlendirmede, kuruluşun ya da projenin yapısına, karmaşıklığına, eldeki kullanılabilir verilere, yönetim yaklaşımlarına bağlı olarak değişik yöntemler kullanılabilir.

Toplama (Aggregation): Toplama yönteminde, ayrı ayrı risk bileşenleri toplanarak toplam risk değeri bulunur. Toplama sırasında aynı alandaki risklerin etkişimine bakılırken, farklı alanlardaki risklerin etkileşimi de dikkate alınmalıdır. Örneğin, bir ürünün maliyet riski değerlendirilirken, malzeme, işçilik, dolaylı maliyet risklerinin derecesi belirlenir ve sonra toplanır. Değerlendirmenin gerçeğe yakınlığı ve değeri toplama derecesinin ters fonksiyonudur. Riski tahmin etme zamanı ve maliyeti, toplama derecesi arttıkça azalır. Risk toplama kriterlerinin ve hedeflerinin doğru belirlenmesi, bu

[70] Fıkırkoca, a.g.e., s.170-189.
[71] TS IEC 62198, Proje Risk Yönetimi-Uygulama Kılavuzu (Ankara: TSE, 2003)

yaklaşımın etkinliğini doğrudan etkiler. Riskler, belli hedefler doğrultusunda be belli sistematikle toplanmalıdır.

Ayrıştırma (Disaggregation): Ayrıştırma, risklerin bileşenlerine ayrıştırılarak değerlendirilmesidir. Riskin bileşenlerine ayrıştırılma derecesi arttıkça, elde edilen sonucun gerçeğe yakınlığı ve değeri artar. Risk ne kadar ayrıntılı olarak ayrıştırılırsa, o kadar gerçeğe yakın bir risk sonucu elde edilir. Riskin bileşenlerine ayrıştırılma derecesi arttıkça, tahmin maliyeti ve zamanı da artacaktır.

Ayrıştırma, risk alanlarına (teknik, maliyet, takvim) göre yapılabilir. Ayrıştırmada deneyim, beyin fırtınası, benzer programlardan çıkartılan dersler ve risk yönetim planı kılavuzluğunda riskler ve kritik riskler belirlenir.

Simülasyon: Belirli değerlerdeki girdilerin çıktıya etkileri gözlenir. En yaygın olanları aşağıda sunulmuştur:

-Olası En Kötü Durum: Girdilerin olası en kötü değerleri seçilerek çıktı değerlerine etkilerine bakılarak riskler değerlendirilir.

-**Deneye Dayalı:** Yaklaşık ya da göz kararı değerler kullanı1arak, deneysel olarak riskler çözümlenir. Bu yaklaşımla elde edilen risk değerinin gerçeğe yakınlığı ve değeri, tahmin zamanı ve maliyeti, yaklaşık değerler elde edilirken temel alınan geçmiş verilere ve toplama derecesine bağlı olarak değişecektir.

-Olasılılığa Dayalı: Olasılığa dayalı yöntemler, en sık kullanılan yöntemlerdir. Riskler olasılıklara dayalı olarak değerlendirilir. Riskin bileşenlerine ayrıştırılma derecesi arttıkça, elde edilen sonucun gerçeğe yakınlığı ve değeri artar. Diğer yaklaşımlardan daha az tahmin zamanı ve maliyeti gerektirir. Riskin büyüklüğünü belirlemek için kullanılan tekniklerin çoğu olasılık kuramına dayanır .Sahip olunan verilere, riske, risk yönetim stratejilerine ve kişisel deneyimlere bağlı olarak aşağıdaki olasılık yaklaşımları kullanılır:

-Analitik

-Geçmiş verilere dayalı

-Öznel ve deneyime dayalı

-**Nedenlere Dayalı Yöntemler (Deterministic):** Risklerin nedenlere dayalı olarak çözümlenmesidir. Nedenlere dayalı yaklaşımla, risklerin değerlendirilmesi

sonucunda elde edilen risk değerinin gerçeğe yakınlığı ve değeri, ayrıştırma derecesinin fonksiyonudur. Diğer yaklaşımlardan daha fazla tahmin zamanı ve maliyeti gerektirir.[72]

2.2.2.2. Risk Belirleme

Risk belirleme sürecinin temel hedefi, projenin maliyetini, performansını ve takvimini olumsuz yönde etkileyebilecek risklerin en erken aşamada belirlenmesidir. Program riskleri, program yaşam çevrimi boyunca tüm işler, süreçler ve ürün gerekleri değerlendirilerek belirlenir.

Risk belirleme sürecinde, her bir riskin nedenlerinin belirlenmesi, kritik bir konudur. Riskin oluşmasının bir çok nedeni olabilir; ancak yüzeysel nedenler değil kök nedenin belirlenmesi önemlidir. Kök nedenin doğru belirlenmesinde, ele alınan konu hakkında sahip olunan deneyim ve bilgi birikimi önemlidir.

Risk yönetiminin etkinliği, temelde risklerin belirlenmesine bağlıdır. Bu nedenle, bu belirleme işlemi bir sistematik proses olmalıdır. Çoğu durumda, risk belirleme, beklenen risk alanlarının tahminine ve yorumlanmasına dayanmaktadır.

Çok sayıda risk belirleme metodu bulunmaktadır. Bu metotlar aşağıda belirtilenleri içerebilir:

-Uzman görüşmeleri

-Beyin fırtınası

-Soru formları

-Geçmiş uygulama bilgileri

-Deney ve modelleme

-Tasarım gözden geçirmeleri

-Proje gözden geçirmeleri[73]

Riskleri belirlemek için başka bir yaklaşım da, kritik süreçlerin ve bu süreçlerle ilgili risklerin belirlenmesidir. Üretimden tasarıma geçişte, kritik süreçler ve bunlara ilişkin riskler verilir. Her önemli teknik faaliyet için bir şablon tanımlanır.Her şablon, potansiyel risk alanlarını tanımlar. Her şablon projeye uyarlanarak riskli alanlar belirlenir.

---

[72] Fıkırkoca, a.g.e., s.170-189.

[73] TS IEC 62198, Proje Risk Yönetimi-Uygulama Kılavuzu (Ankara: TSE, 2003)

Risk belirleme faaliyetlerinin sonuçları, risk yönetim planında belirtildiği gibi prosedür haline getirilmelidir. Bu dokümanlar, programa ilişkin riskleri, kritiklik derecesi ile birlikte risk senaryolarını, risk yönetim kontrol faaliyetlerini de içerebilir.[74]

Örnek olarak Bilgi Teknolojileri (BT) ile ilgili 21 potansiyel senaryoyu kapsayan risk senaryolarının genel bir listesi Tablo 3'te verilmiştir.

Tablo 3. BT ile İlgili Risk Senaryolarının Listesi

BT ile İlgili Risk Senaryoları	
Ref	**Olay**
S01	Yetersiz sistem & ağ kapasitesi
S02	3. şahıs iflası ve/veya anlaşmazlığı
S03	Doğal Felaket
S04	Şirket kaynaklarının yanlış kullanımı
S05	İnsan hatası
S06	Çalışan sorunları (dahili ve harici)
S07	Veri/işlem gizliliğini tehlikeye sokacak kötü niyet ve sabotaj
S08	Çalışma yöntemleri ve prosedürleri (şimdiki ve geçmişteki) yetersiz tanımlanmış veya belgelenmiş
S09	Yazılım hatası
S10	Yetersiz bütçe & planlama
S11	Veri bozulması
S12	İletim hatası
S13	Veri/işlem bütünlüğünü tehlikeye sokacak kötü niyet ve sabotaj
S14	Veri/işlem erişilebilirliğini tehlikeye sokacak kötü niyet ve sabotaj
S15	Dahili fiziksel olay (kablo, yangın, …)
S16	Yetersiz altyapı/mimari
S17	Proje & Program Yönetim Başarısızlıkları
S18	BT ve hizmet sağladıkları kişiler arasındaki yetersiz iletişim
S19	Eksik veya yanlış yönlendirilmiş bilgi birikimi & beceriler
S20	BT için artan düzenleyici uyum gereklilikleri
S21	Yetersiz veri modelleme

Okay, (20 Mart 2006), http://kamubib.tbd.org.tr/dokumanlar/cg2.doc

2.2.2.3. Risk Analizi

Risk analiz sürecinde, risklerin büyüklüğünü belirlemek için riskin oluşma olasılığı ve sonuca etkisi incelenmektedir. Uygulamada, risk belirleme ve analiz faaliyetleri birbirinden tam olarak ayrı yürütülmez. Her iki faaliyet, çoğu zaman iç içedir. Çoğunlukla, risk belirlenirken aynı zamanda analizde edilir. Örneğin, bir uzmanla görüşme tekniği ile, risk belirlenirken, riskin oluşma olasılığı, sonuca etkisi ve

[74] Fıkırkoca, a.g.e., s.170-189.

ne zaman oluşabileceği de incelenir. Belirlenen riskler, sayısal değerlere dönüştürülerek nicel hale getirilir. Risk değerleri tahmine dayalı olarak belirlenir. Tahminler;

-Olasılık

-Sonuçlar

-Zaman çerçevesi,

için yapılır. Analizler, nicel ve nitel olabilir. Nicel ve nitel analizlerin dengelenmesi, projeden projeye değişir. Analizler, projenin karmaşıklığına, eldeki verilere, projenin hangi aşamasında olunduğuna, maliyet-etkinlik ihtiyacına göre nicel ya da nitel olarak yürütülür.

Proje hedeflerine ulaşmak için, belirlenen tüm risklerin etkisinin bileşimi kurulmalıdır.

Risklerin her biri için, proje hedeflerini ne ölçüde etkiyebileceğine bağlı olarak, bağıl önem derecesi belirlenir.

Analiz süreci, kritik riskleri belirlemek için aynntılı çalışmalarla başlar. Riskin oluşma olasılığına ve oluşması durumunda maliyet, takvim, performansı ne ölçüde etkileyeceğine karar verebilecek kadar bilgi toplanmalıdır. Bu aşamada, tam ve kapsamlı dokümantasyona sahip olmak önemlidir. Riskin sonuca etkilerinin değerlendirilmesi çoğunlukla özneldir ve mümkün olduğunca, aşağıdaki tekniklerden elde edilen, detaylı bilgilerden yararlanılmalıdır:

-Benzer sistemlerle karşılaştırma

-Geçmişten çıkarılan dersler

-Deneyim

-Test ve prototip geliştirrne faaliyet sonuçlan

-Mühendislik ve diğer modellerden toplanan veriler

-Uzman bilgisi

-Planların ve ilişkili dokümanların analizi

-Modelleme ve simülasyon, alternatif analizler[75]

Bilişim sistemlerinin risk analizinde; varlıkların değeri, tehditler ve zayıflıklar analiz edilir. Burada riskler, bilişim sistemlerinin gizliliğinin, bütünlüğünün, güvenirliğinin, potansiyel etkilenme şiddetine bağlı olarak değerlendirilir.[76]

---

[75] Fıkırkoca, a.g.e., s.190.

2.2.2.3.1. Risk Derecelendirme

Nicel tekniklerle, riskin oluşma olasılığı ve sonuç üzerindeki etkisi sayısal değerlere dönüştürülür ve risk büyüklüğü sayısal bir değer olarak hesaplanılır. Bu süreç, risk nicelleme ya da risk sayısallaştırma olarak adlandırılır. Nitel tekniklerle riskin derecesi belirlenir ve bu süreç, risk derecelendirme olarak ifade edilir.

Riskin oluşturacağı potansiyel kaybın nicel tekniklerle değerlendirilme sonucunda, kayıp maliyeti tahmin edilir.

Riskin oluşma olasılığı, nicel tekniklerle belirlenebildiği gibi, nitel tekniklerle değerlendirilerek de derecelendirilir. Oluşma olasılığı, riskin ne sıklıkta oluşacağı terimi ile (çok sık, sık, nadiren gibi) ya da hangi periyotlarda oluştuğuna göre (yılda bir kez gibi) derecelendirilir. Riskin oluşması durumunda performans, takvim ve maliyet açısından sonuca etkisi, nitel teknikler kullanılarak derecelendirilir. Riskin sonuç üzerinde yaratacağı etki, potansiyel kayıptır. Potansiyel kayıp, nitel tekniklerle "çok az, çok büyük" v.b. şekilde derecelendirilebilir. Riskin oluşma olasılığı ve sonuca etki derecelerine bağlı olarak risk derecesi belirlenir.

Risk derecesi, risklerin bir program üzerindeki potansiyel etkilerinin bir göstergesidir. Bir olayın oluşma olasılığını ve sonuçlarını gösteren bir metriktir. Risk derecelendirme ve önceliklendirme, risk analiz sürecinin bir parçasıdır.

Risk derecelendirmede, İDA temel alınır ve her bir İDA bileşeni için risklerin derecesi belirlenir. Her İDA bileşeni için risk olaylarının oluşma olasılığı belirlenir. Her bir risk olayının oluşması durumunda, sonuca etkisi, risk alanlarına (ömeğin; teknik, takvim, maliyet) göre derecelendirilir. Risk olayının oluşması durumunda, her bir risk alanını ne ölçüde etkileyeceği dikkate alınarak, sonuca etki bileşeni için bir derece belirlenir. Her bir risk olayı, oluşma olasılığı ve sonuca etki bileşenleri için belirlenen derecelerden yola çıkılarak derecelendirilir. Öncelikle, risk bileşenleri derecelendirilir. Riskin oluşma olasılığı ve sonuca etki bileşenleri, değişik düzeylere ayrılarak en etkin şekilde derecelendirilmelidir. Örneğin, üç düzeyde, beş düzeyde, on düzeyde. Riskin oluşma olasılığı ve sonuca etkisi, ayrı ayrı derecelendirilir. Risk bileşenleri derecelendirme düzeyi, kullanılan yönteme bağlı olarak daha detaylandırılabilir.

---

[76] ISO/IEC TR 13335-1, Information Technology - Security Techniques - Management of Information and Communications Technology Security (Part 1, 1996)

Örneğin, risk derecelendirme düzeyleri, 1 'den 5'e ya da 1 'den 10' kadar belirlenebilir. Risk bileşenlerinin derecesinden yola çıkılarak, riskin büyüklüğü ya da derecesi bulunur. Risk dereceleri, genel olarak yüksek orta ve düşük olmak üzere üç düzeyde ifade edilir.

Tablo 4 ve 5'te, riskin olasılık ve sonuç bileşenleri için derecelendirme kriterlerine örnekler verilmektedir. Tablo 6, riskin derecelendirme kriterleri ve Şekil 20'de risk derecelendirme matrisi (üç düzeyde derecelendirme; düşük (D), orta (O), yüksek (Y)) için örnek bir gösterimdir.

Tablo 4. Oluşma Olasılığının Derecelendirme Kriterleri

Düzey	**Risk olayının oluşma olasılığı**
1	Yok denecek kadar düşük
2	Olası değil
3	Olası
4	Yüksek olarak olası
5	Belirsizliğe yakın (çok yüksek)

Fıkırkoca, 2003, s.193.

Tablo 5. Sonuca Etkinin Derecelendirme Kriterleri

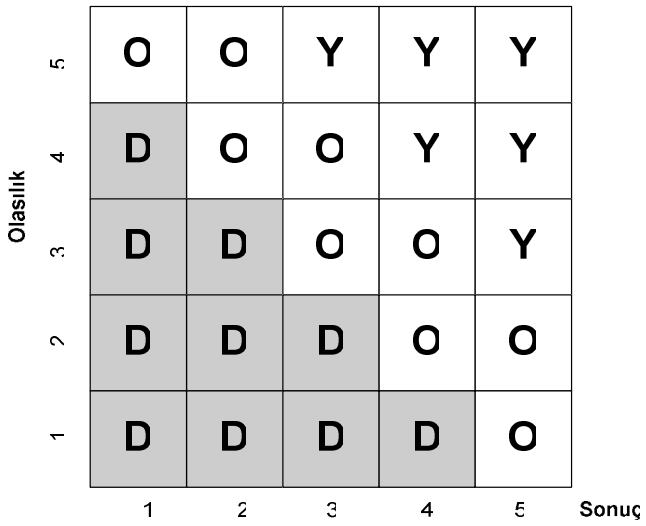
Düzey	**Performans**	**Takvim**	**Maliyet**
1	Çok az ya da etkisi yok	Çok az ya da etkisi yok	Çok az ya da etkisi yok.
2	Risk azaltılarak kabul edilebilir	Ek kaynak gereklidir, istenen tarihte yapılabilir	<%5
3	Riskler önemli azaltmalarla limitler içinde kabul edilebilir	Kritik tarihlerde küçük kaymalar, iş istenen tarihte yapılamayabilir.	%5-7
4	Kabul edilebilir pay yok	Kritik tarihlerde önemli kayma, kritik yol etkilenir.	%7-10
5	Kabul edilemez	Önemli program kilometre taşlarına ulaşılamayabilir.	>%10

Fıkırkoca, 2003, s.193.

Tablo 6. Riskin Derecelendirme Kriterleri

Derece	**Anlatımı**
Yüksek	Önemli bozulma olasılığı
Orta	Bir miktar bozulma
Düşük	Minimum etki

Fıkırkoca, 2003, s.193.



Şekil 20. Risk Derecelendirme Matrisi

Fıkırkoca, 2003, s.194.

Risk değerlendirme süreci çıktısı bir risk matrisidir. Risk matrisi, riskleri, risklerin oluşma olasılığı, sonuca etkisi, büyüklüğü ve oluşabileceği zaman aralığı gibi bilgileri içeren bir dokümandır. Risk matrisi, risk azaltma ve izleme faaliyetlerinin girdisini oluşturan özet bilgileri içerir.

2.2.2.3.2. Risk Önceliklendirme

Risk önceliklendirme risk analizi sürecinin bir önceliklendirme sürecinde, belirlenen risk dereceleri/büyüklüklerine bağlı olarak riskler öncelik sırasına

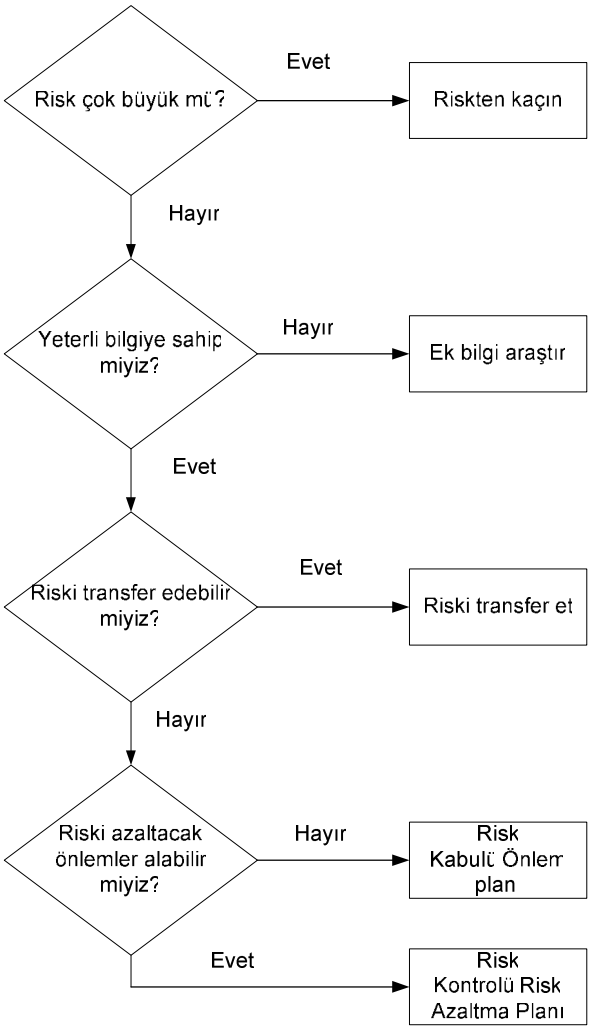
konulur. En öncelikli risk, en önce çözümlenmesi gereken risktir. En yüksek dereceye sahip risk, azaltma faaliyetlerinde en öncelikli olarak ele alınması gerekli olandır.

Risk önceliklendirme süreci sonucunda, program için en kritik olan riskler belirlenir. Risk önceliklendirme sürecinin çıktısı olan önceliklendirilmiş risk listesi, risk azaltma plan1arının geliştirilmesinde, azaltma faaliyetlerinin hazırlanmasında, azaltma için kaynak planlamada temel olarak alınır. Önceliklendirme, en kritik risklerden başlayarak risk azaltma faaliyetlerinin planlanmasına olanak tanır. En kritik risklere, öncelikle kaynak ayrılarak, kısıtlı program kaynaklarının etkin kullanımı sağlanır.

2.2.3. Risk Azaltma Önlem Alma

Risk azaltma, risk yönetiminin kritik bir sürecidir. Risk değerlendirme sonuçlarına dayalı olarak riskler için önlem alınıp alınmayacağına karar verilir. Risk kararları, kuruluşun risk yönetim kültürüne, risk stratejisine bağlı olarak risk almakla risk almamak arasında değişir. Büyük riskler büyük fırsatlar yaratabileceğinden, fırsatlar öngörülerek risk almaktan kaçınılmamalıdır. Risk alınması durumunda riski en aza indirgeme, fırsata dönüştürme yolunda yoğun ve bilinçli bir çaba harcanmalıdır.

Risk azaltma sürecinde temel hedef, risklerin en erken aşamada problem haline dönüşmeden önlenmesidir ve öncelikle riskin oluşma olasılığını en aza indirgemektir. Risklerin erken bir aşamada belirlenemediği durumlar olabilecektir. Riskler belirlenerek azaltma faaliyetleri yürütülmesine karşın, tam olarak ortadan kaldırılamazsa, belli bir ölçüde sonuç üzerinde istenmeyen bir etki yaratabilir. Risk azaltma faaliyetlerinin etkin olarak yürütülememesi durumunda, risklerin en aza indirgenmesinde başarılı sonuçlar elde edilemeyebilir. Belirsizliğin tam olarak kontrol altına alınması olayın doğasına aykırıdır. Riskli bir durum, bazı zamanlarda, herhangi bir azaltma faaliyeti yürütmeksizin kabul edilebilir. Tüm bu ve benzeri koşullar için, risklerin probleme dönüşmesi durumu için de önlem planları geliştirilmelidir. Risk azaltma sürecine ilişkin karar mekanizması Şekil 21'de verilmiştir.



Şekil 21. Risk Azaltma Süreci

Fıkırkoca, 2003, s.345.

Riskler değerlendirildikten sonra, kritik risklerin oluşma olasılığını ve etkisini azaltmak için yaklaşımlar geliştirilmelidir. Bu yaklaşımlar, program tedarik stratejisi ile uyumlu olmalı ve riskle ilgili ne yapılacağını belirtmelidir. En etkin risk azaltma stratejisinin ve tekniklerinin belirlenmesinde, aşağıdaki değerlendirmelerin bilinmesine ihtiyaç vardır:

-Riskin büyüklüğü,

-Yeterli bilgi sahipliği,

-Riskin transferi,

-Riski azlatmak yada ortadan kaldırmak,

-Riski üstlenmek.

Riskin Büyüklüğü : Risk kabul edilemeyecek kadar büyükse, proje stratejileri ve taktikleri daha az riskli alternatifleri seçmek için değiştirilir ya da projenin yapılmamasına karar verilebilir. Örneğin, proje takvim kısıtları çok sıkı ise, ileri teknoloji gerektiriyorsa, projede yeni bir tekniğin kullanılmamasına karar verilebilir.

Yeterli Bilgi Sahipliği : Yeterince bilgiye sahip olunmadığı durumda, hedeflenen sonuca ulaşma konusundaki belirsizlik fazladır. Bilginin edinilmesi ile belirsizlik ve riskler azaltılacaktır.

Risk Transferi : Riskin başka bir organizasyona transferi planlanabilir. Örneğin, sözleşme aşamasında, projenin bazı kısımları, alt yüklenicilere verilerek risk transfer edilebilir. Sistem gereksinimlerinin analizi sırasında riskler gereksinimler arasında paylaşılarak azaltılabilir. Başka bir risk transfer yöntemi de, projeye uygun sözleşme yapılarak riskin yüklenici ve tedarikçi arasında paylaşılmasıdır.

Riski Kontrol Altına Almak/Azaltmak : "Riskin farkındayım ve riskin oluşumunu ve etkilerini hafifletmek için gerekli her şeyi yapacağım", durumuna karşılık gelir. Risk oluşma olasılığını ve/veya sonuca olumsuz etkilerini en aza indirgemek amacı ile planlı bir dizi faaliyet yürütülür. Riskin oluşma olasılığını ve sonuca etkilerini azaltmak için riskin izlenmesi ve yönetilmesi faaliyetlerinden oluşan bir süreçtir. En yaygın kullanılan risk azaltma tekniğidir. Proje ya da program koşulları sürekli olarak izlenerek gerekli olduğunda, riskin oluşma olasılığını ve oluşması durumunda sonuca etkilerini en aza indirgeyecek faaliyetlerin yürütülmesi sürecidir. Riskin kontrol edilmesi, risk azaltma planının geliştirilmesini ve daha sonra planın izlenilmesini gerektirir.

Risk Üstlenme : Risk üstlenme, özel bir risk durumunun varlığının kabulüdür ve riski azaltmak için herhangi bir çaba harcanmayabilir. Bu yöntem, düşük risk durumları için daha uygundur. Bu tür riskler, ya programın doğasında var olabilir ya da diğer risk azaltma faaliyetleri sonucunda, kalan artık risktir. Risklerin üstlenilmesi, onların ihmal edildiği anlamına gelmez. Gerçekte, onları belirlemek ve anlamak için çaba harcanmalı ve uygun yönetim faaliyetleri planlanmalıdır. Ayrıca, üstlenilen riskler geliştirme

sırasında izlenmelidir. İzleme faaliyetleri, başlangıçtan itibaren iyi planlanmalıdır. Risk üstlenme, riskin oluşması durumunda, yaratacağı sonuçların kabul edilmesi kararıdır. Tedarik programlarında her zaman bir miktar risk üstlenilir. Proje yönetimi tarafından, alınan riskin düzeyinin uygun olduğu belirlenmelidir. Bir projede üstlenilen risk, önemli miktarda başka riskleri de içerir. Bu nedenle alınan riskler, kapsamlı olarak değerlendirilmeli ve ona göre risk üstlenme kararı verilmelidir.

2.2.4. Risk İzleme Denetim ve Raporlama

Risk izleme süreci, planlanan bütün risk yönetim faaliyetlerinin etkin olarak gerçekleştirildiğini güvence altına almak için resmi, sistematik ve sürekli olarak yürütülen bir süreçtir. Riskin durumu program boyunca sürekli olarak izlenir. Riskin durumunda önemli bir değişiklik olduğunda riskler yeniden değerlendirilir. Risk izleme mevcut durumdaki değişikliklere odaklanır. Risk izleme sürecinde, program yaşam çevrimi boyunca, belirlenmiş metriklere göre risk azaltma faaliyetlerinin performansı, sistematik ve sürekli olarak izlenir ve değerlendirilir. Bu süreç, aşağıdaki temel faaliyetleri içerir:

-Mevcut risklerin izlenmesi

-Risk durumunun güncellenmesi

-Faaliyetlerin periyodik olarak gözden geçirilmesi

-Risklerin periyodik olarak yeniden değerlendirilmesi

-Raporlama ve geri bildirim

Risk izleme, potansiyel problem çözme tekniği değildir; risk azaltma sonuçlarını gözlemek ve yeni riskleri belirlemek amacı ile yürütülür. İzleme süreçlerinde kritik olan konu, program yönetimi tarafından programın durumunu değerlendirmekte ku1lanılacak bir maliyet, çizelge ve performans yönetim gösterge sisteminin kurulmasıdır. Yönetim gösterge sistemi, yönetim faaliyetlerine yol göstermek amacı ile, potansiyel problemler için erken uyarı verecek şekilde tasarlanmalıdır.

Marangozlukta sıklıkla kullanılan " İki ölç, bir biç " deyimi; bir kararı vermeden önce ölçüm yapmak, ölçüm sonuçlarını değerlendirmek, geçmiş verileri incelemek, kapsamlı ve derinlemesine düşünmek ve daha sonra karar vermek gerekliliğini vurgulayan bir deyimdir. Karar verildikten sonra, çoğu zaman geri dönüş zordur. Geri dönebilmek için belli ölçüde kaybı kabullenmek gerekir. Ölçümlere dayalı karar verme

ile kararların doğruluğu artırılır, geri dönme gereksinimi ve oluşacak kayıplar azaltılır. Ölçme süreci ile şunlar hedeflenir:

-Strateji, hedef ve amaçlara ulaşabilmek

-Problemleri ve riskleri en erken aşamada belirleyebilmek

-Süreçleri anlamak ve yetersizlikleri belirlemek

-İyileştirme ve atılım niteliğinde kazançlar sağlayabilmek

Risk yönetiminin etkinliği, nicel ve nitel metriklere dayalı olarak ölçülür ve çizelgelenir. Her ölçüm için hedef değer ve tolerans belirlenir. Ölçüm sonuçları, sistematik olarak değerlendirilerek risk yönetiminin etkinliği kontrol edilir. Risk izleme süreç ürünleri değerlendirilerek risk yönetiminin projenin sonuçlarını ne ölçüde etkilediği belirlenir. Risk yönetim süreçlerinin etkinliğinin kontrolü için ürün, süreç, insan/kaynak metrikleri toplanarak analiz edilir.[77]

Risk izleme ve kontrol aşamasından elde edilen sonuçlar, çıktıları oluşturur. Bunlar; düzeltici faaliyetler ve risk yönetim planı güncellemesidir. Düzeltici faaliyetler öncelikle planlanan risk yönetimi uygulamalarının gerçekleştirilmesini içerir. Risk yönetim planı, beklenen risklerin oluşmasından sonra, gerçekleşen risklerin etkilerinin değerlendirilmesinde, olasılık ve değer tahminlerinin yenilenmesinde güncellenir.[78]

2.3. Risk Yönetiminde Dokümantasyon ve Raporlama

Risk yönetiminin bilgi temelli ve etkin bir şekilde yürütülmesi, sahip olunan verilerin tamlığı ve doğruluğu ile doğru orantılıdır. Risk yönetim faaliyet sonuçlarının dokümantasyonu, bilgiye dayalı risk yönetiminin temel gereklerindendir. Gerçekleştirilen risk yönetim faaliyetlerine ilişkin toplanan veriler, daha sonra yürütülecek risk yönetim faaliyetlerine temel oluşturacaktır.

Dokümantasyon, risk yönetim sürecinin uygulanmasını ve kontrolünü, özellikle farklı proje safhalarının el değiştirme noktalarında kolaylaştırır. Dokümantasyon, plânlamaya, gelişmenin değerlendirilmesine ve izlenebilirliğe yardımcı olur. Risk yönetim süreci ve riskler ile bunların iyileştirilmesi dokümante edilmelidir.[79]

---

[77] Fıkırkoca, a.g.e., s.353-375.

[78] Ayşe Küçük Yılmaz, Havacılıkta Emniyet Açısından Risk Yönetimi ve Havacılık Örgütlerinden Uygulama Örnekleri, (Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, 2003), s.147-148.

[79] TS IEC 62198, Proje Risk Yönetimi-Uygulama Kılavuzu (Ankara: TSE, 2003)

Risk yönetim süreçlerinin sonuçları, belirlenen format ve yöntemle doküman haline dönüştürülür. Bunlar, risk yönetim raporları, risk bilgi formları, risk matrisi, risk değerlendirme raporu, risk azaltma dokümanlarıdır.

Risk Yönetim Raporları: Raporlar karar vericilere ve program ekibine, risk azaltma faaliyetlerinin etkinliği ve risklerin durumu hakkında bilgi iletmek amacı ile kullanılır. Riskle ilişkili raporlar resmi olmayan sözlü raporlardan, resmi yazılı raporlara kadar uzanan değişik yollarda sunulur.

Risk Bilgi Formu : Risk bilgi formları, risk verilerinin tutulması, ekiplere ve yöneticilere temel risk bilgilerinin raporlanması amacı ile hazırlanır. Tedarikçi, yüklenici ve proje ekibine risk bilgisinin raporlanması için bir format sunar. Potansiyel bir risk belirlendiği ve bilgi güncellendiği zaman kullanılır.

Risk Matrisi: Risk matrisi, program yürütülürken yönetimin özel dikkat göstermesi gereken alanları listeler. Risk matrisi incelenerek risk azaltma faaliyetlerinin etkinliği izlenebilir. Risk değerlendirme sonuçlarına dayalı olarak hazırlanır. Program ilerlerken listeye yeni kalemler eklenebilir.

Risk Değerlendirme Raporu: Risk değerlendirme raporu, program kararlarının çoğu için bir temel sağlar. Risk belirleme, analiz ve azaltma süreçlerinin sonuçlarını gösterir. Bu rapor risk azaltma planlarının geliştirilmesinde temel sağlar. Oldukça kapsamlı dokümanlar olabilir, dosya olarak saklanabilir.

Risk Azaltma Dokümantasyonu: Risk azaltma dokümantasyonu, risk azaltma seçeneklerinden birine karar verebilmek için gerekli olan bilgiyi sağlar. Bu doküman, risk azaltma seçeneklerinin incelenmesi ve seçilmesi için gerekli bilgileri içerir. Her risk azaltma işi için bir plan olmalıdır. Risk azaltma planları, risk değerlendirme sonuçlarına dayalı olarak hazırlanır.[80]

---

[80] Fıkırkoca, a.g.e., s.377-385.

ÜÇÜNCÜ BÖLÜM

BİLGİ GÜVENLİK YÖNETİM SİSTEMİ KURULUMU

1. TS ISO 17799 BİLGİ GÜVENLİK YÖNETİM SİSTEM İHTİYAÇLARI

Bilgi sistemlerinin güvenli hale getirilmesi konusu, kapsamlı ve bütünleşik bir yaklaşımla ele alınmadığı takdirde, başarı kazanmak büyük olasılıkla mümkün olmayacaktır. Bilgi güvenliğinin sağlanması üç temel açıdan ele alınabilir. Bu üç süreç alanı Şekil 22'de gösterildiği gibi:

-Yönetsel önlemleri,

-Teknoloji uygulamalarını,

-Eğitim ve farkındalık yaratmayı, kapsamaktadır.

Şekil 22. Bilgi Güvenliğinin Sağlanmasında Bütünleşik Yaklaşım

Bilişim Güvenliği,2003, s.16.

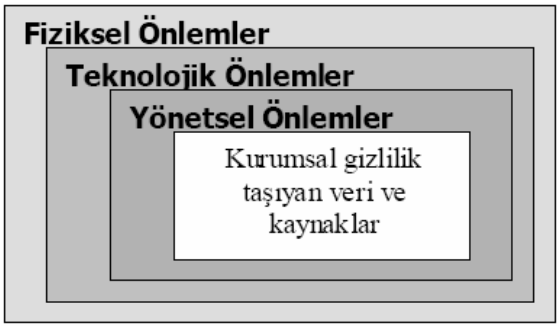
Güçlü bir güvenlik altyapısı kurabilmek için bu üç parçayı birbiri ile bütünleştirmek ve hepsini birlikte bütünsel bir yaklaşımla ele almak gerekir. Bu bahsedilen süreç alanlarının içinde, bilgisayar ve bilişim güvenliği teknolojilerinin dışında kalan farklı alanlar da bulunmaktadır. Diğer bir deyişle, bir kurumun, kurumsal

bilgi güvenliği sağlamak amacıyla, sadece bilişim teknolojilerini devreye sokarak başarıya ulaşma şansı oldukça azdır. Bütün bunlara ek olarak, bu üç süreç alanından her biri, başarıya ulaşmak için diğer iki süreç alanının tam ve eksiksiz çalışıyor olmasına ihtiyaç duyar. Bu üç alan birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Birlikte çalışmalarından oluşacak sinerji, kuruma bilişim güvenliği yönünden tehdit oluşturacak tüm etkenlere karşı güçlü bir kalkan görevini üstlenecektir.

Yönetsel Önlemler, güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi, bilişim güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından, belirlenenlerin yazıya dökülmesi, diğer bir deyişle prosedür, yönerge ve talimatlar gibi dokümanların oluşturulması gelmelidir.[81]

Yönetsel önlemlerle ortaya konulan kurumun güvenlik ihtiyaçlarının karşılanmasında, teknolojik uygulamalardan da faydalanılır. Günümüzde bir bilgisayar ağına ya da tek başına bir bilgisayara yapılacak bir saldırının sonuçlanması saniyelerle ifade edilen çok kısa bir süre içinde oluşur. Bu tür saldırılara, ancak teknolojik bir takım önlemler ile karşı koyulabilir. Bunun yanında kullanılan teknolojiler, güvenlik yöneticilerinin hayatının kolaylaştırılması ve kurumun, bilişim güvenliği açısından bütün resminin görülmesi gibi yararlar da getirirler.

Şekil 23'te gösterildiği gibi, işletmenin sahip olduğu bilgi varlıklarının korunması için yönetsel önlemlerin uygulanması, teknoloji uygulamaları ve eğitim süreçlerinin yanında fiziksel güvenlik uygulamaları ile de desteklenmelidir.[82]



Şekil 23. İşletmenin Sahip Olduğu Bilgi Varlıklarının Korunması

Bilişim Güvenliği,2003, s.16.

[81] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.15-17.
[82] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.48.

Bilgi güvenlik yönetiminde, uygulamaya gelindiğinde, bu alanda uluslar arası tanınan ve yaygın olarak, güvenlik politikaları taslağı hazırlanmasında kullanılan BS 7799 / ISO 17799 en iyi başvuru kaynağınızdır. BS 7799 / ISO 17799 standardı iki parça halinde yazılıp yayınlanmaktadır:

-ISO/IEC 17799 Bolum 1: Bilgi güvenlik yönetimini uygulamakta kullanılacak kodu içermektedir. İçerdiği tavsiye ve önerilerle, şirketinizin bilgi güvenliğinden emin olmanız için on ayrı alanda uygulamalarıyla rehberlik etmektedir.

-BS 7799 Bolum 2 (ISO/IEC 27001): Bilgi güvenlik yönetimi etkili bir Bilgi Güvenlik Yönetim Sistemi (BGYS) oluşturulmasında kullanılmak üzere vereceği tavsiyelerle yol göstermektedir.[83]

İki standart arasındaki ilişki Şekil 24'te gösterildiği gibi, ISO 17799 bilgi güvenliği yönetiminde yer alabilecek güvenlik önlemlerine on temel başlık altında yer verirken, BS 7799-2 ise, bilgi güvenliğinin üç temel bileşeni olan bilginin gizliliği, erişilebilirliği ve bütünlüğü içeren bir Bilgi Güvenliği Yönetim Sisteminin kurulması, uygulanması, izlenmesi, sürdürülmesi ve geliştirilmesi için gerekli adımları ortaya koyan süreçsel yaklaşımın çerçevesini çizer.[84]

Şekil 24. İki Standart Arasındaki İlişki (ISO/IEC 17799 ve BS 7799-2)

Uygulamalı BS7799 Eğitim Dokümanı, TÜBİTAK,2005

[83] Jacquelin Bisson , René Saint-Germain ,BS7799/ISO 17799 Standardı ile Güvenlik Politikaları Uygulaması, (Callio Technologies)

[84] Uygulamalı BS7799 Eğitim Dokümanı (TÜBİTAK-UEKAE, 19/12/2005)

ISO 17799, güvenlik politikası geliştirme ve güvenlik denetlemesi yapma konularını kapsayan uluslararası bir standarttır. Bu standart, 10 alt bölümden oluşur. Her bölümde, o bölümde anlatılan konunun, kurumsal güvenlik politikasına nasıl dahil edileceği ve bu faaliyetlerin nasıl denetleneceği ile ilgili bilgiler vardır.

ISO, BS 7799'u temel alarak ISO 17799 standardını hazırlamıştır. Aşağıda söz konusu standardın bilgi güvenliği yönetiminde yer alan on temel güvenlik önlemlerinin neler olduğu açıklanmaktadır.[85]

1.1. Güvenlik Politikası

Güvenlik politikasından beklenen amaç, bilgi güvenliği için yönetimin yönlendirilmesi ve desteğini sağlamaktır. Bu amaçla yönetim, tüm işletme içinde bilgi güvenliğine ilişkin açık bir politika ortaya koymalı ve bunun için destek vermeli ve bağlılık göstermeli, bilgi güvenliği politikasını herkese bildirmeli ve sürekliliğini sağlamalıdır.[86]

Güvenlik Politikası, bilgi güvenliğinin sağlanması için Kurum çapında kullanılacak bilgi güvenliğinin omurgasını oluşturacaktır. Yapının sağlıklı olabilmesi için bu politika ile birlikte kullanılacak ilişkili alt politikaların ve prosedürlerin de hazırlanması gerekmektedir. Bilgi Güvenlik Politikaları kurum yönetimi tarafından onaylandıktan sonra iki faz olarak bilgi güvenliği yapısının oluşturulması ve Bilgi Güvenlik Politikası'nın uygulanması hedeflenmelidir.[87]

Güvenlik Politikası, kurumda güvenliğin oynadığı rolün genel bir anlatımıdır. Güvenlik Politikası üst yönetim, seçilmiş bir Kurul ya da bir Komite tarafından yazılabilir. Güvenlik Politikaları, bireylerden ve teknolojiden bağımsız hazırlanmalıdır. Kurumda uygulanacak güvenlik kontrolleri, ayrıntıya girilmeden kavramsal olarak tanımlanmalıdır.[88]

Sonuç olarak, işletmeler bilgi güvenliğinin sağlanmasında öncelikle bilgi güvenliği politika belgesi yayınlamalı ve yayınlanan bu politikanın belirli aralıklarla

---

[85] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.48.
[86] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002)
[87] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003), s.29.
[88] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.25.

uygulama durumu ve güncelliğinin korunması açısından gözden geçirilmesi gerekmektedir. Bu süreçlere ilişkin ihtiyaçların detayları aşağıda sunulmuştur.

1.1.1. Bilgi Güvenliği Politika Belgesi

Bu bağlamda bilgi güvenlik politika ve alt politikaların hazırlanarak birim onayına sunulması gerekmektedir.[89]

Bir politika belgesi, yönetim tarafından onaylanmalı, tüm çalışanlara uygun olarak yayınlanmalı ve bildirilmelidir. Yönetim politika belgesine bağlılığını belirtmeli ve bilgi güvenliğini yönetmek için işletmenin yaklaşımını ortaya koymalıdır. Bir politika belgesi aşağıdakileri içermelidir:

-Bilgi güvenliğinin tarifi, geniş kapsamlı hedefi ve amacı ve bilgi paylaşımını etkinleştiren bir yöntem olarak güvenliğin önemini,

-Hedefleri ve bilgi güvenliğinin prensiplerini destekleyen yönetim amacını,

-Güvenlik politikalarının, prensiplerinin, standardlarının ve işletme için belirli öneminin uygun gereklerinin kısa bir açıklamasını,

-Güvenlik raporlaması konuları da dahil, bilgi güvenliği yönetimi için genel ve belirli sorumlulukların tarifini,

-Politikayı destekleme ihtimali olan belgelendirmeler için referanslar, örneğin belirli bilgi sistemleri için daha detaylı güvenlik politikaları ve süreçleri veya kullanıcıların uyması gereken güvenlik kurallarını.[90]

Güçlü ve anlamlı bir bilgi güvenliği politikası her başarılı bilinçlendirme çalışmasının temelini oluşturur. Bilinçlendirme çalışmasına başlamadan önce tüm üst seviye hedeflerin ve güvenlik programının gereklerinin yazılı olması kritik önem taşımaktadır. Politika açık ve kısa ifadeler ile yazılmış olmalı ve kurumun bilgi güvenliği konusundaki önceliklerini yansıtmalıdır. Politika ortaya konduktan sonra kullanıcılar politikanın varlık ve içeriğinden haberdar olmalıdır. Kullanıcılar aynı zamanda politikaya uymamanın doğuracağı sonuçlar hakkında da bilgi sahibi olmalıdır.[91]

---

[89] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003),s.30.

[90] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.4.

[91] Fatih Emiral, Bilgi Güvenliği Bilincinin Genele Yayılması, (14 Nisan 2006) http://www.deloitte.com/dtt/article/0,1002,sid%253D8497%2526cid%253D53205,00.html

Bir kurumun en büyük hedefi, her türlü ortam (kağıt, cd, teyp, bilgisayar, ağ, Internet vb.) üzerinde bulunan veri ve bilgilerin güvenliğini sağlamak, veri bütünlüğünü korumak ve veriye erişimi denetleyerek gizliliği ve sistem devamlılığını sağlamaktır. Bunun yapılabilmesi için bütün güvenlik çözümlerinin bir arada değerlendirilmesi ve uygulanacak politika doğrultusunda güvenlik önlemlerinin alınması gerekmektedir.[92]

1.1.2. Bilgi Güvenlik Politikasının Gözden Geçirilmesi

Politikanın, sürekliliğinin sağlanmasından ve tanımlanmış yöntemlere göre gözden geçirilmesinden sorumlu bir sahibi olmalıdır. Ayrıca, belirli aralıklarda politikaların etkinliği, denetimlerin etkileri ve teknolojik gelişimlerin etkileri açısından, Bilgi Güvenlik Politikaları gözden geçirilmelidir.[93]

1.2. Organizasyon Güvenliği

Bilgi güvenliği, yönetim takımının tüm bireylerince paylaşılan bir iş sorumluluğudur. İşletme içersinde bilgi güvenliğinin gerçekleşmesini başlatmak ve kontrol etmek üzere bir yönetim sistemi kurulmalıdır. Bilgi güvenlik politikasını onaylamak, güvenlik rolleri tayin etmek ve tüm işletme içinde güvenlik yürütümlerini düzenlemek için yönetim önderliğiyle uygun yönetim sistemi kurulmalıdır. Eğer gerekirse, bir uzman bilgi güvenliği tavsiyesi kaynağı kurulmalı ve işletme içinde etkin kılınmalıdır. Endüstriyel eğilimleri yakalamak, standardları ve değerlendirme yöntemlerini gözlemek ve güvenlik olaylarıyla ilgilenirken uygun irtibat sağlamak için, harici güvenlik uzmanlarıyla iletişim geliştirilmelidir.

Organizasyon güvenliğinin sağlanmasında, organizasyon içi bilgi güvenlik altyapısının kurulması, üçüncü taraf erişim güvenliğinin oluşturulması ve gerek duyulduğunda bilgi işleme sorumluluğunun başka bir organizasyondan sağlandığında alınacak tedbirleri içermektedir. Söz konusu üç konu alt başlığına ilişkin detaylar, aşağıda gözden geçirilmektedir.

---

[92] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003), s.35.
[93] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.4.

1.2.1. Bilgi Güvenliği Altyapısı

Güvenlik süreçlerinin yönetilmesi için, sorumluluklar açıkça tanımlanmalıdır. Bilgi güvenlik altyapısının kurulmasında temel olarak; bilgi güvenlik sorumluluklarının organizasyon içinde dağıtılması, bilgi işleme araçları için yetkilendirme, gerektiğinde uzman desteği alınması, organizasyonlar arası işbirliğine gidilmesi, tüm yönetim desteğinin alınması için güvenlik forumu oluşturulmalıdır.

Güvenlik öncelikleriyle ilgili açık bir yönlendirmenin ve görünür yönetim desteğinin olduğunu garanti eden bir yönetim forumu oluşturulmalıdır. Bu forum, uygun bağlılık ve doğru kaynaklar aracılığıyla organizasyon içersindeki güvenliği desteklemelidir. Bu forum varolan yönetim yapısının bir parçası da olabilir.

Organizasyonların tümü uzman danışman istihdam etmek istemeyebilir. Böyle durumlarda, sürekliliği temin etmek ve güvenlikle ilgili karar verme aşamalarında yardım sağlamak üzere, firma içi bilgi ve deneyimleri düzenlemesi için uygun harici uzman danışman görevlendirilebilir. Söz konusu danışmana, en üst seviyede verimlilik ve etki için, tüm organizasyon içinde yönetime doğrudan erişim izni verilmelidir.

İlave olarak, güvenlik arızasının gerçekleşmesi durumunda uygun eylemlerin hızlıca harekete geçirilmesini ve tavsiyelerin alınabilmesini temin etmek üzere bilgi sağlayıcı yasa koyucu organizasyonlar arası uygun ilişkiler kurulmalıdır.[94]

Bilgi güvenlik organizasyonu oluştururken ekip çalışması ve iş bölümlerinin yapılması gerekmektedir. Bu ekipler Bilgi Güvenlik Birimi, Bilgi İşlem Birimi ve kurumun diğer birimleri olarak sıralanabilir. Ancak güvenlikle ilgili tüm faaliyetlerden bir yönetici sorumlu olmalıdır. Bu birimlerin görevleri aşağıda listelenmiştir.

Bilgi Güvenlik Birimi Görevleri:

-Proje koordinasyonu,

-Proje raporlama ve dokümantasyonu,

-Kapsam ve detay çalışmaları için kullanılacak standartların ve uygulanacak yöntemin yer aldığı, yol gösterici dokümanların hazırlanması,

-Bilgi güvenlik politikasının kapsam ve içeriğinin belirlenerek hazırlanması,

-Bilgi güvenlik politikasının alt politikaları ve prosedürlerinin belirlenerek hazırlanması,

---

[94] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.4-9.

-Birimlerden gelen isteklerin değerlendirilerek gerekli görülmesi durumunda proje dokümanlarına yansıtılması,

-Proje çalışmalarının planlanması, varlıkların belirlenmesi, sınıflandırılması, risk analizi, bilgi güvenlik planları, iş devamlılık planları hazırlanması gibi proje aktiviteleri için kullanılacak yöntem, standartların ve yardımcı dokümanların hazırlanması,

-Yapılacak çalışmalar için eğitimlerin verilmesi,

-Birimlerden gelen çalışma sonuçlarının değerlendirilmesi, incelenmesi, takibi ve kontrolü.

Bilgi İşlem Biriminin Görevleri:

-Bilgi Güvenlik Birimi tarafından belirlenen yöntemlerle yapılacak varlık belirlenmesi ve sınıflandırılması, risk analizi, iş devamlılık planları hazırlanması, bilgi güvenlik planlarının hazırlanması vb. proje çalışmalarına katılmak,

-Bilgi Güvenlik politikasının alt politikaları ve prosedürlerinin hazırlanması çalışmalarına destek olmak.

Kurum Birimlerinin Görevleri:

-Kurum için hazırlanan Bilgi Güvenlik politikası ve alt politikaları ile prosedürlerinin incelenmesi,

-Yürütülen çalışmalarda, Kurumun Bilgi Güvenlik Politikasına uyumunun değerlendirilmesi için gerekli desteğin verilmesi,

-Kurumda onaylanan politikaların duyurulması ve eğitim planlamasının yapılması şeklindedir.[95]

1.2.2. Üçüncü Taraf Erişiminin Güvenliği

Bilgi, eksik güvenlik yönetimiyle üçüncü tarafların erişimi aracılığıyla risk altına girebilir. Bir üçüncü tarafla ticari ilişki kurulması gerektiğinde, belirli denetimler için her gerekeni tanımlamak üzere bir risk değerlendirmesi yürütülmelidir. Bu risk değerlendirmesi, istenen erişim biçimini, bilginin değerini, üçüncü tarafça kullanılan denetimleri ve bu erişimin organizasyonun bilgi güvenliğine dahil edilmesini dikkate

[95] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.30.

almalıdır. Denetimler üçüncü tarafla yapılacak bir sözleşme içersinde karşılıklı olarak onaylanmalı ve tanımlanmalıdır.

1.2.3. Dışarıdan Kaynak Sağlama

Bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından dışarıdan sağlandığında bilgi güvenliğinin sürdürülmesi amaçlanmıştır. Yönetim ve bilgi sistemleri, ağlar ve masaüstü ortamların tümü veya bir kısmı için dışarıdan kaynak sağlayan organizasyonların güvenlik gerekleri, taraflar arasında yapılması anlaşılmış bir sözleşme içinde belirtilmelidir.[96]

1.3. Varlıkların Sınıflandırması

Varlıkların sınıflandırılmasındaki amaç, işletmeye ait varlıklar için uygun korunmanın sağlanmasıdır. Bilgi varlıklarıyla ilgili atanmış bir sorumlu sahibi olmalıdır. Bu sorumluluk, uygun korumanın sağlandığının garanti edilmesine yardımcı olur. Bu amaçla öncelikle işletmeye ait varlıkların envanteri çıkarılmalı, takiben varlıların güvenlik seviyesi ve değerlerine göre sınıflandırması yapıldıktan sonra varlığın işleme yöntemine uygun olarak etiketlenmelidir. Bu kapsamda süreçlerin detaylarına ilişkin faaliyetler aşağıda sunulmuştur.

1.3.1. Bilgi İşlem Varlıklarının Envanteri

Bilgi sistemiyle bağlantılı olan önemli bilgi varlıklarını içerecek şekilde, ilgili yönetim birimlerince hazırlanmalı, korunmalı ve bu envanter periyodik olarak ve değişiklikler oldukça güncellenmelidir. Bu çalışmada:

-Her bir varlık açıkça tanımlanmalı,

-Varlık sahipleri belirlenmeli,

-Varlıkların güvenlik sınıflandırmaları yapılmalı,

-Varlığın mevcut bulunduğu yer (bu kayıp ve hasarlar giderilmeye çalışıldığında önemlidir) belirtilmelidir.

Bilişim sistemleriyle ilgili varlıklar, Bilgi Varlıkları, Yazılım Varlıkları, Fiziksel Varlıklar ve Hizmetler olarak kategorize edilebilir. Bunlar:

---

[96] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.7-9.

Bilgi Varlıkları: Veritabanları ve veri dosyaları, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, arşivlenmiş bilgiyi,

Yazılım Varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları ve yazılımlarını,

Fiziksel Varlıklar: Bilgisayar ekipmanları (kasa, ekranlar, diz üstü bilgisayarlar, modemler), iletişim ekipmanları (yönlendirici, telefon, faks), manyetik kayıt ortamları (teyp, kartuş, disket, disk, CD), diğer teknik ekipmanlar (güç kaynakları, adaptör, havalandırma üniteleri), mobilyayı,

Hizmetler: Bilgi işleme (bilgisayar) ve iletişim (haberleşme) hizmetleri, genel hizmetleri (ısıtma, aydınlatma, elektrik, havalandırma), kapsamaktadır.

1.3.2. Varlıkların Sınıflandırılması

Bilgi varlığı, korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmalıdır. Varlık sınıflandırması için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Bilgi varlığı aşağıdaki şekilde sınıflandırılabilir:[97]

-Çok Gizli

-Gizli

-Kuruma Özel

-Hizmete Özel

-Kişiye Özel

-Tasnif Dışı

Bilgi çoğu kez belirli bir süre geçtikten sonra hassas ve önemli olmaktan çıkar, örneğin bilginin genel olarak duyurulması verilebilir. Bu açılar dikkate alınmalıdır, çünkü gerektiğinden fazla sınıflandırma gereksiz ilave ticari harcamalara sebep olabilir. Sınıflandırma kılavuzu, bilgiyle ilgili verilmiş her öğenin sınıflandırılmasına, her zaman uygulanmasına gerek olmadığının ve önceden belirlenmiş politikalara göre değişebileceğinin gerçeğinin önceden tahmin edilmesine izin vermelidir.[98]

---

[97] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003), s.27.

[98] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.10.

1.3.3. Bilgi Etiketleme

Gerekli olduğu durumda, fiziki ve elektronik ortamda olan bilgi varlıkları; sınıflandırma derecesini gösterecek şekilde etiketlenmelidir. Bilgi etiketleme ve işleme için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Bilgi etiketleme ve işlemede aşağıdaki kurallar uygulanmalıdır.[99]

-Fiziksel etiketler, mümkün olduğu durumlarda kullanılmalıdır. Bununla beraber, elektronik biçimdeki belgeler gibi bazı bilgi varlıkları, fiziksel olarak etiketlenemezler. Bu nedenle, bu tür belgelerde elektronik anlamda etiketlemenin kullanılması gerekmektedir.

-Dokümanlar, içerdiği bilginin en yüksek güvenlik seviyesi göz önüne alınarak sınıflandırılmalı ve bu sınıflandırma derecesi her sayfanın sol üst ve alt köşesinde büyük harflerle ve altı çizili olarak yer almalıdır.

-Manyetik kayıt ortamındaki (kartuş, disk, disket, CD, kaset vb.) bilgiler yine en üst güvenlik seviyesi dikkate alınarak etiketlenmeli ve sınıflandırma seviyesi büyük harflerle ve altı çizili olarak medya üzerine yazılmalıdır.

-Elektronik ortamdaki belgelerde de (Word, Excel, Powerpoint dosyaları vb), bilginin güvenlik seviyesini gösteren ibare, dosya içerisinde her sayfada sol üst ve alt köşede büyük harflerle ve altı çizili olarak bulunmalıdır.

-Çok gizli, gizli, hizmete özel bilgilerin gerekli güvenlik önlemi alınmadan posta, faks veya elektronik ortamda aktarılmaması gerekmektedir. Yine bu seviyedeki bilgiler, izinsiz kişilerce eline geçirme riski olduğundan, cep telefonu, sesli mesaj, telefon gibi ortamlarda aktarılmamalıdır.

-Çok gizli, gizli, hizmete özel güvenlik seviyesine sahip bilgi varlıklarına sahip kişiler, bu varlığın bilmesi gerekenlerden başkasının görmemesini sağlamalıdır.

Her sınıflandırma için, işleme yöntemleri, aşağıdaki bilgi işleme faaliyetleri biçimlerini kapsayacak bir biçimde tanımlanmalıdır:[100]

-Kopyalama

-Depolama

---

[99] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003), s.28.
[100] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.4.

-Posta, faks ve elektronik mesaj aracılığıyla aktarma

-Cep telefonu, sesli mesaj, telefonlar gibi sözlü kelimelerle aktarımı

-Yok etme

1.4. Personel Güvenliği

Personel güvenliğinden amaçlanan, insan hatalarını, hırsızlığı, sahtekarlığı ve araçların yanlış kullanılması risklerinin azaltılmasıdır. Bu nedenle, personel güvenlik sorumlulukları işe alma sırasında belirtilmeli, sözleşmeler içinde yer almalı ve bir kişinin işe alınması süresince gözlenmelidir. Olası işe alınmalar uygun bir şekilde elenmeli, özellikle hassas görevler için dikkat edilmelidir. Bilgi işleme araçlarının tüm çalışanları ve üçüncü taraf kullanıcılar bir gizlilik anlaşması imzalamalılardır.

Özetle, işletmeler personel güvenliğinin sağlanmasında, personel iş tanımlarına güvenlik ifadesi eklenerek, tüm personelin tehditlere karşı alınabilecek önlemler konusunda eğitim aldırarak ve güvenlik saldırılarında personel sorumlulukları belirlenerek aşılabilecektir. Personel güvenliğini oluşturan bu konu başlıklarının detayları aşağıda sunulmuştur.

1.4.1. İş Tanımlarında Güvenlik

İşletmeye yeni alınacak personelin sorumlulukları arasına işletme politikası gereği güvenliğin ilavesi, yeni alınacak personelin işe alım kriteri olarak uygulanması, güvenlik politikası gereği personel elemeleri ve çalışanlar ile gizlilik anlaşmaları takip edilerek güvenlik kriterleri sağlanabilir. Bu süreçlerin içeriklerini alt başlıklar altında açacak olursak, şu şekilde sıralanabilir:

İş sorumluluklarına güvenliğin dahil edilmesi: Güvenlik rolleri ve sorumlulukları, organizasyonun bilgi güvenliği politikasında sunulduğu gibi, uygun olan yerde belgelenmelidir. Bunlar, güvenlik politikasını gerçekleştirmek ve sürdürmek için her türlü genel sorumluluğun yanında, belirli varlıkların korunması veya belirli güvenlik işlemlerinin veya faaliyetlerinin yürütülmesi için her özel sorumluluğu içermelidir.

İşe alma koşulları ve şartları: İşe almanın koşul ve şartları, çalışanın bilgi güvenliği ile ilgili sorumluluklarını belirtmelidir. Uygun olan yerde, istihdam sona erdikten sonra bu sorumluluklar tanımlanmış bir zaman dilimi için devam etmelidir. Çalışanın güvenlik gereklerine uymaması karşısında ne gibi önlemler alınacağını da içermelidir.

Personel eleme ve personel politikası: Sürekli personel üzerinde doğruluk kontrolü, işe başvurulduğu zaman yapılmalıdır. Bu aşağıdaki denetimleri içermelidir:

-Tatminkar kişisel referansların varlığı (örneğin bir işle ilgili, bir şahsi)

-Başvuranın özgeçmişinin kontrolü (bütünlük ve doğruluk)

-İddia edilen akademik ve uzman niteliklerin teyidi

-Bağımsız kimlik kontrolü (pasaport ve benzeri belgeler)

Yönetim, hassas sistemlere erişim için yetkilendirilmiş yeni ve deneyimsiz personel için gereken gözetimleri değerlendirmelidir. Tüm personelin çalışmaları, kıdemli personel tarafından belirli zaman dilimlerine gözden geçirilmeli ve onaylama yöntemlerinden geçirilmelidir.

Yöneticiler personellerinin kişisel şartlarının da çalışmalarını etkileyebileceğinin farkında olmalıdırlar. Kişisel veya mali sorunlar, davranışlarındaki veya yaşam şekillerindeki değişiklikler, tekrarlama dalgınlığı ve stres veya depresyon belirtileri, sahtekarlığa, hırsızlığa, hataya veya diğer güvenlik arızalarına yöneltebilir. Bu bilgiyi, yasal yetki sınırları çerçevesi içinde yer alan uygun hükümlere göre ele alınmalıdır.

Gizlilik anlaşmaları: Gizlilik veya kapalılık (ifşa etmeme) anlaşmaları, bilginin gizli veya sır olduğunun bildirimini vermek için kullanılır. Çalışanlar normalde böyle bir anlaşmayı işe alınmalarının öncelikli şartları ve koşullarının bir parçası olarak imzalamalılardır.

1.4.2. Kullanıcı Eğitimi

İşletmenin tüm çalışanları ve ilgili yerlerde, üçüncü taraf kullanıcılar, organizasyona ait politikalar ve yöntemlerle ilgili uygun eğitim ve düzenli güncelleme almalıdırlar. Bu, bilgiye veya hizmetlere erişimi tayin etmeden önce, güvenlik gereklerini, yasal sorumlulukları ve iş denetimlerinin yanı sıra, oturuma giriş yöntemleri, yazılım paketlerinin kullanımı gibi bilgi işleme araçlarının doğru kullanım eğitimini almayı içermektedir.

1.4.3. Güvenlik Saldırılarının Bildirilmesi

Güvenlik saldırılarında meydana gelen hasarın en aza indirilmesi ve bu gibi olayların gözlenmesi ve bunlardan öğrenilmesi amaçlanmaktadır.

Tüm çalışanlar ve sözleşmeli kimseler, işletmeye ait varlıkların güvenliği üzerinde etkisi olabilecek farklı biçimdeki saldırılar (güvenlik kırılması, tehdit, zayıflama veya bozulma) rapor etme yöntemlerinden haberdar olmalıdırlar. Bu kişilerden, gözlemlenmiş ve şüphelenilmiş beklenmedik her olayı, mümkün olan en kısa süre içince belirlenmiş iletişim noktalarına rapor etmeleri istenmelidir. İşletme, güvenlik kırılmaları suçu işleyen çalışanlarla ilgilenmek üzere resmi bir disiplin süreci kurmalıdır.[101]

1.5. Fiziksel ve Çevresel Güvenlik

Geçmiş zamanlarda önemli bilgiler, taşlara kazılarak daha sonra da kağıtlara yazılarak fiziksel ortamlarda saklanmış, duvarlarla, kale hendekleriyle ve başlarına dikilen nöbetçilerle koruma altına alınmıştır. Çoğu zaman fiziksel koruma yeterli olmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir.

Günümüzde de fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar yapılmaktadır. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler kullanılmaktadır.[102]

Fiziksel ve çevresel güvenlikten amaç, iş alanına ve bilgilerine yetkisiz erişim, hasar ve müdahalenin engellenmesidir. Önemli ve hassas ticari bilgi işleme araçları güvenli bir yere yerleştirilmeli, uygun güvenlik engelleri ve giriş denetimleriyle, tanımlanmış güvenli bir çevre aracılığıyla korunuyor olmalıdır. Bu araçlar, fiziksel olarak yetkisiz erişimlerden, hasarlardan ve müdahalelerden korunmalıdır. Sağlanan koruma, tanımlanmış risklerle orantılı olmalıdır. Temiz masa ve temiz ekran politikası, belgelere, ortama ve bilgi işleme araçlarına yetkisiz erişim veya hasar risklerini azaltmak için tavsiye edilmektedir.

---

[101] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.11-13.

[102] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003), s.12.

Fiziksel ve çevresel güvenlik sağlamak için gereken kriterleri, güvenli bölgeler oluşturmak, teçhizat güvenliğini sağlamak ve gerekli denetimleri oluşturacak önlemler başlıkları altında inceleyebiliriz.

1.5.1. Güvenli Bölgeler

Fiziksel güvenlik, firmaların kaynaklarını ve değerli bilgilerini tehdit eden açıklarını kapatmakta kullanılan en önemli yöntemlerden biridir. Fiziki korunma, iş ve bilgi işleme araçları çevresinde sayısız fiziki engeller yaratarak sağlanabilir. Her bir engel, her biri sağlanan toplam korumayı arttıran bir güvenlik çevresi oluşturur. İşletmeler güvenlik çevrelerini, bilgi işleme araçları içeren alanları korumak için kullanmalıdırlar. Güvenlik çevresi, bir engel oluşturan, örneğin bir duvar, kart kontrollü giriş kapısı veya bir kişi tayin edilmiş danışma masası gibi her şeydir. Her bir engelin yerleştirilmesi ve gücü, risk değerlendirmesinin sonucuna bağlıdır.

Güvenli bölgeler oluşturulabilmesi için, bilginin bulunduğu alanlara girişin fiziksel giriş denetimi yapılması, bilgi kaynaklarının bulunduğu alanların fiziki çevresel koruma altında tutulması, güvenli alan denetimleri ve yükleme alanlarının bilgi kaynaklarına ulaşımına engellenecek şekilde ayrılması faaliyetlerini içermektedir. Bu faaliyetlerin yönetilmesinde dikkat edilecek konular şu şekilde sıralanabilir:

Fiziki giriş denetimleri: Güvenli alanlar, sadece yetkili personelin erişimine izin verildiğinin temin edilmesi için uygun giriş denetimleriyle korunuyor olmalıdırlar.
Aşağıdaki denetimler göz önüne alınmalıdır:

-Güvenli alanlarda ziyaretçilere eşlik edilmeli veya üstleri aranmalıdır ve giriş ve çıkış tarihleri ve saatleri not edilmelidir. Sadece belirli, yetkili amaçlar çerçevesinde erişimlerine izin verilmeli ve alana ait güvenlik gereklerinin direktifleriyle ilgili ve acil durum yöntemleriyle ilgili bilgilendirilmelidirler.

-Hassas bilgilere ve bilgi işleme araçlarına erişim denetlenmeli ve sadece yetkili kullanıcılara sınırlı olmalıdır. Kimlik doğrulama denetimleri, örneğin giriş kartı ve parola, tüm erişimleri yetkilendirmek ve geçerli kılmak için kullanılmalıdır. Tüm erişimlerin bir kontrol zinciri güvenli olarak korunmalıdır.

-Tüm personelden, görünür biçimde kimlik kartı taşımaları istenmelidir ve eşlik edilmeyen bir yabancıya veya kimlik kartı taşımayan birine rastlandığında hemen bildirmeleri teşvik edilmelidir.

-Güvenli alanlara erişim hakları düzenli aralıklarla gözden geçirilmeli ve güncelleştirilmelidir.[103]

Günümüzde bu konu üzerine çalışan bir çok güvenlik firması ve bu firmaların yeterince geniş yelpazede ürünleri vardır. Firmalar genellikle, akıllı giriş kartları kullanmaya başlamıştır. Bu kartların en önemli avantajı giriş çıkışların kayıtlarını tutmasıdır. Fakat bir dezavantajı ise kaybolma riski taşımasıdır. Zaten bu riski nasıl azaltılabilir şeklinde düşünen üretici firmalar, çalışanların yanlarında taşıdıkları ve kaybolma riski bulunmayan fiziksel özellikleri kullanmaya karar vermektedirler. Böylece biyometrik giriş sistemleri kullanıma sürülmüştür. Bu kapsamda gözümüzü veya parmak izimizi kullanarak erişim hakkımız olan bölgelere girip çıkmaya başlanmıştır.

Diğer önemli bir konu ise şirkete gelen ziyaretçilerin şirket içindeki hangi bölgelere nasıl gireceğinin ve yanlarında eşlik edecek bir kişinin gerekip gerekmediğinin belirlenmesidir. Ayrıca ziyaretçi giriş çıkışlarının düzenli olarak kaydının tutulması çok önemlidir. Bu konuda ziyaretçilere verilecek ve adlarına kayıt yapılacak kartlar kullanılabilir.[104]

Bürolar, odalar ve araçların güvenlik altına alınması: Güvenli bir alan, kilitlenmiş bir büro veya içinde birçok oda bulunan, kilitlenmiş olan ve kilitlenebilir dolaplar veya korumalar içeren fiziki bir güvenlik çevresi olabilir. Güvenli bir alanın seçimi veya tasarımı, yangın, sel, patlama, askeri saldırı ve diğer biçimdeki doğal veya insan yapımı afetlerden meydana gelebilecek hasar ihtimallerini göze almalıdır. Ayrıca ilgili sağlık ve korunma standardlarına ve kurallarına da dikkat edilmelidir. Ayrıca komşu çevrelerden, örneğin diğer alanlardan su borusu akıntısı gibi, gelebilecek olan güvenlik tehditleri de göz önünde bulundurulmalıdır. Aşağıdaki denetimler dikkate alınmalıdır:

-Herkes tarafından erişimi engellemek için anahtar araçlar yerleştirilmelidir.

-Binalar göze çarpmayan bir şekilde olmalıdır ve bilgi işleme faaliyetlerinin, bina içinde veya dışında, varlığını tanımlayan belirgin bir işaret olmaksızın amaçlarıyla ilgili en az göstergeyi vermelidir.

---

[103] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.11-13.

[104] Ayhan ERGUN, Fiziksel Güvenliğinizden Emin misiniz?, (09 Mayıs 2006), http://www.acemiler.net/pc_guvenlik.phtml

-Fotokopiler, faks makineleri gibi destek fonksiyonları ve donanımları, bilgiyi tehlikeye atan erişim taleplerini engellemek için güvenli alan içine uygun bir şekilde yerleştirilmiş olmalıdır.

-Pencereler için özellikle de zemin kat seviyesinde ihmal edilmiş ve harici koruma göz önüne alındığında, kapılar ve pencereler kilitlenmiş olmalıdır.

-Profesyonel standardlarda uygun izinsiz girişleri tespit sistemi ve düzenli olarak denetlenmesi, tüm harici kapıları ve erişilebilir pencereleri kapsayacak şekilde yerleştirilmelidir. Boş alanlar her zaman uyarı sinyalleriyle donatılmış olmalıdır. Kapsama, bilgi işlem odası veya haberleşme odaları gibi diğer alanları da kapsamalıdır.

-İşletme tarafında yönetilen bilgi işleme araçları, fiziksel olarak üçüncü taraflarca yönetilenlerden ayrılmış olmalıdır.

-Hassas bilgi işleme araçlarının yerini gösteren telefon rehberi veya dahili telefon kitapçıkları, başkaları tarafından erişilebilir yerlerde olmamalıdır.

-Tehlikeli ve patlamaya hazır maddeler, güvenli alandan uygun bir uzaklıkta güvenli bir şekilde toplanmalıdır. Kırtasiye malzemeleri gibi tedarikler, gerek duyulmadıkça güvenli alan içinde toplanmamalıdır.

-Yedek donanımlar ve yedekleme ortamı, ana alanda oluşabilecek felaketler sonucundaki yıkımı önlemek üzere uygun bir uzaklıkta yerleştirilmelidir.[105]

Cihaza fiziksel olarak erişebilen saldırganın konsol arabirimi aracılığıyla cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel ekipmanla erişim sağlayarak, hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir kıymeti bulunmamaktadır.[106]

Güvenli alanlarda çalışmak: Personel, güvenli alanın varlığını ve içerde yürütülen faaliyetleri, bilmesi gerektiği kadarından haberdar edilmelidir. Güvenlik sebeplerinden dolayı ve kötü niyetli faaliyetlere fırsat vermemek için güvenli alanlarda denetlenmemiş çalışmalardan kaçınılmalıdır. Güvenli bir alanın güvenliğini genişletmek için ilave denetimler ve kılavuzlar gerekebilir. Bunlar, güvenli alanda çalışan personel veya

---

[105] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.11-13.

[106] Enis Karaaslan, Güvenlik Nedir ? , (09 Mayıs 2006), http://www.birdenbire.com.tr/Guvenlikne.htm

üçüncü tarafların denetiminin yanında burada yer alan üçüncü taraf faaliyetlerinin denetimini de içermelidir.

Ayrılmış dağıtım ve yükleme alanları: Dağıtım ve yükleme alanları denetlenmeli ve eğer mümkünse yetkisiz erişimi engellemek için bilgi işleme araçlarından ayrılmalıdır. Bu gibi bölgeler için güvenlik gerekleri risk değerlendirmesi aracılığıyla belirlenmelidir. Aşağıdaki denetimler göz önünde bulundurulmalıdır .

-Bina dışından bulundurma bölgesine erişim, tanımlanmış ve yetkili personelle sınırlandırılmalıdır.

-Bulundurma bölgesi, dağıtım elemanlarının binanın diğer kısımlarına erişimi kazanmaksızın malzemeleri boşaltabilecekleri şekilde tasarlanmış olmalıdır.

-Dahili kapı açık olduğunda, bulundurma bölgesine ait harici kapıların güvenli olması gerekmektedir.

-Dışarıdan gelen malzemeler, bulundurma bölgesinden kullanım noktasına taşınmadan önce, olası tehlikelere karşı kontrol edilmelidir

-Dışarıdan gelen malzemeler, eğer uygunsa alana girişinde kaydedilmelidir.

1.5.2. Teçhizat Güvenliği

Teçhizat güvenliğinden amaç, varlıkların kayıplarını, hasar veya tehlikelerini ve ticari faaliyetlerdeki kesilmenin önlenmesidir. Teçhizatlar güvenlik tehditlerinden ve çevresel tehlikelerden fiziki olarak korunmalıdır. Teçhizatların korunması (alan dışında kullanılanlar dahil) veriye yetkisiz erişim riskini azaltmak ve kayıp ve hasara karşı korumak için gereklidir.

Tehlikelere veya yetkisiz erişimlere karşı teçhizatları korumak için, donanım yerleştirilmesi, güç kaynakları, kablo güvenliği, donanım bakımı, işletme dışında güvenlik ve donanımların tekrar kullanımı için özel denetimlere gerek duyulabilir. Bu süreçlerde alınacak önlemleri aşağıdaki başlıklar altında özetlenmiştir:

Donanım yerleştirilmesi: Teçhizatlar, çevresel tehditler ve tehlikelerden oluşan riskleri ve yetkisiz erişim fırsatlarını azaltmak üzere yerleştirilmeli ve korunmalıdır. Aşağıdaki denetimler göz önünde bulundurulmalıdır.

-Teçhizatlar iş alanları içinde gereksiz erişimi azaltmak üzere yerleştirilmelidir.

-Hassas veriler tutan bilgi işleme ve yükleme araçları, kullanımları sırasında gizlice izlenme riskini düşürmek üzere yerleştirilmelidir.

-Özel koruma gerektiren öğeler, gereken genel koruma seviyesini düşürmek için ayrılmalıdır.

- Denetimler, olası tehditlerle ilgili riskleri en aza indirmek için kurulmalıdır.

-Bir organizasyon, yiyecek, içecek ve sigara içme politikalarını bilgi işleme araçlarına yakınlığına göre gözden geçirmelidir.

-Çevresel şartlar, bilgi işleme araçlarının faaliyetlerini geri dönülemez biçimde etkileyen şartlara göre gözlemelidir.

-Endüstriyel çevreler içindeki teçhizatlar için, dokunmaya duyarlı klavyeler gibi özel koruma yöntemleri düşünülmelidir.

-Yakın çevrede oluşan felaketler örneğin komşu binada çıkan bir yangın, çatıdan akan su veya zemin kat seviyesinden aşağıdaki katlara akan su veya caddede olan bir patlama göz önünde bulundurulmalıdır.

Güç kaynakları: Teçhizatlar, güç kaynağı bozulmalarından veya diğer olağandışı elektriksel olaylardan korunmalıdır. Donanım üreticisinin belirttiği özelliklere uygun elektrik kaynağı sağlamalıdır.

Kablo güvenliği: Veri taşıyan veya bilgi hizmetlerini destekleyen güç ve haberleşme kabloları, durdurmalardan veya hasarlardan korunmalıdır.

Donanım bakımı: Teçhizatların, elverişliliğinin ve güvenilirliğinin garanti edilmesi için doğru bir biçimde bakımı sağlanmalıdır.

Çevre dışı teçhizatların güvenliği: Sahibine bakmaksızın, bilgi işleme için organizasyonun çevresi dışında her donanımın kullanımı yönetim tarafından yetkilendirilmelidir. Sağlanan güvenlik organizasyonun çevresi dışında çalışmanın risklerini dikkate alarak, aynı amaçla alan içinde kullanılan teçhizatlarla eşit olmalıdır. Bilgi işleme teçhizatları, ev çalışması için tutulan veya normal iş yerleşiminden uzağa taşınan her çeşit kişisel bilgisayarları, düzenleyicileri, cep telefonlarını, kağıt veya diğer belgeleri içerir.

Teçhizatların düzenlenmesi ve tekrar kullanımı: Bilgi, teçhizatların dikkatsizce düzenlenmesi ve tekrar kullanımıyla tehlikeye girebilir. Hassas bilgiler içeren depolama aygıtları, standart silme fonksiyonunu kullanmak yerine, fiziksel olarak yok edilmeli veya güvenli olarak üstüne yazılmalıdır. Depolama ortamı içeren, örneğin takılmış sabit diskler, teçhizatların tüm öğeleri, tüm hassas verilerin ve lisanslı yazılımların

düzenlenmeden önce kaldırılmış olduğunu veya üstüne yazılmış olduğunu temin edilmesi için kontrol edilmelidir.[107]

1.5.3. Genel Denetimler

Güvenlik denetimi, bir kurumun güvenlik altyapısının, güvenlik politikasının, prosedürlerinin ve personelinin ayrıntılı bir biçimde ele alınması, zayıf yönlerin tespiti ve bu zayıflıkların giderilmesi için öneriler sunulmasıdır. Başarılı bir denetim, tüm ilgili tarafların işbirliği ile gerçekleştirilebilir. Genelde güvenlikle ilgili bir denetim söz konusu olduğunda, birçok insan olumsuz bir önyargıya kapılır ve rahatsız olur. Bununla birlikte, güvenlik denetimi kurum içinde güvenlik politikasına uygun çalışılıp çalışılmadığının tespitinde kullanılabilecek tek yoldur.[108]

Denetlenecek faaliyetler, personel tarafından temiz masa ve ekran politikasının uygulanabilirliği ve teçhizatların uygun kullanımı başlıkları altında sınıflandırabilir ve bunlara ilişkin detaylar aşağıda sunulmaktadır:

Temiz masa ve temiz ekran politikası: Organizasyonlar, normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kağıtlar ve kaldırılabilir depolama ortamları için temiz masa politikasını uygulamayı ve bilgi işleme araçları için temiz ekran politikasını uygulamayı göz önünde bulundurmalıdır. Politika, bilgi güvenlik sınıflandırmalarını, yerini tutan riskleri ve organizasyonun kültürel konularını dikkate almalıdır. Masalarda bırakılmış bilgilerin yangın, sel veya patlama gibi felaketlerde hasar görme ve yok olma olasılığı çok yüksektir. Aşağıdaki denetimler göz önünde bulundurulmalıdır.

-Uygun olan yerlerde, kağıt ve bilgisayar ortamı, kullanılmadığında özellikle de çalışma saatleri dışında uygun kilitli depolarda veya diğer çeşit güvenlik mobilyalarında depolanmalıdır.

-Hassas ve önemli iş bilgileri, gerekmedikleri zamanda özellikle de büro boş olduğunda, kilitlenmelidir (ideal olarak yangına dayanıklı korumalarda veya dolaplarda)

---

[107] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.11-13.

[108] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.30.

-Kişisel bilgisayarlar ve bilgisayar terminalleri ve yazıcılar, başıboş olduklarında oturum açık olarak bırakılmamalılardır ve anahtar kilitler, şifreler veya diğer denetimler aracılığıyla kullanılmadıkları zamanlarda korunmalıdırlar.

-Gelen ve giden mesaj noktaları ve başıboş faks veya teleks makineleri korunmalıdır.

-Fotokopi makineleri, normal çalışma saatlerinin dışında kilitlenmelidir (veya yetkisiz kullanımlardan başka yollardan korunmalıdır).

-Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen temizlenmelidir.

Teçhizatların kullanımı: Teçhizat, bilgi veya yazılım yetkisiz olarak alan dışına çıkarılmamalıdır. Uygun ve gerekli olan yerlerde, geri döndürüldükleri zaman teçhizatların kaydedilmeleri gerekir. Teçhizatların yetkisiz kaldırımını tespit etmek için nokta denetimler üstlenilmelidir. Nokta denetimlerin uygulanacağı hakkında kişiler haberdar edilmelidir.

1.6. Haberleşme ve İşletim Yönetimi

Haberleşme ve işletim yönetiminden amaçlanan, bilgi işlem tesislerinin doğru ve güvenle işletildiğinden emin olunmasıdır. Bu amaçla tüm bilgi işlem tesislerinin işletim ve yönetim prosedürleri ile sorumlulukları tesis edilmelidir. Haberleşme ve işletim yönetimi, işletim prosedürleri ve sorumlulukların belirlenmesi, sistem planlama, kötü niyetli yazılımlara önlemler, yedekleme, ağ yönetimi, bilgi ortamı yönetimi ve bilgi/yazılım değişimi toplam yedi başlık altındaki süreçleri kapsamaktadır.

1.6.1. İşletim Prosedürleri ve Sorumluluklar

İşletim prosedürlerinin ve sorumlulukların belirlenmesi ile bilgi işleme olanaklarının doğru ve güvenli işletimi sağlanmaktadır. Prosedürlerde sistemin, bilerek ya da bilmeyerek yanlış kullanım riskini bulunduğu yerlere göre görevler ayrılmalıdır. İşletim prosedürleri ve sorumlulukları, temel olarak beş alt başlık altında incelersek, bunlar; yazılı prosedürler, olay yönetim prosedürleri, değişim yönetimi, görevlerin ayrılması ve geliştirme ve işletim tesislerinin ayrılmasından oluşmaktadır.

Yazılı işletim prosedürleri: Güvenlik politikasında tanımlanan işletim prosedürleri, yazılı ve sürekli olmalıdır. İşletim prosedürleri, gücünü yönetimden alan resmi belge ve

değişiklikler şeklinde işlem görmelidir. Bilgisayarların açılıp kapanması, yedekleme, teçhizatın bakımı, bilgisayar odası ve posta alma-gönderme yönetimi ve emniyet gibi işlem ve iletişim tesisleriyle beraber yürütülen sistem idame faaliyetleri için yazılı prosedürler hazırlanmalıdır.

Olay Yönetim Prosedürleri: Olay yönetim prosedürleri ve sorumlulukları, güvenlik olaylarına çabuk, etkin ve bir sıra dahilinde müdahale edilmesini sağlamak maksadıyla tesis edilmiştir. Bu konu ile ilgili olarak aşağıdaki kontroller göz önüne alınmalıdır.

-Güvenlikle ilgili tüm potansiyel türleri kapsayan prosedürler oluşturulmalıdır.

-Prosedürler, normal, ani durum planlarını içerecek şekilde hazırlanmalıdır.

-Resmi bulgular ve kanıta benzer şeyler, uygun şekilde toplanıp emniyet altına alınmalıdır.

-Güvenlik ihlallerinin giderilmesi hareketi ve düzgün sistem arızaları, dikkatli bir biçimde ve resmi olarak kontrol altında olmalıdır.

Değişim Yönetimi: Bilgi işlem tesisleri ve sistemlerine dair değişiklikler kontrol altında tutulmalıdır. Bilgi işlem tesisleri ve sistemlerinin değişikliklerine ilişkin kontrolün yetersizliği, sistem ya da emniyet konusundaki aksaklıkların en önde gelen nedenlerindendir. Resmi yönetim sorumlulukları ve prosedürler, teçhizat, yazılım ve prosedürlere ilişkin tüm değişiklerin tatmin edici bir şekilde kontrolünü sağlayan bir konumda olmalıdır. İşletim kuralları, en katı değişiklik kurallarına maruz kalmalıdır. Programlar değiştiğinde, konu ile ilişkili tüm hususları kapsayan bir izleme kaydı tutulmalıdır.

Görevlerin Ayrılması: Görevlerin ayrılması, kazara ya da kasten sistemin yanlış kullanım riskini azaltan bir metottur. Yetki verilmeyen değişikliklerin meydana gelmesini ya da bilgi veya servislerin yanlış kullanımını azaltmak maksadıyla belli görevlerin yerine getirilmesi ya da yönetimi veya sorumluluk alanlarının ayrılması değerlendirilmelidir. Küçük organizasyonlar, bunu başarılması zor bir kontrol metodu olarak değerlendirebilirler, fakat bu prensip mümkün olabildiği kadar uygulanmalıdır. Ne zaman ayrım yapmak zorlaşırsa, faaliyetlerin izlenmesi, yönetim gözetimi ve kayıtların denetimi gibi diğer kontroller dikkate alınmalıdır. Güvenlik denetiminin bağımsız olması önem arz etmektedir. Göz ardı edilmemelidir ki, hiç kimse, fark

edilmeden tek kişinin sorumluluğunda bulunan yerlerde dolandırıcılık suçunu işleyemez.

Geliştirme ve İşletim Tesislerinin Ayrılması: Geliştirme, deneme ve işletim tesislerinin ayrılması, ilgili rollerin ayrılmasını başarmak bakımından önemlidir. Geliştirme sürecinden işletim durumuna yazılımın transfer edilmesinin kuralları tanımlanmalı ve yazılı olmalıdır. Geliştirme, deneme ve işletim faaliyetlerini ayırmak suretiyle, iş verilerine ve işletim yazılımına yetkisiz erişimi veya kazara değişiklik yapma tehlikesi azaltılır.

1.6.2. Sistem Planlama ve Kabul

Planlamadan amaçlanan, sistem arızalarını en az seviyeye indirilmesidir. İleri planlama ve hazırlık, yeterli kapasite ve kaynakların uygunluğunu kesinleştirmek için ihtiyaç duyulur. Gelecek kapasite ihtiyaçlarının projeksiyonları, sistemin aşırı yükleme riskine karşılık yapılmalıdır. Yeni sistemin işletim ihtiyaçları belirlenmeli, yazılmalı ve kabul edilip kullanılmadan denenmeli, sistem testleri yapılmalıdır. Bu kapsamda kapasite planlama ve sistem testlerinin içeriğinde gerçekleştirilecek faaliyetleri göz gezdirecek olursak, bunlar:

Kapasite planlama: Kapasite talepleri izlenmeli ve gelecekteki kapasite ihtiyaçlarının projeksiyonları yeterli işlem gücü ve uygun depolamadan garanti olmak şartıyla yapılmalıdır. Yeni iş ve sistem ihtiyaçlar ile organizasyonun bilgi işlemindeki mevcut ve tahmin edilen eğilimler hesaba katılmalıdır. Yeni kapasitenin tedariki için daha çok para ve zaman gerektiğinden ana bilgisayar konumundaki bilgisayarlara özel önem verilmelidir. Ana sistemlerin yöneticileri, işlemciler, esas saklama, dosya saklama, yazıcılar, diğer çıktı aygıtları ve iletişim sistemlerini kapsayan anahtar sistem kaynaklarının kullanımını izlemelidirler. Özellikle iş konuları ya da bilgi sistem aygıtları ile ilişkili mevcut eğilimleri tanımlamalıdırlar.

Sistem kabulü: Yeni bilgi sistemleri, yükseltmeler ve yeni versiyonların kabul etme kriterleri tespit edilmeli ve sistem kabul edilmeden önce denenmelidir. Yöneticiler, ihtiyaçların ve yeni sistemin kabulü için belirlenen kriterlerin açıkça ifade edildiğinden, mutabık kalındığından, yazıldığından ve denendiğinden emin olmalıdır.

1.6.3. Kötü Niyetli Yazılımlara Önlemler

Yazılım ve bilgi işlem tesisleri, bilgisayar virüsleri, ağ kurtları, Truva atları ve mantık bombaları gibi kötü niyetli yazılımın girişine karşı hassastır. Kullanıcılar, kötü niyetli ve yetkisiz yazılımlardan haberdar edilmeli; yöneticiler uygun olan yerlerde bunları girişlerini önleyen veya tespit eden özel kontrol tedbirlerini tanıtmalıdır. Özellikle, kişisel bilgisayarlarda bilgisayar virüslerini tespit eden ve koruyan tedbirlerin alınması gereklidir.

1.6.4. Yedekleme

Kararlaştırılan yedekleme stratejisini sürdürmek, veri kopyalarının yedeklenmesini almak, olayların ve hataların kayıt altına alınması ve mümkün olması halinde donanımın bulunduğu çevrenin izlenmesine dair alışılmış prosedürler, tesis edilmelidir. Amaç, bilgi işlem ve iletişim hizmetlerinin kullanılabilirliliği ve bütünlüğünün sürdürülmesidir. Bilgi yedeklemesi, işletme kayıtları ve hata kayıtları başlıkları altında sunulan faaliyetlerin içerikleri:

Bilgi yedeklemesi: Gerekli iş bilgisi ve yazılımın yedekleme kopyaları düzenli olarak alınmasıdır. Tüm iş bilgileri ve yazılımın bir felaket ya da ortamın zarar görmesi sonrası yeniden kurtarılabilen yeterli yedekleme tesislerinin bulunmasını kapsamaktadır.

İşletme kayıtları: İşletmeler, yaptıkları faaliyetlerin bir kaydının yapılması ve bağımsız denetimlere tabi tutulmasını içermektedir.

Hata kayıtları: Bilgi işlem ya da iletişim sistemleri ile ilgili olarak kullanıcılar tarafından rapor edilen hataların kaydının tutulmasını ve ilgili hataların rapor edilmesi ve düzeltici tedbirlerin alınmasını içermektedir.[109]

1.6.5. Ağ Yönetimi

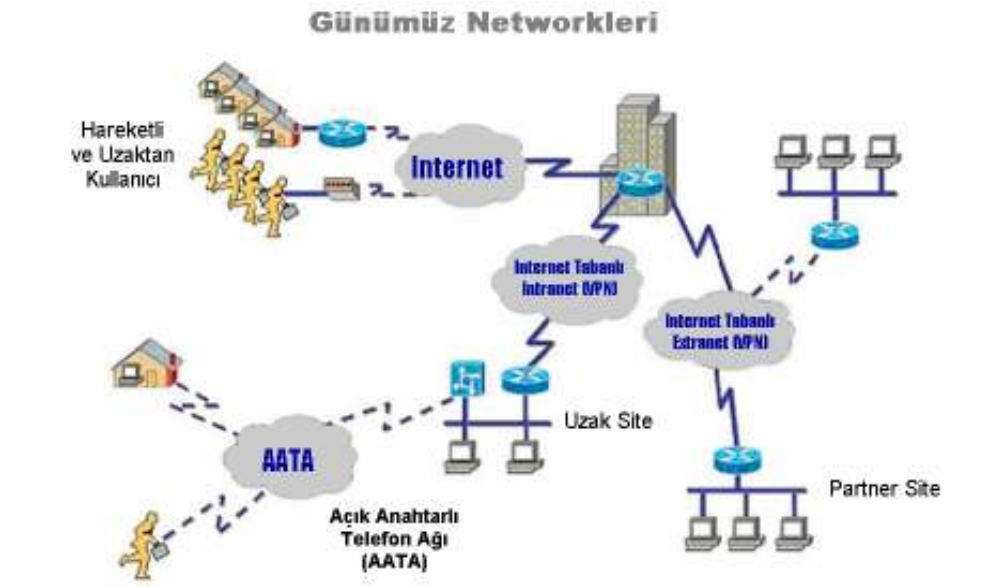
Bir yerel alan ağını oluşturan sunucu ve istemciler kablolu ya da kablosuz olarak birbirleriyle iletişim kurabilirler. Bir ağ ortamında kullanılan sistemlerin ve bu sistemler üzerinde saklanan her türlü verinin korunması ancak etkin bir ağ güvenliği denetimi ile yapılabilir. Bu kapsamda öncelikle bir ağın güvenilirliği ile ilgili olarak Güvenilir Sistem teriminin açıklanması gerekebilir.

---

[109] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.15-23.

Güvenilir Sistem, hem ağ içi haberleşmede hem de ağın dış dünya ile haberleşmesinde ağ trafik yoğunluğunun artması, içerden/dışarıdan yetkisiz erişim veya önemli bir verinin saklanması gibi durumlarda hiç bir zafiyet oluşturmadan ağ güvenliğini sağlayabilen güçlü sistemdir. Bu sistem hem kullanılan ağ cihazlarının ve hem de bu cihazlar üzerinde çalışan uygulama programlarının iyi bir konfigürasyonla seçilmesi ve çalışmasının devamı ile mümkündür.

Günümüzde kullanılan ağ yapıları ve güvenlik önlemleri Şekil 25'te sunulmuş olup, ağ güvenliğini sağlayabilmek için Güvenlik Duvarları, Saldırı Tespit Sistemleri (IDS) ve Rol Tabanlı Erişim Kontrolleri (RBAC) kullanılabilir. Örneğin Internet, güvensiz bir ağdır. Internet'i güvensiz yapan paylaşımın fazlalığı ve insanın doğal yok etme içgüdüsüdür. Yerel ağdaki özel bilgileri Internet'in getirdiği risklerden korumak için Güvenlik Duvarı kullanılır. Güvenlik Duvarları, bir ya da birden fazla ağ bölümü arasında duran ve bu ağlar arasındaki geçişleri denetleyen sistem ya da sistemler bütünüdür. Dolayısıyla, çeşitli ağ parçalarının birbiriyle iletişim kurmalarını kısıtlamak ve bir ağı veya sunucuyu korumak amaçlı olarak Güvenlik Duvarı kullanılabilir. [110]



Şekil 25. Günümüz Ağları ve Güvenlik Önlemleri
Bilişim Sistemleri Güvenliği El Kitabı,2003,s.37.

[110] Bilişim Sistemleri Güvenliği El Kitabı (Ankara: Türkiye Bilişim Derneği, Haziran 2003), s.36.

Bilgisayar ağlarındaki güvenliği tesis edip sürekliliğini sağlamak için, bir dizi kontrole gereksinim duyulur. Ağ yöneticileri, ağlardaki verinin güvenliği ve bağlı bulunulan servislere yetkisiz kişilerce erişilmesinden korunmasını sağlamak maksadıyla kontrolleri gerçekleştirmelidirler.[111]

1.6.6. Bilgi Ortamı Yönetimi

Bilginin yetkisiz kişilerce ifşa edilmesi ya da yanlış maksatlarla kullanılmasını önlemek için bilgi güvenliği ve yönetimi için prosedürler oluşturulmalıdır. Kendi içindeki sınıflandırmayla tutarlı olarak, yazılı belgeler, bilgisayar sistemleri, ağlar, mobil bilgisayarlar, mobil iletişim, posta, sesli posta, sesli iletişim, çoklu ortam, posta hizmetleri/tesisleri, faks makinesi ve diğer hassas parçaların kullanılırken (örneğin, boş çekler, fatura vb.) bilginin yönetilmesi için prosedürler düzenlenmelidir. Bu maksatla aşağıdaki hususlar dikkate alınmalıdır:

-Tüm ortamın etiketlenmesi ve yönetilmesi ,

-Yetkisiz kişileri tanımlamak için erişim sınırlamaları,

-Veri kullanan yetkisiz kişiler için bir resmi kaydın tutulması,

-İşlemin doğru bir şekilde tamamlayan ve çıktı geçerliliğinin uygulamaya koyan girdi verisinin eksiksiz olmasının sağlanması,

-Kendi duyarlılığı ile uygun bir seviyede çıktıyı bekleyen zarar görmüş verinin korunması,

-Ortamın, üretici firma şartlarına uygun bir yerde bulundurulması,

-Veri dağıtımını en alt düzeyde tutulması,

-Yetkisiz kişilerin dikkatini çekebileceğinden verinin tüm kopyalarındaki işaretlemelerin temizlenmesi,

-Düzenli aralıklarla yetkisiz kişilerin ve dağıtım listelerini gözden geçirilmesidir.

Gereksinim ortadan kalktığında, emniyetli ve kesin bir şekilde bilgi ortamından kurtulmak gerekir. Hassas bilgiler ortamın yok edilmesi esnasında dikkatsiz kişilerce başka insanlara sızabilir. Ortamın kesin olarak yok edilmesindeki resmi prosedürler oluşturulmalı ve bu tehlikeyi en aza indirmek maksadıyla denetimler yapılmalıdır.

---

[111] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.24.

1.6.7. Bilgi ve Yazılım Değişimi

BGYS'de organizasyonlar arasında yazılımın ve bilginin değişimi, kontrol altında bulundurulmalı ve ilgili yasalarla uyumlu olmalıdır. Bilgi ve yazılım değişimleri, anlaşma esaslarına göre yapılmalıdır. Nakil esnasındaki ortam ve bilgiyi korumak için prosedürler belirlenmelidir. Karşılıklı elektronik veri değişimi, elektronik ticaret ve elektronik posta ile kontrol tedbirlerinin gereksinimleriyle birleşen iş ve güvenlik konuları göz önünde tutulmalıdır.

Bilgi ve yazılım değişimi süreçlerinin kapsamı:

- Bilgi ve yazılım değişim anlaşmaları,
- Nakil esnasındaki bilgi ortamının güvenliği,
- Elektronik ticaret güvenliği,
- Elektronik ofis sistemlerinin güvenliği,
- Halka açık sistemler,
- Bilgi değişiminin diğer şekilleri, başlıkları altında aşağıda sunulmuştur.

Bilgi ve yazılım değişim anlaşmaları: Bazıları resmi olan ve uygun olan hallerde üçüncü şahıslarla yapılan yazılım antlaşmalar, organizasyonlar arasında bilgi ve yazılımın değişimi için yapılmalıdırlar. Bu tür bir anlaşmanın güvenlik içeriği, ilişkili olduğu işin duyarlılığını yansıtmalıdır.

Nakil esnasındaki bilgi ortamının güvenliği: Bilgi, postaya verildiği ya da kurye ile gönderildiği hallerde fiziki olarak hareket halindedir ve yetkisiz kişilerin erişimine, yanlış maksatlarla kullanılmalara ya da zarar görmeye karşı hassastır. Siteler arasında gidip gelen bilgisayar ortamının güvenliği için aşağıdaki kontrol tedbirleri uygulanmalıdır.

-Güvenilir kuryeler ve ulaşım vasıtaları seçilmelidir. Yetkili kuryelerin bir listesi, kuryeler için yapılan tanımları kontrol eden bir prosedür ve yönetimle kararlaştırılmalıdır.

-Üretici firmanın şartlarına uygun ve içerdiği bilginin hareket halinde iken zarar görmekten koruyan yeterli bir paketleme olmalıdır.

-Gerektiğinde, yetkisiz açma ve değiştirmeleri önlemek maksadıyla, özel kontrol tedbirleri uygulanmaktadır.

Elektronik ticaret güvenliği: Elektronik ticaret, karşılıklı elektronik veri değişimi, elektronik posta ve Internet gibi geniş halk kitlelerinin erişimine açık çevrim içi işlemlerin kullanımını içerir. Elektronik ticaret, hileli kazanç faaliyetleri, anlaşma itilafları ya da bilginin değişikliğe maruz kalması gibi bir dizi ağ şebekesi tehditlerine karşı hassastır. Elektronik ticareti bu tür tehditlerden korumak için kontrol tedbirleri uygulanmalıdır.

Elektronik ofis sistemlerinin güvenliği: Elektronik ofis sistemleriyle müşterek iş ve güvenlik tehlikelerini kontrol etmek maksadıyla politikalar ve genel hatlar belirlenmeli ve uygulanmalıdır. Bunlar; belgelerin, bilgisayarların, mobil bilgi işlem ve mobil iletişimin, postanın, sesli mesajın, sesli haberleşmenin, çoklu ortamın, posta teşkilatının ve faks makinelerinin kombinasyonunu kullanarak iş bilgilerinin paylaşılması ve düşüncelerin daha hızlı yayılması konusunda fırsat sağlamaktadır.

Halka açık sistemler: Yetkisiz kişilerin şirketin itibarını zedeleyebilecek şekildeki değişiklikler yapmalarını önleyerek elektronik olarak yayılan bilginin bütünlüğünü korumaya özen gösterilmelidir. Halka açık sistemlerdeki bilgi, örneğin, Internet yolu ile erişilen Web sayfasındaki bilgiler, ticaretin yapıldığı ya da sistemin bulunduğu mahkemelerdeki yasalar, kurallar ve düzenlemelerle uyumlu olmaya ihtiyaç gösterir. Bilgi halka yayılmadan önce resmi bir yetkilendirme prosesi oluşturulmalıdır.

Bilgi değişiminin diğer şekilleri: Ses, faks ya da video iletişim gereçlerini kullanarak bilgi değişimini önlemek yerine, prosedürler ve kontrol tedbirleri kullanılmalıdır. Bilgi, farkında olmadan ve kullanılan politika ve prosedürler nedeniyle doğru olarak kullanılmayabilir. Örneğin, halka açık bir yerde cep telefonu ile çok yüksek sesle konuşmak, sesi çok açık olan bir bant kaydı dinlemek, sesli mesaj sistemine yetkisiz kişilerin erişim sağlaması, faks cihazını kullanarak faksın yanlış adrese gönderilmesi verilebilir. Ancak iletişim gereçleri kullanılamazsa, iş ilişkileri bozulabilir, bilgi yanlış değerlendirilebilir. Bu nedenle, ses, faks ve video iletişiminde kullanılırken takip edilecek prosedürlerin açık bir şekilde ifade edilmesine gerek vardır.[112]

[112] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.24-53.

1.7. Erişim Denetimi

Bilişim güvenliğinde en önemli konularda biri, kaynaklara kimin nasıl eriştiğini kontrol etmek, bu sayede bilgi üzerinde yetkisiz değiştirme ve açığa çıkarma olaylarını engellemektir. Bu amaçla yapılan faaliyetlere genel olarak erişim denetimi denir. Bir kullanıcı bilgisayarından ağ üzerindeki bir dizine ulaşmak istediğinde ona kullanıcı adı ve parola soran bir ekranla karşılaşması, erişim denetimine örnek olarak verilebilir. Erişim denetimi, yazılım ve donanım tabanlı olarak sağlanabilir. [113]

Bilgiye erişim denetim yöntemleri, yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan, kullanıcıların tüm yaşam döngüsü basamaklarını kapsamalıdır. Sadece gerekli olan personele, gerektiği kadar erişim yetkisi sağlanmalı, erişim kontrolü kuralları ve süreçleri belirlenmelidir. Kullanıcı kayıt, kullanıcıya tanınan ayrıcalık özellikleri, kullanıcı şifre yönetimi, erişim haklarının gözden geçirilmesi gibi işlemler için detaylı talimatlar oluşturulmalı, her bir konuya ilişkin isterler/kurallar politika dokümanına yansıtılmış olmalıdır. Kullanıcılar erişim hakları ile bu konuda kendi sorumluluk ve yükümlülükleri hakkında bilgilendirilmiş, bilinçlendirilmiş olmalıdır.[114]

Erişim denetim yöntemlerini:

- Kullanıcı sorumluluğu,
- Ağ erişimi denetimi,
- İşletim sistemi erişim denetimi,
- Uygulama erişimi denetimi,
- Sistem erişiminin gözlenmesi ve kullanımı,
- Mobil bilgi işlem ve uzaktan çalışma,

olmak üzere toplam altı başlık altında aşağıda sunulmuştur:

Kullanıcı sorumluluğu: Etkin bir güvenlik için yetkili kullanıcıların işbirliği çok önemlidir. Kullanıcılar, etkin erişim denetimlerini, özelliklede parolaların kullanımı ve

---

[113] Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.41.
[114] Şule Küçükoğlu, Uygun Güvenlik Çözümüne Yolculuk, (16 Mayıs 2006), http://www.infosecurenet.com/macroscope/macroscope6.pdf

kullanıcı teçhizatlarının güvenliği ile ilişkili olarak, sağlamak için sorumlulukları hakkında bilgilendirilmelidir. Kullanıcılar parolaların seçimi ve kullanımında doğru güvenlik uygulamalarını izlemelilerdir.

Ağ erişimi denetimi: Ağ oluşturulmuş hizmetlerin korunması için, dahili ve harici kurulmuş ağların her ikisine de erişim denetlenmelidir. Bu, ağlara ve ağ hizmetlerine erişimi olan kullanıcıların, ağ hizmetlerinin güvenliğini tehlikeye atmadıklarından emin olmak gereklidir.

İşletim sistemi erişim denetimi: Yetkisiz bilgisayar erişiminin engellenmesi için, işletim sistemi düzeyinde güvenlik Araçları, bilgisayar kaynaklarına erişimi engellemek için kullanılmalıdır. Tüm kullanıcılar (işlemciler, ağ yöneticileri, sistem programcıları ve veritabanı yöneticileri gibi teknik destek personelleri dahil), yapılan işlemlerin sonradan sorumlu bireyler kapsamında izlenebilmesi için, kişisel ve tek kullanımlara ilişkin özel birer tanımlayıcıya (kullanıcı kimliği) sahip olmalıdırlar. Ayrıca tanımlanmış bir çalışmazlık (etkinsizlik) süresinden sonra erişim hizmetini kapatılması için, terminal zaman aşımı ve yüksek riskli uygulamalarda bağlantı süresi sınırlaması dikkate alınmalıdır.

Uygulama erişimi denetimi: Uygulama sistemleri içersinde erişimi kısıtlamak için güvenlik araçları kullanılmalıdır. Yazılım ve bilgiye mantıksal erişim, yetkili kullanıcılarla kısıtlanmalıdır.

Sistem erişiminin gözlenmesi ve kullanımı: Erişim denetim politikasından sapmaları tespit etmek için sistemler gözlenmeli ve güvenlik arızalarının çıkması ihtimaline karşı bulgu sağlayabilmek için gözlenebilir olayları kaydedilmelidir. Sistemin gözlenmesi, kabul edilmiş (benimsenmiş) denetimlerin etkinliğinin kontrol edilmesine ve erişim politikası modeline uygunluğunun teyit edilmesine izin verir.

Mobil bilgi işlem ve uzaktan çalışma: Mobil bilgi işlem kullanıldığında, korunmasız çevrelerde çalışmaya ait riskler dikkate alınmalı ve uygun koruma yöntemleri uygulanmalıdır. Uzaktan çalışma gerektiğinde, işletme çalışılan alana uygun koruma sağlamalı ve bu çalışma şekilleri için uygun düzenlemelerin yapıldığını temin etmelidir.

1.8. Sistem Geliştirme ve Bakım

Sistem geliştirme ve bakım süreçlerinde güvenliğin ele alınması ve mevcut uygulamaların güvenli olarak bakımının sağlanması beklentilerini içerir.

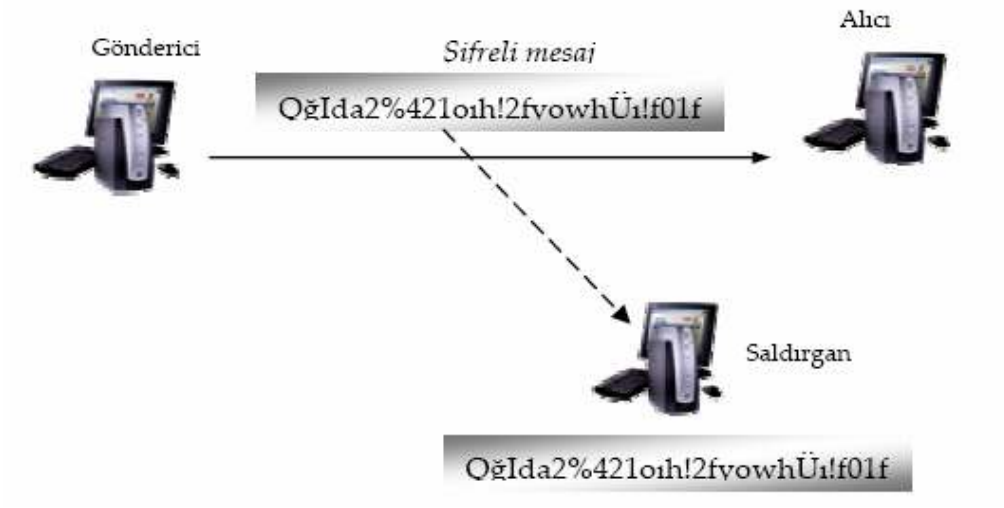
Bilgi işlem sistemlerinin geliştirilmesinden önce, güvenlik gerekleri belirlenmeli ve bu konuda uzlaşmaya varılmalıdır. Güvenlik gerekleri ve kontroller ilgili bilgi desteklerinin ve güvenlikteki bir aksaklıktan ya da güvenlik yoksunluğundan doğabilecek muhtemel iş kaybının iş açısından değerini yansıtmalıdır. Güvenlik gereklerini incelemeye ve bunları karşılayacak olan kontrolleri belirlemeye ilişkin altyapı risk değerlendirmesi ve risk denetimidir. Tasarım aşamasında yürütülen kontrollerin kurulması ve bakımı, kurulum sırasında ya da kurulumdan sonra dahil edilenlere göre, belirgin ölçüde daha ucuzdur.

Sistem geliştirme ve bakım süreçlerini aşağıdaki başlıklar altında açıklamaya çalışalım:

- Uygulama sistemlerinde güvenlik,
- Şifreleme kontrolleri,
- Sistem dosyalarının güvenliği,
- Geliştirme ve destek süreçlerinde güvenlik.

Uygulama sistemlerinde güvenlik: Uygulama istemlerindeki kullanıcı verilerinin kaybedilmesini, değişmesini ya da hatalı kullanımının önlenmesi amacı ile, kullanıcı yazılı uygulamaları da dahil olmak üzere, uygun kontroller ve kontrol zincirleri ya da etkinlik kayıtları tasarlanmalıdır. Bunlar arasında, girilen verilerin, iç işleyişin ve son verilerin geçerli kılınması yer almalıdır.

Şifreleme kontrolleri: Bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması için şifreleme sistemler ve teknikler kullanılmalıdır. Şifrelemenin bir çözümün uygun olup olmadığı konusunda bir karar vermek risklerin değerlendirilmesi ve kontrollerin seçilmesi yolundaki daha geniş bir işlemin bir parçası olarak görülmelidir. Bilginin verilmesi gereken seviyesinin belirlenmesi için bir risk değerlendirmesi yapılmalıdır. Daha sonra bu değerlendirme, şifrelemenin uygun olup olmadığını, ne tür ve hangi amaçla ve hangi iş etkinlikleri için bir kontrol uygulanması gerektiğini belirlemek için kullanılabilir. Şekil 26'da bir saldırganın hattı dinleyerek mesajı ele geçirmesi gösterilmiştir. Ancak saldırgan mesaja sahip olsa bile, mesaj kriptolu olduğundan içeriği konusunda bilgi sahibi olamaz.



Şekil 26. Hattı Dinleyen Bir Saldırgana Karşı Şifrelemenin Kullanılışı

Bilişim Güvenliği,2003, s.32.

Sistem dosyalarının güvenliği: İşletim sistemlerinin bozulma riskini asgariye indirmek için bazı kontroller yapılması gerekir. Bu kontroller şu şekilde değinilebilir:

-İşletim programları kütüphanesinin güncellenmesi yalnız uygun yönetim yetkilendirmesi ile tayin edilen kitaplık görevlisi tarafından gerçekleştirilebilir.

-Mümkünse, işletim sistemleri yalnız makine kodu taşımalıdır.

-Başarılı testlere ve kullanıcı onayına ilişkin kanıtlar elde edilinceye ve karşılık gelen program kaynak belgelikleri güncelleninceye kadar, makine kodu bir işletim sistemi üzerine yerleştirilmemelidir.

-İşletim belgeliklerine uygulanan tüm güncellemelerini içeren bir kontrol kaydı tutulmalıdır.

-Beklenmedik durum önlemi olarak yazılımın önceki versiyonları saklanmalıdır.

Geliştirme ve destek süreçlerinde güvenlik: Uygulama sistemlerinden sorumlu yöneticiler projenin ve destek ortamının güvenliğinden de sorumlu olmalıdırlar. Sistemin ya da işletim ortamının güvenliğini bozmadığından emin olmak için, planlanan tüm sistem değişikliklerinin gözden geçirilmesini temin etmelidirler.

1.9. İş Devamlılığı Yönetimi

İş devamlılık yönetimi; felaketler ve güvenlik başarısızlıkları (örneğin, doğal felaketler, kazalar, araç gereç başarısızlıkları ve kasıtlı hareketlerin sonuçları olabilir)

nedeniyle oluşan bozulmayı, koruyucu ve yenileyici kontrollerin birleşmesi ile, kabul edilebilir bir seviyeye indirmek için uygulanmalıdır.[115]

İş devamlılık ve olağanüstü durum yönetimi, tüm dünyada son yıllarda, özellikle de terör saldırılarının artmasıyla birlikte, üzerinde daha da önemle durulan bir konu haline gelmiştir. Bu kapsamda, kurumlar kendi içlerinde olağanüstü durum organizasyonları oluştururken, tüm ülke boyutuna ulaşan kapsamlı hazırlık ve çalışmalar da gündeme gelmiştir.[116]

Felaketlerin, güvenlik başarısızlıklarının ve servis kayıplarının sonuçları incelenmelidir. Ticari işlemlerin gereken zaman aralıklarında düzeltilebilmesinin devamlılığının sağlanması için olası planlar geliştirmelidir ve uygulanmalıdır. Bu planların diğer bütün ticari işlemlerin bağlantılı bir parçası olması için sürekliliğinin ve pratikliliğinin sağlanması gereklidir. İş devamlılık yönetimi, riskleri tanımlamak ve en aza indirgemek, gelen zararların sonuçlarını sınırlandırmak için kontroller içermelidir ve operasyonlar için zaman sağlanmalıdır. İş devamlılık planlama işlemleri aşağıdakileri ele almalıdır:

-Tüm sorumluluk ve olağan üstü durumlarda yapılacak işlemlerinin belirlenmesi ve karar verilmesi,

-Gerekli zaman aralığında yenilenmenin yapılmasını sağlamak için ilkyardım işlemlerinin uygulanması,

-Karar verilen işlemler ve işlem sıralarının belgelerinin hazırlanması,

-Personele, olağan üstü durumlarda yapılmasına karar verilen işlemlerin ve işlem sıralarının, sorun durumundaki yönetimi de içeren uygun bir eğitimin verilmesi,

-Planların test edilmesi ve güncellenmesidir.

İş birimleri iş devamlılığına yönelik olarak, işlemlerini ikincil merkezden yürütmeyi B Planı olarak ele almışlarsa, bilişim hizmetleri olmaksızın da iş sürekliliğini ne şekilde sağlayabileceklerini bir C Planı çerçevesinde ele almalıdırlar. Bu süreç, işlerin daha çok kağıt ortamında nasıl takip edileceğine yöneliktir. İş birimleri, işin kağıt ortamında nasıl gerçekleştirilebileceğini ifade eden genel bir doküman hazırlamış

---

[115] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.24.

[116] M.Okay, A.Pekel, O.Yaman, D.Soyar , N.Kuleyın, A.Mete, Bilişim Teknolojilerinde Risk Yönetimi, (Kamu Bilişim Platformu, 20 Mart 2006), http://kamubib.tbd.org.tr/dokumanlar/cg2.doc

olmalıdırlar. Tüm planlara ilişkin dokümanların bir kopyası ikincil yerleşmede korumalı bir şekilde hazır tutulmalıdır. Ayrıca, bu yerleşmede ihtiyaç duyulacak her türlü ekipman (bilgisayar, yazıcı, toner, kağıt, telefon, faks, teleks, kırtasiye malzemeleri v.b.) yedek olarak hazır bulundurulmalıdır. Yedek merkezden hizmet verilmesi ile ilgili olarak bilgisayar firmalarıyla yapılacak servis ve destek hizmetleriyle ilgili sözleşmelerde ikinci yerleşmede alınacak hizmetlerle ilgili maddeler bulunmalı ve alınacak hizmetlerin kapsamı doğru ve detaylı olarak tarif edilmelidir.[117]

1.10. Uyumluluk

Bilgi sistemlerinin şekli, operasyonu ve kullanımı herhangi bir güvenlik gereksinimi için, yasal, düzenleyici ve kurucu yaptırımların konusu olabilir. Belirli bir kanuni gereksinim hakkındaki öneriler, organizasyonun kanuni tavsiyecileri tarafından verilmelidir. Kanuni gereksinimler ülkeden ülkeye çeşitlilik gösterir ve bilgilerin bir ülkeden diğer ülkeye geçiş vardır (geçiş köprüsü veri akışı).

Bütün uygun yasal, düzenleyici ve kurucu gereksinimler her bilgi sistemi için kesin olarak tanımlanmalı ve dokümantasyonu yapılmalıdır. Bu gereksinimlerle çakışan belirli kontroller ve bireylerin sorumluluklarının da aynı şekilde tanımının yapılması ve dokümantasyonunun sağlanması gereklidir.

Yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasında uygun işlemler yürürlülüğe sokulmalıdır. Kopya hakkının ihlal edilmesi bir suçtur.[118]

2. TS ISO/IEC 27001 BİLGİ GÜVENLİK YÖNETİM SİSTEMİ (BGYS) (MD.4)

BGYS, bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası olarak adlandırılabilir.

Bir işletme için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ticari ihtiyaçlar ve amaçlardan doğan güvenlik gereksinimlerinden, kullanılan proseslerden ve kuruluşun büyüklüğü ve

---

[117] M.Okay, A.Pekel, O.Yaman, D.Soyar , N.Kuleyın, A.Mete, Bilişim Teknolojilerinde Risk Yönetimi, (Kamu Bilişim Platformu, 20 Mart 2006), http://kamubib.tbd.org.tr/dokumanlar/cg2.doc

[118] TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri (Ankara: Türk Standardları Enstitüsü, 2002), s.24-53.

yapısından etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Basit durumların basit BGYS çözümlerini gerektireceği beklenir.

İşletme etkin bir şekilde işlev görmesi için, bir çok faaliyetini tanımlamalı ve yönetmek durumundadır. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir proses olarak düşünülebilir. Çoğunlukla, bir prosesin çıktısı doğrudan bunu izleyen diğer prosesin girdisini oluşturur. Kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak tanımlanabilir. ISO 27001 standardı, bir kuruluşun BGYS'sini kurmak, gerçekleştirmek, işletmek, izlemek, bakımını yapmak ve etkinliğini arttırmak için bir proses yaklaşımının benimsenmesini özendirir. BGYS kurulumuna yönelik gereksinimleri, aşağıdaki toplam yedi başlık altında açıklanacaktır.Bunlar:

-Genel gereksinimler,

- BGYS'nin kurulması ve yönetilmesi,
- Dokümantasyon gereksinimleri,
- Yönetim sorumluluğu,
- BGYS iç denetimleri,
- BGYS'yi yönetimin gözden geçirmesi,
- BGYS iyileştirme, başlıkları olacaktır.

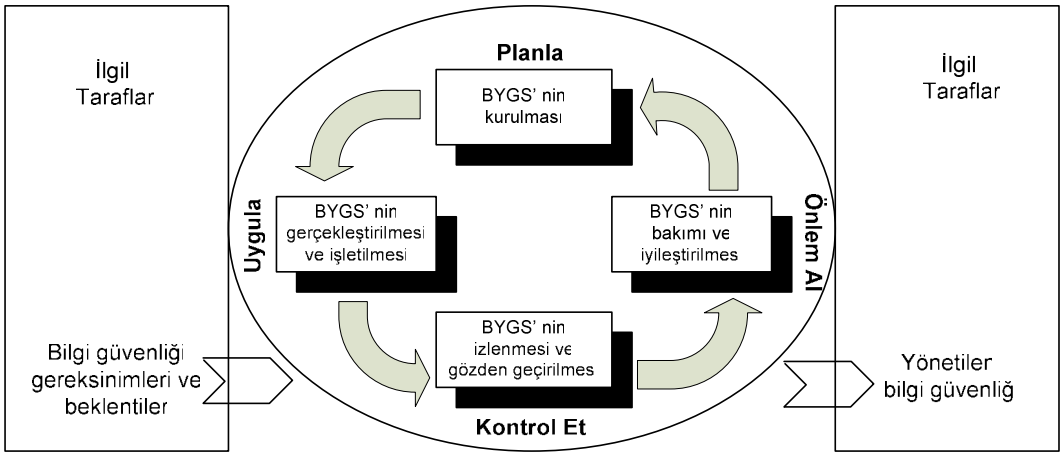
2.1. Genel Gereksinimler (Md.4.1.)

Kuruluş, yazılı hale getirilmiş bir BGYS'yi, kuruluşun tüm ticari faaliyetleri ve riskleri bağlamında, geliştirir gerçekleştirir, sürdürür ve sürekli ilerletir. Bu standardın bir gereği olarak, kullanılan proses, PUKÖ modeline dayanır.[119]

"Planla-Uygula-Kontrol Et-Önlem al" (PUKÖ) modeli olarak bilinen model, bu standart'ta benimsenen tüm BGYS proseslerine uygulanabilir. Şekil 27'de bir BGYS'nin bilgi güvenlik gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını (örneğin, yönetilen bilgi güvenliği) nasıl ürettiğini gösterir.

---

[119] TS ISO/IEC 27001, Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler (Ankara: TSE, Mart 2006), s.1.

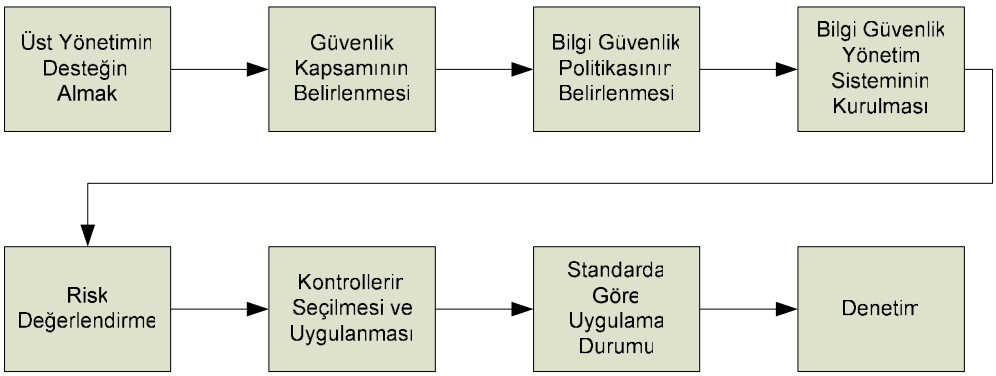


Şekil 27. BGYS Proseslerine Uygulanan PUKÖ Modeli

TS ISO/IEC 27001, 2006, s.2.

2.2. BGYS'nin Kurulması ve Yönetilmesi (Md.4.2.)

ISO 27001 standardına uygun olarak BGYS kurulması sürecinin aşamaları Şekil 28'de gösterilmektedir. BGYS'nin kurulumuna ilişkin bu adımların detayları söz konusu standarda göre 2.2.1. numaralı başlık altında sunulmuştur.



Şekil 28. ISO 27001 Sürecinin Aşamaları

Carlson, 2001, s.11.

2.2.1. BGYS'nin Kurulması (Md.4.2.1.)

İşletmeler, BGYS kurmak için temel olarak aşağıdaki faaliyetleri gerçekleştirmek durumundadırlar. Bunlar:

-İşin, kuruluşun, yerleşim yerinin, varlıklarının ve teknolojisinin özelliklerine göre BGYS kapsamı ve sınırlarının tanımlanması gerekmektedir.

-İşletme özelliklerine göre aşağıdaki özelliklere sahip bir BGYS politikası tanımlaması gereklidir. Bu politika oluşturulurken aşağıdaki hususlara dikkat edilmelidir. Dolayısı ile politikalar:

- Amaçlarını ortaya koymak için bir çerçeve içeren ve bilgi güvenliğine ilişkin bir eylem için kapsamlı bir yön kavramı ve prensipleri içermeli,
- İş ve yasal ya da düzenleyici gereksinimleri ve sözleşmeye ilişkin güvenlik yükümlülüklerini dikkate almalı,
- BGYS kurulumu ve sürdürülmesinin yer alacağı stratejik kurumsal ve risk yönetimi bağlamını düzenlemeli,
- Risk değerlendirme yapısının tanımlanacağı kriterleri kurmalı,
- Yönetim tarafından kabul edilmiş, olmalıdır.

-Risk değerlendirmesine ilişkin sistematik bir yaklaşım tanımlanmalıdır. İşletmeler, BGYS'ye ve tanımlanmış iş bilgisi güvenliğine, yasal ve düzenleyici gereksinimlere uygun bir risk değerlendirme yöntemini tanımlanmalıdır. Riskleri kabul edilebilir bir seviyeye indirmek için, BGYS politika ve amaçlarını ortaya koymalı ve kabul edilebilir riskler için seviye ve kriterler belirlenmelidir.

-Kuruluşlar tarafından riskler tanımlanmalıdır. Bunlar kısaca:

- BGYS kapsamındaki varlıkları ve bu varlıkların sorumluları tanımlanmalı,
- Bu varlıklar için var olan tehditleri tanımlanmalı,
- Tehditlerin fayda sağlayabileceği açıklıklar belirlenmeli,
- Gizlilik, bütünlük ve kullanılabilirlik kayıplarının varlıklar üzerinde olabilecek etkileri tanımlanmalıdır.

-Riskler çözümlenmeli ve derecelendirilmelidir. İkinci bölümde anlatılan risk değerlendirme yöntemleri göz önüne alınarak:

- Varlıkların gizliliğine, bütünlüğüne ya da kullanılabilirliğine ilişkin oluşan kayıpların olası sonuçlarını dikkate alarak, bir güvenlik başarısızlığından kaynaklanabilecek iş hasarlarını neler olabileceği belirlenmeli,

- Mevcut tehditler, açıklıklar ve bu varlıklarla ilişkili tesirler ışığında oluşan bu gibi güvenlik başarısızlıklarının gerçekçi olasılığını ve gerçekleştirilen mevcut kontroller değerlendirilmeli,
- Risk seviyelerinin tahmin edilmeli
- Riskin kabul edilebilir mi olduğunu yoksa risk değerlendirme maddesinde saptanan kriterler kullanılarak iyileştirme mi gerektirdiğine karar verilmesi gereklidir.

-Risk iyileştirmesi için seçenekler tanımlanmalı ve değerlendirilmelidir. Olası eylemler aşağıdakileri içermektedir:

- Uygun kontrollerin uygulanması,
- Kuruluşun politikasını ve risk kabul kriterlerini açıkça karşılaması şartıyla, bilerek ve nesnel olarak risklerin kabul edilmesi,
- Risklerden kaçınma,
- Bağlı iş risklerini diğer taraflara, örneğin, sigorta şirketlerine, tedarikçilere aktarmaktır.

-Risk iyileştirmesi için kontrol amaçları ve kontroller seçilmelidir. Uygun kontrol amaçları ve kontroller, risk değerlendirme ve risk iyileştirme proseslerinde tanımlanan gereksinimleri karşılamak için seçilmeli ve gerçekleştirilmelidir.

-Sunulan artık risklere ilişkin yönetim onayı alınmalıdır.

-BGYS'yi gerçekleştirmek ve işletmek için yönetim yetkilendirmesi alınmalıdır.

-Uygulanabilirlik Bildirgesi hazırlanmalıdır. Seçilen kontrol amaçları ve kontroller ve bunların seçilme nedenleri Uygulanabilirlik Bildirgesi dokümanında yer almalıdır. Aynı şekilde seçilmeyen kontrollere ilişkin seçilmeme nedenlerine de yer verilmelidir.

2.2.2. BGYS'nin Gerçekleştirilmesi ve İşletilmesi (Md.4.2.2.)

Kuruluşların, BGYS'yi gerçekleştirebilmek ve işletebilmek için gerekli faaliyetleri şu şekilde sıralanabilir:

-Bilgi güvenlik risklerini yönetmek için uygun yönetim eylem, sorumluluklar ve öncelikleri tanımlayan bir risk iyileştirme planı hazırlamalı,

-Finansman değerlendirmesi, roller ve sorumlulukların tahsisini içeren, tanımlanan kontrol amaçlarına ulaşmak için risk iyileştirme planı uygulanmalı,

-Kontrol amaçlarını karşılamak için seçilen kontroller uygulanmalı,

-Seçilen kontrollerin etkinliğinin nasıl ölçüleceği ve daha sonra bu ölçüm sonuçlarının nasıl kullanılacağı tanımlanmalı,

-Eğitim ve farkında olma programları gerçekleştirilmeli,

-BGYS'nin işleyişini yönetmeli,

-BGYS'nin kaynaklarını yönetmeli,

-Güvenlik olaylarını anında saptayabilme ve yanıt verebilme kabiliyetine sahip prosedür ve kontroller gerçekleştirilmelidir.

2.2.3. BGYS'nin İzlenmesi ve Gözden Geçirilmesi (Md.4.2.3.)

Kuruluşlar BGYS'ni izlenmesi ve gözden geçirilmesi için aşağıdakileri gerçekleştirmek durumundadır:

-İzleme prosedürlerini ve diğer kontrolleri aşağıda belirtilen amaçlara ulaşmak için yürütülmelidir. Bunlar:

- İşleme sonuçlarındaki hataları anında saptamak,
- Denenen ve başarılı olan güvenlik kırılmalarını ve ihlal olaylarını anında tanımlamak,
- Yönetimin, kişilere devredilen ya da bilgi teknolojisince gerçekleştirilen güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığını belirleyebilmesini sağlamak,
- Güvenlik olaylarını saptama ve belirteçler kullanarak güvenlik ihlal olaylarını engellemeye yardım etmek,
- Bir güvenlik kırılmasını çözmek için alınan önlemlerin etkili olup olmadığını karar vermektir.

-Güvenlik denetimlerinin, olaylarının, önerilerinin sonuçlarını ve tüm ilgili taraflardan geri bildirimleri dikkate alarak BGYS'nin (güvenlik politikaları ve amaçlarını karşılama, ve güvenlik kontrollerini gözden geçirme dahil) etkinliği düzenli olarak gözden geçirilmelidir.

-Güvenlik gereksinimlerinin karşılandığını doğrulamak için kontrollerin etkinliğini ölçülmelidir.

-Oluşacak değişiklikleri dikkate alarak, artık risklerin ve kabul edilebilir risklerin seviyesi gözden geçirilmelidir.

-Planlanan aralıklarda iç BGYS denetimleri gerçekleştirilmelidir.

-BGYS'nin yönetim tarafından düzenli olarak gözden geçirilmesi üstlenilmelidir.

-İzleme ve gözden geçirme faaliyetlerindeki bulgular dikkate alınarak güvenlik planları güncelleştirilmelidir.

-BGYS etkinliğinde ya da performansında bir etkisi olabilecek eylemleri ve olayları kaydedilmelidir.

2.2.4. BGYS'nin Sürekliliği ve İyileştirilmesi (Md.4.2.4.)

İşletmeler, süreklilik sağlama ve iyileştirme amacı ile belirli aralıklarla aşağıdaki faaliyetleri yapmak durumundadırlar:

-BGYS'deki tanımlanan gelişmeleri gerçekleştirmelidirler.

-Uygun düzeltici ve engelleyici önlemler alınmalıdır. Diğer kuruluşların ve kendisine ait güvenlik deneyimlerinden alınan dersler uygulanmalıdır.

-Sonuçları ve eylemleri bildirilmeli ve ilgili tüm taraflarla mutabık kalınmalıdır.

-İyileştirmelerin tasarlanan amaçlara ulaşması sağlanmalıdır.

2.3. Dokümantasyon Gereksinimleri (Md.4.3.)

Dokümantasyon yönetim kararlarının kayıtlarını içermeli, eylemlerin yönetim kararları ve politikalarına izlenebilir olmasını ve kaydedilen sonuçların yeniden üretilebilir olması sağlanmalıdır. Tüm dokümantasyon BGYS politikası gereğince kullanılabilir yapılmalıdır. BGYS dokümantasyonu aşağıdakileri kapsamalıdır:

-BGYS politikası ve kontrol amaçlarının dokümante edilmiş ifadeleri,

-BGYS kapsamını,

-BGYS'yi destekleyici prosedür ve kontrolleri,

-Risk değerlendirme metodolojisinin bir tanımı,

-Risk değerlendirme raporu,

-Risk iyileştirme planı,

-Kuruluş tarafından, bilgi güvenliği proseslerinin etkin planlanlanmasını, işlemesini ve kontrolünü sağlamak için gereksinim duyulan dokümante edilmiş prosedürleri,

-İhtiyaç duyulan kayıtları,

-Uygulanabilirlik Bildirgesi.

2.3.1. Dokümanların Kontrolü (Md.4.3.2.)

BGYS tarafından talep edilen dokümanlar korunur ve kontrol edilir. Dokümante edilmiş bir prosedür, aşağıdakilere ihtiyaç duyan yönetim eylemlerini belirlemek için kurulmalıdır:

-Yayınlanmadan önce dokümanları uygunluk açısından onaylama,

-Gerektiğinde dokümanları gözden geçirme, güncelleme ve tekrar onaylama,

-Doküman değişikliklerinin ve mevcut revizyon durumunun tanınmasını sağlama,

-İlgili dokümanların en son sürümlerinin kullanım noktalarında kullanılabilir olmasını sağlama,

-Dokümanların okunaklı ve hazır olarak tanınabilir olmasını sağlama,

-Dış kaynaklı dokümanların tanınmasını sağlama,

-Doküman dağıtımının kontrol edilmesini sağlama,

-Yürürlükte olmayan dokümanların istenmeden kullanımını engelleme,

-Eğer herhangi bir amaç için tutuluyorsa, bu dokümanlara uygun bir kimlik uygulanmasını kapsar.

2.3.2. Kayıtların Kontrolü (Md.4.3.3.)

Kayıtlar, gereksinimlere uygun olduğuna ve BGYS'nin etkin işlediğine dair kanıtlar sağlamak için kurulmalı ve sürdürülmelidir. Kayıtlar korunmalı ve kontrol edilmelidir. BGYS, ilgili her yasal gereksinimi dikkate alır. Kayıtlar, okunabilir, hazır olarak tanınabilir ve geri alınabilir halde tutulur. Kayıtların tanınması, saklanması, korunması, geri alınması, tutulma ve düzenleme zamanları için gereken kontroller yazılı hale getirilmelidir. Kayıtlar, proses performansına ve BGYS ile ilgili tüm güvenlik ihlal olaylarının oluşumlarına ilişkin tutulmalıdır. Kayıtlara ilişkin örnek olarak, ziyaretçi defterleri, denetim kayıtları ve erişim yetkilendirme formları verilebilir.[120]

---

[120] TS ISO/IEC 27001, Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler (Ankara: TSE, Mart 2006), s.2-10.

2.4. Yönetim Sorumluluğu (Md.5.)

Yönetim desteği bilgi güvenliği programının olmazsa olmaz unsurudur. Güvenlik mesajlarının etkili olabilmeleri için en yukarıdan desteklenmeleri gereklidir. Pek çok yönetici bu tür çalışmalar konusunda desteğini dile getirse de, desteğin gerçekleşmesi söylemek kadar kolay olmamaktadır. Bu durum yöneticilerin kendi iş ve sorumluluklarının bulunmasından kaynaklanmaktadır.[121]

BGYS kurulumunda yönetim sorumluluğu, yönetimin bağlılığı ve kaynak yönetim başlıkları altında açıklanmaya çalışılacaktır.

2.4.1. Yönetimin Bağlılığı (Md.5.1.)

Yönetim BGYS'nin kurulumuna, gerçekleştirilmesine, işletimine, izlenmesine, gözden geçirilmesine, sürdürülebilirliğine ve iyileştirilmesine olan bağlılığını aşağıdaki faaliyetleri gerçekleştirerek kanıtlamalıdır:

-Bir bilgi güvenlik politikası kurarak,

-Bilgi güvenlik amaçlarının ve planlarının kurulmasını sağlayarak,

-Bilgi güvenliği için rolleri ve sorumlulukları kurarak,

-Kuruluşa, bilgi güvenlik amaçlarını karşılamanın ve bilgi güvenlik politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi bildirerek,

-BGYS'yi geliştirmek, gerçekleştirmek, işletmek ve bakımını yapmak için yeterli kaynak sağlayarak,

-Kabul edilebilir risk seviyesini belirleyerek,

-İç BGYS denetimlerini sağlayarak,

-Yönetimin BGYS incelemelerini yürüterek.

2.4.2. Kaynak Yönetimi (Md.5.2.)

BGYS gerçekleştirmede yönetim sorumluluğu kapsamında yer alan kaynak yönetim kapsamını, kaynakların belirlenmesi, sağlanması ve uygun yeterlilikte personel için gereken faaliyetleri içermektedir. Bu faaliyetleri sırası ile inceleyecek olursak:

---

[121] Fatih Emiral, Bilgi Güvenliği Bilincinin Genele Yayılması, (02 Mayıs 2006), http://www.deloitte.com/dtt/article/0,1002,sid%253D8497%2526cid%253D53205,00.html

Kaynakların Sağlanması (Md.5.2.1.): Kuruluş, BGYS faaliyetlerinin planlandığı şekilde sürdürülmesine yönelik aşağıdaki faaliyetler için gereken kaynaklara karar vermeli ve bunları yürütmelidir.

-Bir BGYS kurmak, gerçekleştirmek, işletmek, sürdürmek ve iyileştirmek,

-Bilgi güvenlik prosedürlerinin iş gereksinimlerini desteklemesini sağlamak,

-Yasal ve düzenleyici gereksinimleri ve sözleşmeden doğan güvenlik yükümlülüklerini tanımlamak ve ifade etmek,

-Gerçekleştirilen tüm kontrollerin doğru uygulamalarıyla, uygun güvenliği sürdürmek,

-Gerektiğinde incelemeleri yürütmek ve bu gözden geçirme sonuçlarına uygun olarak hareket etmek,

-İhtiyaç olduğunda, BGYS etkinliğini geliştirmektir.

Eğitim, Farkında Olma ve Yeterlilik (Md.5.2.2.): İşletmeler, ilgili tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin ve BGYS amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olmasını sağlamalıdır. Bu amaçla kuruluşlar;

-BGYS'yi etkileyecek işleri gerçekleştiren personel için gerekli yeterlilikleri belirlemeli,

-Yeterli eğitimi sağlama ve, gerekirse, bu ihtiyaçları karşılamak üzere yeterli personel istihdam etmeli,

-Alınan önlemlerin etkinliğini değerlendirmeli,

-Eğitime, öğretime, becerilere, deneyime ve niteliklere ilişkin kayıtları tutmalıdır.

2.5. BGYS İç Denetimleri (Md.6)

Kuruluş, BGYS kontrol amaçlarının, kontrollerinin ve prosedürlerinin standardın gereklerine, tanımlanan bilgi güvenliği gereksinmelerine uyup uymadığını belirlemek için, planlanan aralıklarla iç denetimler yürütmelidir.

Bir denetleme programı, bir önceki denetim sonuçlarının yanı sıra denetlenecek proseslerin ve alanların durumu ve önemi dikkate alınarak planlanmalıdır. Denetim kriterleri, kapsamı, sıklık ve yöntemler tanımlanmalıdır. Denetmenlerin seçiminde ve denetimlerin gerçekleştirilmesinde, denetim prosesinin nesnel ve tarafsız olarak işlemesi sağlanmalıdır. Denetmenler kendi çalışmalarını denetlememelidirler.

Denetimlerin planlanması ve yürütülmesinde ki ve sonuçların raporlanması ve kayıtların tutulmasında ki sorumluluklar ve gereksinimler, yazılı hale getirilmiş bir prosedür içinde tanımlanır.

Denetlenen alandan sorumlu olan yönetim, saptanan uygunsuzlukların ve bunların nedenlerinin giderilmesi için, gereksiz gecikmeler olmaksızın önlemlerin alınmasını sağlamalıdır. İzleme faaliyetleri, alınan önlemlerin doğrulanmasını ve doğrulama sonuçlarının raporlanmasını içermelidir.

2.6. BGYS'yi Yönetimin Gözden Geçirmesi (Md.7.)

Yönetim, kuruluşun BGYS'sini planlanan aralıklarla, sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirmelidir. Bu gözden geçirme, güvenlik politikası ve güvenlik amaçları dahil BGYS'nin iyileştirilmesi ve gereken değişikliklerin yapılması için fırsatların değerlendirilmesini de içermelidir. Gözden geçirme sonuçları açıkça yazılı hale getirilmeli ve kayıtlar tutulup saklanmalıdır. Bu nedenden dolayı, gözden geçirme faaliyetlerinin kapsamı gözden geçirme girdisi ve gözden geçirme çıktısı başlıkları altında incelenecektir.

2.6.1. Gözden Geçirme Girdisi (Md.7.2.)

BGYS kapsamında gerçekleştirilecek yönetimin gözden geçirme faaliyetleri için gerekli girdiler, aşağıdakileri içermelidir. Bunlar:

- BGYS denetimleri ve gözden geçirmelerinin sonuçları,

-İlgili taraflardan edinilen geri bildirimler,

-Kuruluşta BGYS'nin performansını ve etkinliği artırmak için kullanılabilecek teknikler, ürünler ya da prosedürler,

-Önleyici ve düzeltici faaliyetlerin durumu,

-Etkinlik ölçümlerinin sonuçları,

-Önceki risk değerlendirilmesinde uygun olarak ifade edilmeyen açıklıklar ya da tehditler,

-Önceki yönetim gözden geçirmelerinden izleme eylemleri,

-BGYS'yi etkileyebilecek herhangi bir değişiklik,

-İyileştirme için önerilerden, oluşmaktadır.

2.6.2. Gözden Geçirme Çıktısı (Md.7.3.)

Bir BGYS yönetim gözden geçirme çıktıları, aşağıdakilerle ilgili her kararı ve eylemi içermelidir.

-BGYS etkinliğini iyileştirmek,

-Risk değerlendirme ve risk işleme planını güncelleştirmek,

-Gerektiğinde, BGYS üzerinde etkisi olabilecek iç ya da dış olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri,

-Kaynak ihtiyaçları,

-Kontrollerin etkinliğinin ölçümünde iyileşme faaliyetleridir.

2.6.3. BGYS İyileştirme (Md.8.)

BGYS proseslerine uygulanan PUKÖ modelinin "Önlem Al" kapsamında, BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici eylemlerin gerçekleştirilmesi gerekmektedir.

2.6.4. Sürekli İyileştirme (Md.8.1.)

Kuruluş, bilgi güvenlik politikasını, güvenlik amaçların, denetim sonuçlarını, izlenen olayların analizini, düzeltici ve önleyici faaliyetleri ve yönetim gözden geçirmelerini kullanarak BGYS etkinliğini sürekli iyileştirmelidir.

2.6.5. Düzeltici Faaliyetler (Md.8.2.)

Kuruluş tekrarları engellemek için, BGYS gereksinimleriyle uygunsuzlukların nedenlerini gidermek üzere önlemler almalıdır. Düzeltici faaliyetler için yazılı hale getirilmiş prosedür aşağıdaki gereksinimleri tanımlamalıdır:

-Uygunsuzlukları tanımlamak,

-Uygunsuzlukların nedenlerini belirlemek,

-Uygunsuzlukların tekrarlanmamasını sağlamak için ihtiyaç duyulan faaliyetleri değerlendirmek,

-Gereken düzeltici faaliyetleri belirlemek ve gerçekleştirmek,

-Gerçekleştirilen faaliyetlerin sonuçlarını kaydetmek,

-Gerçekleştirilen düzeltici faaliyetleri gözden geçirmek, olarak sıralanabilir.

2.6.6. Önleyici Faaliyetler (Md.8.3.)

Kuruluş tekrar ortaya çıkmalarını önlemek için, BGYS gereksinimleriyle olası uygunsuzlukların nedenlerini gidermek üzere alınacak önlemleri belirlemelidir. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. Önleyici faaliyetlerin önceliği, risk değerlendirme sonuçlarına bağlı olarak belirlenir. Önleyici faaliyetler için yazılı hale getirilmiş prosedür aşağıdaki gereksinimleri tanımlamaktadır:

-Olası uyumsuzlukları ve bunların nedenlerini belirlemek,

-İhtiyaç duyulan önleyici faaliyetleri belirlemek ve gerçekleştirmek,

-Gerçekleştirilen faaliyetlerin sonuçlarını kaydetmek,

-Gerçekleştirilen önleyici faaliyetleri gözden geçirmek,

-Değişen riskleri tanımlamak ve dikkatin önemli derecede değişen riskler üzerinde yoğunlaştıracak önleyici faaliyet gereksinimlerini, kapsamalıdır.[122]

[122] TS ISO/IEC 27001, Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler (Ankara: TSE, Mart 2006), s.2-13.

DÖRDÜNCÜ BÖLÜM
ISO 27001 STANDARDINA GÖRE BİLGİ GÜVENLİK YÖNETİM SİSTEMİNİN ASELSAN'DA UYGULAMASI

1. UYGULAMA ÇALIŞMASININ AMACI VE GENEL AÇIKLAMALAR

Daha öncede kısaca değindiğimiz gibi bilgi güvenliği diskte, iletişim ağında, yedekleme ünitelerinde ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasıdır. Bu amaçla geliştirilen bir güvenlik sistemi bilişim teknolojilerinde aşağıdaki hedefler doğrultusunda tasarlanmalıdır:

-Her türlü bilgi, belge ve iletişimin yetkisiz kişilerin ve üçüncü şahısların ellerine geçmesini engellemek amacıyla gizliliklerinin sağlanması,

-Kurumsal dokümanların ve bilgilerin personel hatalarından, virüsler, Truva atları ve üçüncü şahıslar tarafından değiştirilerek bütünlüklerinin bozulmasının engellenmesi,

-Kurumsal doküman ve bilgilere sorunsuz ve zamanında erişilebilmesi ve doğal felaketler sırasında bile bilgiye sorunsuz ulaşabilmesi,

-Şirket kaynaklarının israfının önlenerek çalışanların verimliliğinin arttırılmasıdır.

Bu bölümde, belirlenen bu hedeflere ulaşılabilmesi için ASELSAN organizasyon yapısında yer alan, Mikroelektronik Güdüm ve Elektro Optik Grubu (MGEO) içinde Bilgi Güvenlik Yönetim Sistemi kurulumuna yönelik gerekli prosedürlerin oluşturulması, organizasyonun kurulması, personelin bilinçlendirilmesi sağlanarak, üretilecek bilgi, yazılım kodları ve dokümanların güvenliği sağlanabilecektir. Bu sistemin kurulmasında, Hava Kuvvetlerinin envanterinde bulunan RF-4E uçaklarının modernizasyonu kapsamında, 1 nci Hava İkmal Bakım Merkezi Komutanlığı ile birlikte belirlenen iş paylaşımına göre ASELSAN tarafından yerine getirilecek görevler örnek proje olarak belirlenmiştir. ASELSAN bu proje kapsamda, kullanıcı istekleri doğrultusunda tanımlanan sistemin, tasarlanarak gerekli yazılım, donanım ve doküman üretimini hedeflemektedir.

Bu uygulamadan beklenen amaç, BGYS uygulama nedeni, risk yönetiminin şirketlere nasıl uygulanabileceği, BGYS'nin nelerden oluştuğu ve ISO 27001 standardının BGYS olarak seçilme nedenine yönelik dört temel araştırma sorularına cevap bulmak şeklinde özetlenebilir. Böylece ASELSAN'ın iş yaptığı müşterilere ait her türlü bilginin gizliliğini, bütünlüğünü ve elverişliliğini sağlamak ve gelecekte ASELSAN genelinde ISO 27001 gereklerine uygun bir BGYS kurulumuna esas teşkil

edecek olan altyapının kurulmasına yönelik hazırlıkların yapılması şeklinde özetleyebiliriz. Böylece, uluslararası ihalelere katılım şartı olan ISO 27001 gerekleri sağlanmış olacaktır. İlave olarak ASELSAN müşterileri, kendilerine ait bilgilerin güvende tutulacağı konusundaki taahhütten dolayı kendilerini güvende hissedeceklerdir. Böylece ASELSAN kurumsal değerlerini, yatırımlarını ve hedeflerini sürdürüp, korunabilmesi için ortaya konması gereken kontrollerin firma içinde yerleştirilmesi ve uygulanması sağlanacaktır.

2. ASELSAN'NIN TANITIMI

ASELSAN elektronik ürünler ve sistemler tasarlayan, geliştiren, üreten ve ürünlerinin satış sonrası servis hizmetlerini karşılayan; yüksek teknolojili ve çeşitli ürün yelpazesine sahip bir elektronik sanayi kuruluşudur. ASELSAN'da ürün geliştirme faaliyetlerinde en son elektronik, elektro optik ve mekanik teknolojiler bilgisayar destekli geliştirme ve üretim altyapısı ile birlikte uygulanmaktadır.

ASELSAN çalışmalarını üç başlık altında Haberleşme Cihazları, Mikrodalga Sistemler ve Sistem Teknolojileri ve Mikro elektronik Güdüm ve Elektro-Optik ana faaliyet alanlarında sürdürmektedir. Ana faaliyetlerin kapsamlarına bakacak olursak;

-**Haberleşme Cihazları:** Askeri haberleşme, sivil haberleşme ve sivil elektronik sistemleri içerdiği,

-**Mikrodalga Sistemler ve Sistem Teknolojileri:** Savunma ve silah sistemleri, Elektronik Harp ve İstihbarat, Komuta Kontrol Sistemleri, Radar Sistemleri, Sivil Kontrol ve Otomasyon alt başlıklar kapsadığı,

-**Mikroelektronik Güdüm ve Elektro-Optik:** Elektro-Optik Güdüm ve Seyrüsefer, Aviyonik (elektronik sistemler) ve Mikroelektronik alt konuları içerdiği görülmektedir.

Macunköy tesislerinde faaliyetlerini sürdüren, Haberleşme Cihazları Grubunun ana faaliyet alanı askeri ve profesyonel haberleşme sistemleri, Mikrodalga ve Sistem Teknolojileri Grubunun ana faaliyet alanı ise radar, elektronik harp ve komuta kontrol sistemleridir. Geniş makina-teçhizat parkı ve üstün teknolojik yapıya sahip Macunköy tesislerinde:

-AR-GE,

-Elektronik Üretim,

-Baskı Devre Üretim,

-Mekanik /Kalıp Üretimi bölümleri,

bulunmaktadır.Elektronik üretim ünitelerinde askeri standartta ve ağır çevre koşullarını içeren üretim yöntemleri kullanılmakta ve çağdaş teknolojik gelişmeler yakından izlenmektedir. Üretim hatlarında; çok katlı ve esnek baskı devreler yüzey monte teknolojisi, bilgisayar destekli tasarım-üretim teknolojileri başarıyla kullanılmaktadır.

Akyurt tesislerimizde faaliyetlerini sürdüren Mikroelektronik, Güdüm ve Elektro-Optik Grubu ise hibrid mikroelektronik devreler, gece görüş cihazları, laser işaretleyici ve ataletsel seyrüsefer cihazları ana başlıkları altında, otomasyona dayalı en modern üretim araçlarıyla donatılmış olarak, 2000'li yılların en kritik teknolojileri arasında yer alan mikroelektronik teknolojili üretim ile elektro-optik alanında üretim gerçekleştirilmektedir. Bütün gruplarda bilgisayar destekli tasarım (CAD), mühendislik (CAE) ve üretim (CAM) teknolojileri askeri standartlar ve ISO-9000'e uygun olarak başarıyla uygulanmaktadır.[123]

2.1. Tarihçe

1975 yılı sonunda Kara Kuvvetlerini Güçlendirme Vakfı öncülüğünde Vakıf Kuruluşu bir Anonim Şirket olarak kurulmuştur. Yatırım çalışmalarını kısa sürede tamamlamış ve 1979 yılı başlarında Ankara Macunköy tesislerinde üretim faaliyetine geçmiştir.

Kuruluş yıllarından bu yana ileri teknolojiye dayalı olarak, programlı bir şekilde müşteri ve ürün yelpazesini genişletmiş olup, bugün modern elektronik cihaz ve sistemler geliştiren, üreten, tesis eden, pazarlayan ve satış sonrası hizmetlerini yürüten entegre bir elektronik sanayii kuruluşu haline gelmiştir. Halen 29.4 Milyon YTL sermayeli şirketin ortaklık yapısını, %85'ini Türk Silahlı Kuvvetleri Güçlendirme Vakfı, %15'lik kısmını da Axa OYAK Sigorta ile diğer ortaklar oluşturmaktadır.

2.2. Şirketin Misyonu ve Vizyonu

ASELSAN'ın misyonu, ileri teknolojiyi yakından izleyerek Türk Silahlı Kuvvetleri'nin elektronik cihaz ve sistem gereksinimlerini fiyat-zaman-kalite yönünden en uygun koşullarda ve dışa bağımlılığı en aza indirecek şekilde karşılamak, milli

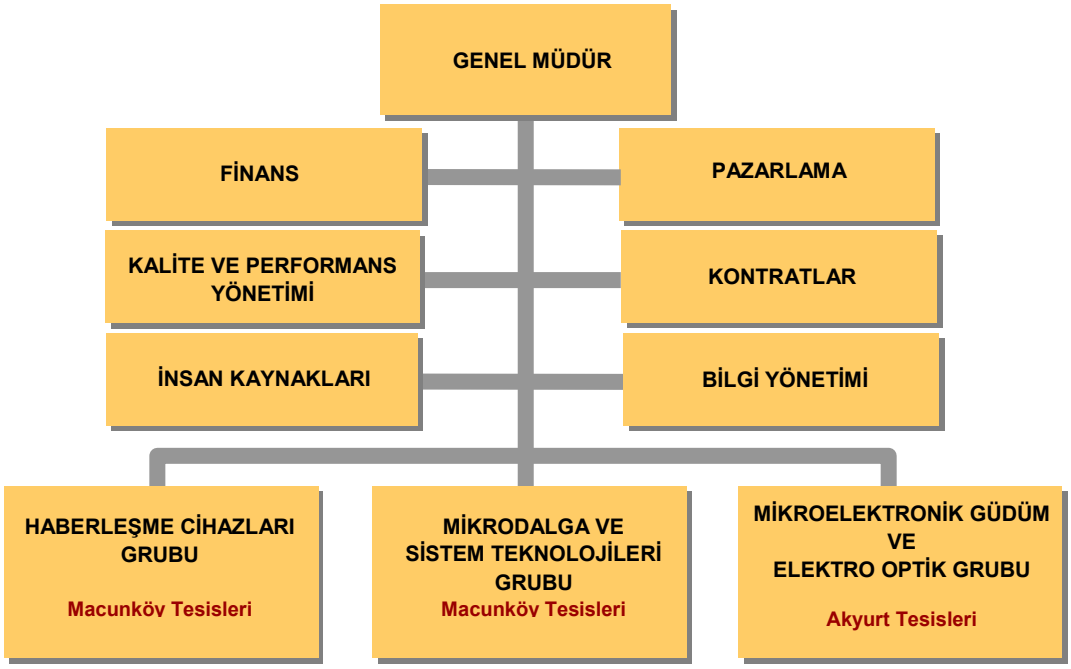
[123] ASELSAN A.Ş.' nin Tanıtımı, (01 Mayıs 2006), http://www.aselsan.com.tr

savunma sanayisinin gelişmesinde önder olmak, sahip olunan bilgi birikimini ülkemizin diğer elektronik sistem ihtiyaçlarının karşılanmasında ve ihracat olanaklarında kullanmak, bu şekilde her türlü şartlar altında devamlılığı ve gelişimi sağlamaktır.

ASELSAN'ın vizyonu, yurt içi ve dışında ulaşılan başarılı konumu sürekli geliştirerek faaliyet alanlarında Türkiye'de en iyi olmak, dürüst ve güvenilir bir firma olarak müşteri memnuniyetini ve ülkemizin beyin gücünün verimli kullanımını sağlamaktır.

2.3. Şirketin Organizasyon Yapısı

Şekil 29'dan görüleceği gibi, ASELSAN farklı yatırım ve üretim yapısı gerektiren proje konularına bağlı olarak Haberleşme Cihazları Grup Başkanlığı (HC), Mikrodalga ve Sistem Teknolojileri Grup Başkanlığı (MST), Mikroelektronik, Güdüm ve Elektro-Optik Grup Başkanlığı (MGEO) olmak üzere üç ayrı Grup Başkanlığı bünyesinde örgütlenmiştir. Ankara'da MACUNKÖY ve AKYURT'ta yerleşik iki ayrı tesiste üretim ve mühendislik faaliyetlerini sürdürmekte olan ASELSAN'ın Genel Müdürlük teşkilatı Ankara Macunköy'de bulunmaktadır. Şekil 30'da Bilgi Güvenlik Yönetim Sistemi kurulmak istenen kısmına ait organizasyon şeması görülmektedir.



Şekil 29. ASELSAN A.Ş. Organizasyon Yapısı

PGD-T007, Haziran 2005

2.4. Uluslararası Faaliyetler

ASELSAN, İstanbul, İzmir Bölge Müdürlükleri ve yurt çapına yayılmış olan satış bayilikleri ile satış sonrası hizmetlerini de başarıyla yürütmektedir. Çeşitli ülkelerde temsilcilikleri bulunan ASELSAN, ilk yurtdışı şirketi olan ASELSAN-BAKÜ şirketini, 1998 yılında Azerbaycan'da kurarak faaliyete geçirmiştir.

2.5. Kullanılan Standartlar

Şirkette teknolojik altyapı, aşağıda sıralanan prosedür ve standartlara göre tasarım ve üretim faaliyetleri gerçekleştirilerek sağlanmaktadır.

-MIL-STD-883 ; Mikroelektronik İçin Test Metotları ve Prosedürleri

-MIL-M-38510 ; Mikroelektronik Genel Özellikleri

-MIL-STD-750; Yarıiletken Cihazlar İçin Test Metotları,

-MIL-S-19500; Yarıiletken Cihazlar Genel Özellikleri

-MIL-STD-45743; Lehimleme, El Tipi Yüksek Güvenirlilikle Elektronik

-MIL-STD-454; Elektronik Cihazlar İçin Genel Standart Gereklilikleri

-MIL-0-13830; Atış Kontrol Aletleri İçin Optik Parçalar; Üretim, Montaj ve Denetim Yönetimi İçin Genel Özellikleri

-MIS-23666; Hibrit Üretim Özellikleri

-MIS-23667; Yarıiletken ve Mikroelektronik Entegreler İçin Kritik Parça Fonksiyon Özellikleri

-SQAP-13047079 ; Ek Kalite Güvenlik Şartları, Görsel Kabul Standartları, Hibrit Mikroelektronik Montajı

-STANAG 4107; Ortak Hükümet Kalite Güvenliği Kabulü ve Birleşik Kalite Güvenliği Yayınlarının Kullanımı

-MIL-STD 1520; Uygun Olmayan Malzeme İçin Düzeltme ve İade Sistemi

-MIL-STD-480; Konfigürasyon Kontrolü, Mühendislik Değişiklik, Sapma ve Feragati

-MIL-STD-1535; Donatıcı Kalite Güvenlik Program Gereklilikleri

-TS-EN ISO 9001:1994 Tasarım / Geliştirme, Üretim, Tesis ve Hizmette Kalite Güvencesi Modeli Kalite Sistem Standardı

-AQAP-110 Tasarım, Geliştirme ve Üretim İçin NATO Kalite Güvence Gerekleri Standardı

-ISO 10012 Ölçme Cihazları için Kalite Güvence Gerekleri Standardı

-IPC-2221, IPC-2222 Baskı Devre Kartı Tasarım Standardları

-IPC-6012, IPC-6013, MIL-P-55110 Baskı Devre Kartı Performans Standardları

-IPC-A-600 Baskı Devre Kartı Kabul Edilebilirlik Gerekleri Standardı

-J-STD-001 Lehimlenmiş Elektrik ve Elektronik Takımlar için Gerekler Standardı

-IPC-A-610 Elektronik Takımların Kabul Edilebilirlik Gerekleri Standardı

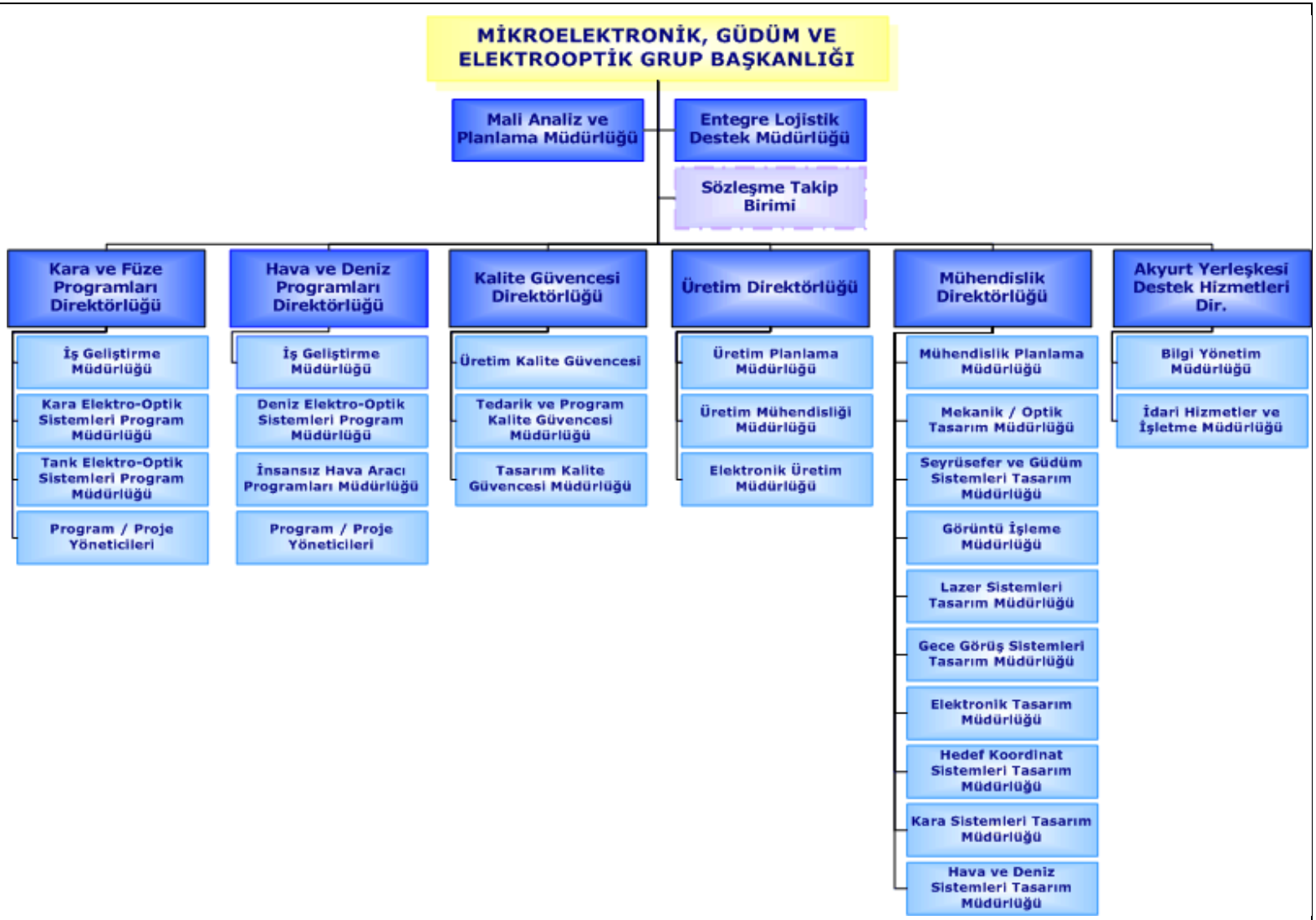
-IPC-7711 Elektronik Takımların Yeniden İşleme Standardı

-IPC-7721 Elektronik Takımların Onarımı Standardı

-MIL-STD-461D, MIL-STD-462D, Elektromanyetik Etkileşim Standardı

-MIL-STD-810 Çevre Koşulları Test Yöntemleri Standardı

-ETS 300 019 Haberleşme Cihazları için Çevre Koşulları Testleri Standardı



Şekil 30. MGEO Organizasyon Yapısı

3. ASELSAN'DA BİLGİ GÜVENLİK YÖNETİM SİSTEMİ KURULUMU

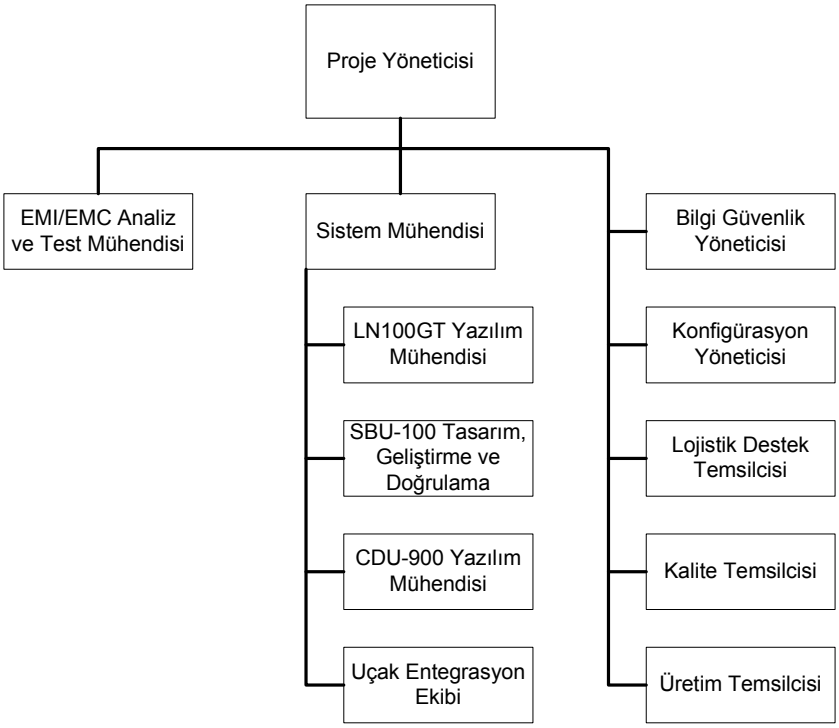
BGYS kurma çalışmaları, 2005-2008 yılları arasında ASELSAN ile 1 nci HİBM.K.lığı arasında yürütülecek proje kapsamında geliştirilmesi, uygulamaya başlanılması ve sonuçlarına bağlı olarak tüm organizasyon düzeyine yayılarak diğer projelerde de kullanılabilmesi hedefi doğrultusunda sürdürülmektedir. Proje kapsamında kullanılacak, işlenecek ve ürün haline dönüştürülecek bilgi kaynaklarının, uluslararası kabul görmüş standart seviyelerde bilgi güvenlik yönetim sistemi altyapısının kurulması temel hedefler arasında yer almaktadır. Bu kapsamda BGYS kurulumuna yönelik gerçekleştirilecek faaliyetleri yönetsel ve teknik faaliyetler başlıkları altında detayları sunulmuştur.

3.1. Yönetsel Faaliyetler

Proje kapsamında işlenecek olan varlıkların mevcut tehditlere karşı güvenliğini sağlamak, yaşanacak güvenlik ile ilgili olan olaylar nedeniyle oluşacak maddi ve manevi kayıpları en aza indirmek, yapılan yatırımların geri dönüşünü en üst seviyeye çıkarmak, temel güvenlik gereksinimleri olan Gizlilik, Bütünlük, Elverişlilik gereksinimlerinin proje kapsamında karşılanmasını garanti etmek ve mevcut tehditlerden kaynaklanan risklerin kabul edilebilir seviyede tutulmasını sağlamak amacıyla Bilgi Güvenlik Yönetim Sistemi kurulumuna yönelik Bölüm 3'te vurgulanan gereksinimleri karşılayacak aşağıda sıralanan yönetsel önlemler alınmıştır.

3.1.1. Bilgi Güvenlik Yönetim Sistemi Organizasyonu

ASELSAN MGEO bünyesinde Hava ve Deniz Sistemler Müdürlüğüne bağlı olarak çalışan proje yöneticisi tarafından yürütülen programa ilişkin yönetim organizasyonu Şekil 31'de sunulmuştur. Bilgi Güvenlik Yöneticisi bu proje kapsamında oluşturulan bilgi varlıklarının ISO 27001 standardına uygun süreç yönetimini sağlamak üzere görevlendirilmiştir.



Şekil 31. ASELSAN RF-4E Proje Yönetim Organizasyon Yapısı

3.1.2. Bilgi Güvenlik Politikası

Bilgi Güvenliği Politikası'nın geliştirilmesi sırasında projenin gereksinimleri ön planda tutularak TS ISO/IEC 17799 standardından yararlanılmıştır. Politika, "Nasıl" sorusuna cevap vermekten çok "Ne" sorusuna cevap vermek üzere yazılmıştır. Bu politikanın sahibi Bilgi Güvenliği Onay Kurulu'dur. Bu kurulun temel görevi politikayı onaylamaktır. Bu kurul, Bilgi Güvenliği Politikası'nın proje kapsamında benimsenmesine ön ayak olur. Kurul, kendisine sunulan raporları değerlendirerek politikada değişiklik yapabilir. Bu kurul şu üyelerden oluşmaktadır:

-MGEO Başkanı

-Proje Yöneticisi

-Bilgi Güvenlik Yöneticisi

Bilgi güvenlik politikası bilgi güvenlik yöneticisinin sorumluluğunda proje yönetim grubu ile yapılan grup çalışmaları sonucunda aşağıdaki şekilde olmasına Bilgi Güvenliği Onay Kurulu tarafından karar verilmiştir. Buna göre;

Bilgisayar sistemlerindeki ve ağlarındaki güvenliğin sağlanması oldukça zor ve meydan okuyan bir problemdir. Yazılım ve donanımın gelişimi ve bilgi teknolojilerine olan sosyal bağımlılığın artması, tüm organizasyonlarda sürekli önlemlerin alınmasını gerekli kılmaktadır.

ASELSAN yeni ürünler üreterek ve bilgi güvenliği hizmetleri vererek müşterilerini rahat ve güven içinde hissetmelerini sağlar. Hizmet kalitesinin arttırıldığı şu noktalarla karakterize edilebilir: çalışanlar, güvenilir alt yükleniciler ve örnek projelerdir.

ASELSAN en önemli değer çalışanlarındır. Onlar başarıya odaklanmıştırlar ve bu nedenle hem profesyonel hem de sosyal yetenekleri vurgulayan süreçler önemli bir rol oynayacaktır. ASELSAN yönetimi çalışanlarına iyi bir atmosfer oluşturarak ve örnek olarak bilgi güveliği konusundaki birikimlerini arttırmaya çalıştırmalıdır.

Tüm projede kaliteyi arttırmak için ASELSAN sadece profesyonelce çalışan alt yükleniciler ile çalışır. Tüm alt yükleniciler ASELSAN'ın güvenlik isteklerine uymak zorundadır. ASELSAN da müşterilerini memnun etmek için elinden geleni yapmalıdır.

Son ama en önemli nokta ise bilgi ve ağ güvenliği alanında iyi örnekler getirerek yeteneğini ispat etmelidir. ASELSAN bilginin ve güvenlik değerlerinin iyi örnek teşkil edeceğine emindir. Her müşteri önce bilgi güvenliği sistemi konusunda güvenilir olduğunu fark edebilmelidir.

Her aksiyon süresince çalışanlar ASELSAN müşterilerini ve onlara proje boyunca yüksek kalite sağlamaya zorunludur. İş süreçlerindeki bilgi güvenliği müşterilerin güvenli ve profesyonelce korunduklarını hissetmelerine izin vermelidir. Herhangi bir yanlış anlaşılmaya izin vermemek için ilave dokümanlar oluşturulmalıdır. Bilgi yönetme politikası, risk analiz verilerine dayanarak, iç ve dış kullanıcı için stratejik bilgileri koruma yolları tanımlayacaktır. Şifre politikası şifre yaratmanın, saklamanın ve değiştirmenin doğru yollarını tanımlayacaktır. Her çalışan gizlilik sözleşmesini imzalamalıdır ve bilgi güvenliği iş sorumluluklarının içine eklenmelidir. Bilgi Güvenliğinin elemanları tüm iş prosedürlerinin içine eklenmeli ve uymayanlar cezalandırılmalıdır.

Bu politikanın kapsamındaki her kişi gözledikleri ihlalleri sorumlu güvenlik temsilcisine rapor etmek zorundadır.

Bilgi varlıklarının kullanılamaması ASELSAN için o varlığın hasar görmesi kadar önemli bir problemdir. Bilgi varlıklarının kullanılamaz olduğu zamanlarda iş süreçlerini devam ettirebilmek için bir iş sürekliliği ve felaket planlaması hazırlanacaktır. Yazılı hale getirilen ve yılda bir kez test ve tatbikatları gerçekleştirilecek bu planla, kaynak sahipleri tarafından kritik olarak değerlendirilmiş tüm bilgi varlıkları kapsanacaktır.

Sistemi düzgün bir biçimde kurup çalışır halde tutması için bir kişi atanmalı ve tüm sonuçlardan sorumlu olmalıdır. Bu kişinin teknik ve organizasyonel bir bakış açısın sahip olması ve iletişim becerilerinin yüksek olması gerekmektedir. Amacımız sistemi gereksiz atışmalardan kurtarmak ama her çalışanın da bu kişinin önerilerini dikkate almasını sağlamaktır.

3.1.3. Bilgi Varlıkları ve Sorumluluklar

Bilgi güvenlik yöneticisi, proje yöneticisi ve üyeleri ile birlikte sistem için kritik varlıkların listesini hazırlamıştır. Tablo 7.'de sunulan liste ilk bakışta tam gibi görülmeyebilir fakat gerçekte bilgi güvenliği açısından gerekli tüm stratejik varlıkları listelemektedir. Monitör ve klavye gibi elemanlar bilgisayar sisteminin parçasıysalar bile sistemin bütününde değerleri küçüktür. Listelenmiş tüm varlıklar sistem içinde anahtar rol oynar. Sunucu yazılımı veya ağ kartları ile ilgili problemler çok daha önemlidir ve kırık bir klavye veya bozuk bir fareden daha fazla soruna neden olurlar.

Tüm sistemin güvenilirliği için hiçbir gerçek değeri olamayan çok fazla varlık, çok fazla zayıflık, çok fazla tehdit, sistemin güvenliği için gereken işi üç katına çıkarabilir. Bu da sistemi yönetilemez hale getirir ve sonuçta sistemin güvenliği azalır. Varlık listesinin doğruluğu proje yöneticisi ve üyelerinden, kontrolü ise güvenlik temsilcisinden sorumlu tutulacaktır.

Tablo 7. Varlık Listesi

S/N	Varlık Kategori/Varlıklar	Sorumlu	Yeri	Güvenlik Sınıflandırması
	Bilgi Varlıkları			
1	Kullanıcı Veri Tabanı			
2	Yazılım Lisansları			

3	Bilgisayar Sistem Dokümantasyonu			
4	Sistem Dokümantasyonu			
	Yazılım Varlıkları			
5	IBM AIX v. 4.3			
6	Apache Daemon 1.3.20			
7	Domain Name Server 8.2.2			
8	FTP Daemon			
9	SendMail Daemon 8.11.0			
10	Telnet INETD			
11	Chargen INETD			
12	Echo INETD			
13	Finger INETD			
14	Windows NT 4.0			
15	Service Pack 6a			
16	Exchange Server 5.5			
17	Microsoft Domain Name Server			
18	Telnet Server			
19	LAN Manager			
	Fiziksel Varlıklar			
20	AIX Server			
21	Hard Drive			
22	Ağ Kartı			
23	Disket Sürücü			
24	CD-Rom Sürücü			
25	NT Server			
26	Sabit Disk			
27	Streamer			
28	Switch			
29	Router Cisco 2600			
30	Ağ Kabloları			
31	Yazılım Yükleme Diskleri			
32	Yedekleme Diskleri			
	Servisler			
33	Elektrik			
34	Su			
35	Havalandırma			

3.1.4. Bilgi Güvenlik Yönetim Sistemi Prosedürleri

Prosedürler daha çok "Nasıl" sorusunu cevaplamak üzere geliştirilmiştir. Analoji yapmak gerekirse, Bilgi Güvenliği Politikası Anayasa'ya, prosedürleri de yasalara benzetilebilir.

Bilgi Güvenlik Yönetim Sisteminin kurulması kapsamında MGEO bünyesinde yer alan proje organizasyonunda güvenlik süreçlerinin yönetimine yönelik oluşturulan prosedürler Tablo 8.'de sunulmuştur.

Tablo 8. Oluşturulan Prosedürler

Prosedür Adı
Bilgi Güvenlik Prosedürü
Varlık Sınıflandırması
Çalışan Personel Prosedürü
Personel Adaylarının Değerlendirilmesi
Gizlilik anlaşması
Personel dosyası oluşturulması
Ulaşım Bilgileri Oluşturulması
Kullanıcı Bilgilerinin Oluşturulması
Personelin Eğitimi
Acil Cevaplama Talimatı
Güvenlik Tehditlerinin Ele Alınma Prosedürü
Bilgisayar Sistemlerinin Sürdürülebilirliği
Risk Yönetim Prosedürü
Kontrol Prosedürü

3.1.4.1. Bilgi Güvenliği Politika Prosedürü

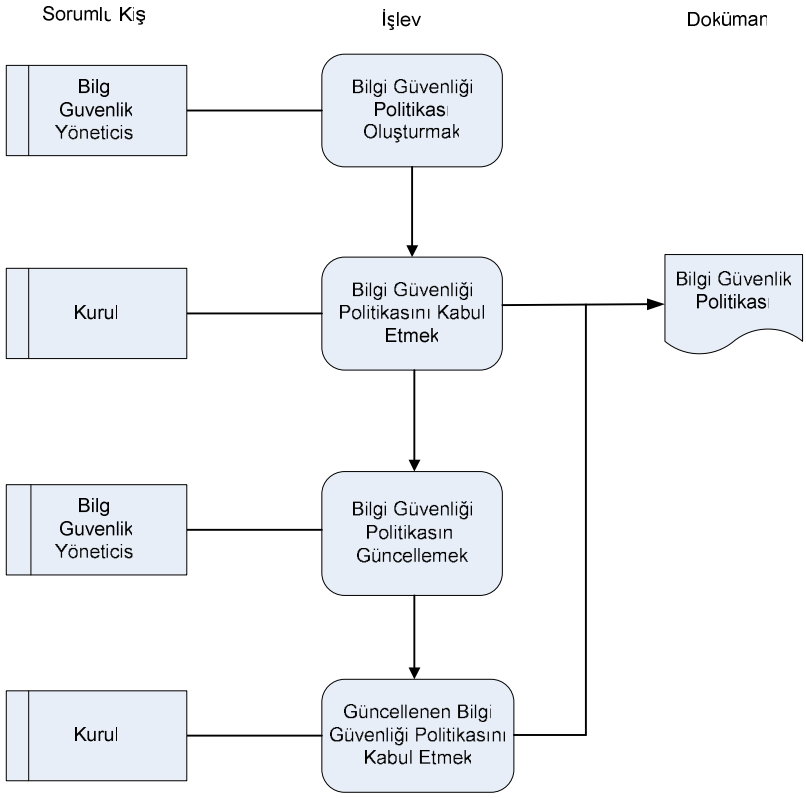
Bu prosedürün ana amacı ASELSAN'ın Bilgi Güvenliği Politikası ile uyumlu çalışmasını sağlamak ve bu politikanın ASELSAN çalışanları tarafından öğrenilmesi, anlaşılması ve kabul edilmesini sağlamaktır. Bu prosedürün ana elemanları:

-Bilgi güvenliği politikası oluşturmak

-Bilgi güvenliği politikasını kabul etmek

-Bilgi güvenliği politikasını güncellemektir.

Güvenlik politikasının oluşturulmasındaki sorumluluklara, görevlere ve çıkan ürünlere ilişkin grafiksel gösterim Şekil 32'de sunulmuştur.



Şekil 32. Bilgi Güvenlik Politika Prosedürü

3.1.4.1.1. Bilgi Güvenlik Politikası Oluşturmak

Bilgi Güvenliği Politikası, ASELSAN'a, müşteri ve ortaklarına ait tüm bilgileri korumak için gerekli aktiviteleri açıklamalıdır. Politika bütün bu aktiviteler için gerekli olan yönetimsel desteği işaret etmeli ve bilgi ve bilgi değerlerinin nasıl ele alacağına ilişkin yön vermelidir.

3.1.4.1.2. Bilgi Güvenlik Politikası Kabul Etmek

Proje yöneticisi iş planlarına bağlı olarak bu prosedürü kabul edilmeli ve zorunlu hale getirmelidir. Güvenlik yöneticisi politikanın iyi biliniyor, anlaşılmış ve tüm proje yöneticisi ve üyeleri tarafından kabullenilmiş olmasını sağlamalıdır. Tüm alt yükleniciler de bu politikayı kabul etmelidir.

3.1.4.1.3. Bilgi Güvenlik Politikasını Güncellemek

Bilgi güvenlik politikasının herhangi bir ihtiyaçta güncellenmesi gerekir. Şirketin ve ortamın gelişimi, politikanın bazı noktalarda eklenti veya değişiklik gerektirebilir. Değişiklikler yönetim tarafından onaylanmalı ve güvenlik temsilcisi tarafından zorunlu hale getirilmelidir.

3.1.4.1.4. Bilgi Güvenlik Politikasının Kabul Edilmesi

Bilgi güvenliği Politikasındaki tüm değişiklikler kurul tarafından onaylanmalıdır. O andan itibaren değişiklikler zorunlu olmakta, eski politikalar iptal edilmeli ve depolanmalıdır. Bütün çalışanların değişikliklerden haberdar edilmesi gerekmektedir.

3.1.4.2. Varlık Belirleme ve Sınıflandırma Prosedürü

Bilgi varlıklarının envanteri, her bilgi sistemiyle bağlantılı olan önemli bilgi varlıklarını içerecek şekilde, ilgili güvenlik yönetim birimlerince hazırlanmalıdır. Bu prosedür:

-Her bir varlığın hangi kategoride olduğu açıkça tanımlanması,

-Varlıkların sınıflandırmasının yapılması,

-Varlık değerinin belirlenmesi,

-Varlık sorumlularının atanması,

-Varlığın mevcut bulunduğu yerin belirlenmesi,

-Her bir varlık için tanımlayıcı bir kod verilmesi, faaliyetlerini içerecektir.

3.1.4.2.1. Varlık Kategorileri

Bilişim sistemleriyle ilgili varlıklar, bilgi, yazılım ve fiziksel varlıklar ile servisler olmak üzere dört kategori altında aşağıdaki Tablo 9'daki gibi bölümlenebilir.

Tablo 9. Varlık Kategorileri

Kategori	No	Tanım
Bilgi Varlıkları	1	Bilgi içeren elektronik ortamda yada basılı bulunan varlıklardır. Alt kategoriler: a) Veritabanları, b) Veri dosyaları, c) Basılı materyal (sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, sözleşmeler vb.) d) Arşivlenmiş bilgi, e) Diğer (Yukarıdaki alt kategoriler dışında bulunan bilgi varlıklarıdır.)
Yazılım Varlıkları	2	Kullanılan dışarıdan temin edilmiş yada kurum içerisinde geliştirilmiş yazılımlar bu kategoride değerlendirilecektir. Alt kategoriler: a) Uygulama yazılımları (dışarıdan alınmış), b) Uygulama yazılımları (kurum içinde geliştirilmiş), c) Uygulama yazılımları (kurum için dışarıdan geliştirilmiş), d) Sistem yazılımları (dışarıdan alınmış), e) Sistem yazılımları (kurum içinde geliştirilmiş), f) Sistem yazılımları (kurum için dışarıdan geliştirilmiş), g) Geliştirme araç ve yazılımları, h) diğer

Fiziksel Varlıklar	3	Birimde kullanılan fiziksel varlıklardır. Alt kategoriler: a) Bilgisayar ekipmanları (pc, server, mainframe, diz üstü bilgisayarlar, modemler vb.), b) iletişim ekipmanları (yönlendirici, telefon, faks vb.), c) manyetik kayıt ortamları (teyp, kartuş, disket, disk, cd vb.), d) diğer teknik ekipmanlar (güç kaynakları, adaptör, havalandırma üniteleri vb.),
Servisler	4	Kurumda sağlanan yada alınan kritik servislerdir. Alt kategoriler: a) Verilen Bilgi işleme hizmeti b) Alınan Bilgi İşleme Hizmeti c) Verilen İletişim hizmeti d) Alınan İletişim hizmeti e) Diğer servisler (Yukarıdaki alt kategoriler dışında bulunan servislerdir.)

3.1.4.2.2. Varlık Sınıflandırması

Bilgi varlığı; korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmalıdır. Bilgi varlığı, çok gizli, gizli, kuruma özel, hizmete özel, kişiye özel ve tasnif dışı olmak üzere toplam altı şekilde güvenlik sınıflandırmasına tabii tutulacaktır. Sınıflandırmaya ilişkin detaylar Tablo 10'da sunulmuştur.

Tablo 10. Bilgi Güvenlik Sınıflandırması

Derece	No	Tanım
Çok Gizli	1	Kaybı yada yetkisiz kişilerin eline geçmesi durumunda çok ciddi sorunların yaşanacağı bilgi varlıklarıdır. Kurum, Bağlı birimler ve diğer kamu birimleri tarafından üretilen veya bu makamlar için üretilerek arz edilen bilgiler, çok gizli kategorisinde olabilirler. Örneğin Bakanlar kurulu kararları, Yönetim Kurulu Kararları, karar dosyaları, Kurum Toplantı Notları, Kurum Strateji Dokümanları, diğer kuramlarla yapılan protokoller vb gibi. İzinsiz olarak açıklandığı takdirde kurumun güvenliğini, çıkarlarını ve diğer kurumlarla ilişkilerini olumsuz yönde etkileyebilecek, kurumun maddi manevi büyük zararına neden olabilecek nitelikte olağanüstü önem taşıyan bilgi varlıkları çok gizli olarak nitelendirilir. Çok gizli bilgi varlıkları, güvenliği sağlanmış ve sadece yetkili kişilerin girebileceği odalarda bulunan kasa ya da kilitli dolaplarda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.
Gizli	2	Kurumun faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda, sorunların yaşanacağı bilgi varlıklarıdır. Gönderilen makamı ilgilendiren, sadece o makamın görebileceği bilgi türüdür. Gerekli izin alınmadan açıklandığında kurumun güvenliği, saygınlık ve çıkarları ciddi suretle zedeleyen, diğer yandan yabancı kurumlara geniş yararlar sağlayabilecek olan bilgi varlıklarıdır. İş planları, fiyat teklifleri, sözleşmelerle ilgili bilgiler gizli kategorisine örnek olarak verilebilir. Kasa ya da kilitli ortamda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.

Kuruma Özel	3	Kurum dahilinde üretilen; yönergeler, standartlar, prosedürler, politikalar ve bu bilgilerin bulunduğu ortamlar vb. gibi, Kurum dışına çıkarılması için üst yönetimden onay alınması gereken bilgi varlıklarıdır. Kurum içinde kullanımında, kopyalanmasında sakınca yoktur. Örneğin personel, sağlık yönetmeliği, izin ve rapor prosedürü gibi. Ancak yukarıda belirtilen dokümanlardan içeriği itibarı ile sadece kurumdaki yetki verilmiş kişilerin erişebileceği dokümanların gizlilik derecesinin kuruma özel olarak değil, uygun olan şekilde (çok gizli, gizli, hizmete özel gibi) verilmesi gerekir.
Hizmete Özel	4	Sadece belli bir grup tarafından, örneğin proje ekipleri, belli bir birim gibi, görülebilecek olan bilgi varlıklarıdır. İçerdiği konular itibarıyla, diğer gizlilik dereceli konular dışında olan, ancak güvenlik işlemine ihtiyaç gösteren bilgi varlıkları hizmete özel olarak sınıflandırılır. Projeler özelinde üretilen proje planı, tasarım ve gereklilik dokümanları, kaynak kodlar ve bu bilgilerin bulunduğu ortamlar vb. örnek olarak verilebilir. Gizli varlıklar gibi, yetkili kişi izni ile kopyalama, iletme ve imha işlemi yapılmalıdır.
Kişiye özel	5	Sahibine özel kullanılan bilgi varlıklarıdır. Herhangi bir güvenlik derecesine sahip olmayan, iş ile ilgili yada iş dışındaki bilgilerdir. Örneğin kişisel elektronik mektuplar gibi.
Tasnif Dışı	6	Kullanılması güvenlik açısından önemli olmayan, kurumdaki veya kurum dışındaki her kişiye açık bilgilerdir. Örneğin duyurular vb.

3.1.4.2.3. Varlık Değerinin Belirlenmesi

Bilgi varlığının kurum açısından değerini Tablo 11'deki verildiği gibi değeri 0'dan başlayarak 4'e kadar belirlenecek ve alçak, düşük, orta, yüksek ve çok yükseğe kadar sınıflandırılacaktır.

Tablo 11.Varlık Değerleri

Derece	**Değeri**	**Tanım**
Alçak	0	Varlık bilgi sisteminin bir parçası değil (Örnek: Sistem Yöneticisinin masasındaki çiçek)

Düşük	1	Varlık bilgi güvenlik sisteminin işleyişi açısından önemli değil fakat sistemin bir parçası ve arızalandığında tamir edilmeli veya değiştirilmeli (Örnek: Monitör, klavye)
Orta	2	Bu varlık, iş sürecinde oldukça değerlidir ve yerine başka varlık kullanılabilir. Kaybı yada zarar görmesi orta derecede etkiye sebep olabilir (Örnek: Ağ Kartı). Bu varlığın yeri doldurulabilir, değerlidir ancak iş devamlılığında hafif bir etkisi olur. Kaybı yada zarar görmesi durumunda, düşük bir maliyetle yeri doldurulabilir.
Yüksek	3	Bilgi Güvenlik Sisteminin kritik bir varlığının yedeğidir (tam yedek diski).
Çok Yüksek	4	Bu bilgi varlığı, Kurum için çok yüksek değer taşımaktadır. Kaybı yada zarar görmesi Kurumun faaliyetlerinin devamlılığında şiddetli etkiye sebep olabilir.

3.1.4.2.4. Varlık Sorumlularının Belirlenmesi

Her varlık için iki kişi sorumlu belirlenmelidir. İlk sorumlu, varlığın yaratıcısı olabileceği gibi, varlığa erişmesi gerekenleri yetkilendirme kararını veren ve varlık üzerinde yapılması gereken işlerde onay alınması gerekli kişidir. İkinci varlık sorumlusu, ilk varlık sorumlusunun ulaşılamadığı durumlarda varlıktan sorumlu olan yedek ikinci kişi olmalıdır.

3.1.4.2.5. Varlığın Bulunduğu Yerin Tespiti

Varlığın bulunduğu bina, kat, oda, (varsa dolap) belirtecek şekilde verilmelidir. Elektronik ortamdaki bilgi varlıklarında sistemin bulunduğu yer bilgisi de belirtilmelidir.

3.1.4.2.6. Varlık Tanımlama Kodu Verilmesi

Her birimin tespit ettiği varlığa vereceği varlık kodu aşağıdaki formatta olmalıdır:

XXX_YY_Z_KKKK

XXX: Bölüm kodu (Tablo 12'de bölüm kodlarının açılımı verilmiştir.)

YY: Varlık kategori no

Z: Varlık alt kategori

KKKK: 0000 dan başlayan dört haneli sayı

Örneğin Bilgi Yönetim Müdürlüğü birimindeki bilgi varlığı için (veritabanı alt kategorisinde) tanımlama kodu "BYM_01_a_0001" şeklinde olmalıdır.

Tablo 12. Bölüm Kodları

Bölüm	**Bölüm Kodu**
Bilgi Yönetim Müdürlüğü	BYM
İdari Hizmetler Müdürlüğü	İHM
Mühendislik Planlama Müdürlüğü	MPM
Mühendislik Optik Tasarım	MOT
Mühendislik Seyrüsefer Tasarım	MST
Mühendislik Görüntü İşleme	MGİ
Mühendislik Laser Tasarım	MLT
Mühendislik Gece Görüş	MGG
Mühendislik Elektronik Tasarım	MSV
Mühendislik Kara Tasarımı	MKT
Mühendislik Hava/Deniz Tasarımı	MHT
Üretim Planlama	ÜP
Üretim Elektronik	ÜE
Üretim Mühendislik	ÜM
Sözleşme Takip	ST
Entegre Lojistik Destek	ELD
Mali Analiz	MA
Bilgi Güvenlik	BG

3.1.4.3. Personel Prosedürü

Bu prosedürün temel amacı bilgi güvenliğinin sağlanması doğrultusunda ASELSAN çalışanlarının ilgili tüm işlemleri ile bir bütünlük oluşturmaktır. Şekil 33'te bilgi güvenliğinin tesisine yönelik personel prosedürüne

ilişkin sorumlulukları, görevleri ve çıkan ürünleri açıklamak üzere oluşturulmuş olup temel olarak ana elemanları şunlardır;

-Çalışmak isteyen adayları incelemek,

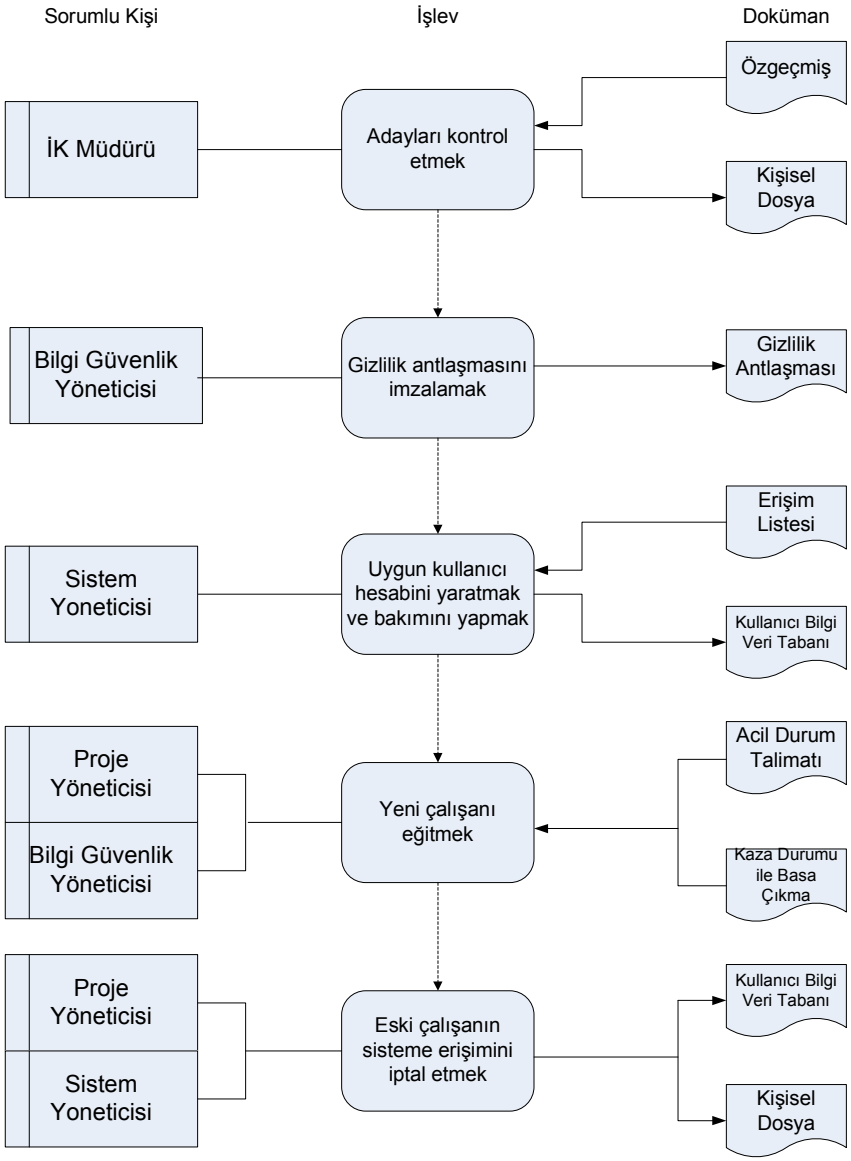
-Gizlilik anlaşmasını imzalamak,

-Kullanıcı bilgi veri tabanı oluşturmak,

-Uygun kullanıcı hesabı oluşturmak,

-Çalışanları eğitmek,

-Eski çalışanın sisteme girişini engellemek, olarak sıralanabilir.



Şekil 33. Personel Prosedürü

3.1.4.3.1. Adayları Kontrol Etmek

Prosedürün bu kısmından amaçlanan, ASELSAN'da çalışmak isteyen adayların kontrolünü standardize etmektir. Bilgi burada kritik bir rol oynar, böylece tüm çalışanlarınızın gerekli yeterliliklere sahip ve güvenilir olmalarından emin olabiliriz. Bu amaçla aşağıdaki kontrollerin yapılmasını gerekli kılar.

-CV'lerin yeterliliklerine göre kontrol etmek,

-Kimlik,

-İş referansının,

-Kişisel referansın kontrolü,

şeklinde sıralanabilir.

3.1.4.3.2. Gizlik Anlaşması İmzalamak

Çalışan ile ASELSAN arasında, iş ile ilgili her türlü kişisel veya şirkete ait bilginin, alt yükleniciler dahil diğer kuruluşlara yazılı izin alınmadığı sürece açıklanamayacağına ilişkin yazılı taahhüt altına alınması işlemidir. Bu anlaşmanın bozulması durumunda yapılacak işlemler gizlilik anlaşmasında tanımlanacaktır.

3.1.4.3.3. Kullanıcı Bilgi Veritabanı Oluşturmak

Kullanıcı bilgi veritabanı tüm gerekli bilgileri ve kimlik kanıtlamak için gerekli bilgileri içerir. İhtiyaç anında çalışanın tüm bilgilerini verebilmesi gerekmektedir. Bilgi veritabanı kullanıcı ismi, şifre ve kullandığı gruplar gibi bilgiler içerir. En gerekli parçası erişim listesidir. İş amaçları için kullanılacaksa e-imza anahtarları (şirket ve kişisel) burada depolanmalıdır.

Kullanıcı bilgi veritabanı bilgisayarın hafızasında depolanır ve başlangıç ve diğer yazılımların çalıştırılmasında kullanılır. Kullanılan platforma göre yapısı ve görünüşü oldukça farklılık gösterebilir. Sistem yöneticisi Proje Yöneticisi ve İK müdüründen aldığı bilgilerle bu veritabanını oluşur.

3.1.4.3.4. Kullanıcı Hesabı Oluşturmak

Bu prosedürün ana amacı kullanıcı hesapların düzenli ve güvenli durmasını sağlamaktır. Kullanıcıların ASELSAN bilgi değerlerine erişimi ancak uygun

ulaşım haklar ile verilebilir. Şekil 34'te kullanıcıların bilgi erişim prosedürü grafiksel olarak gösterilmiş olup, ana elemanları:

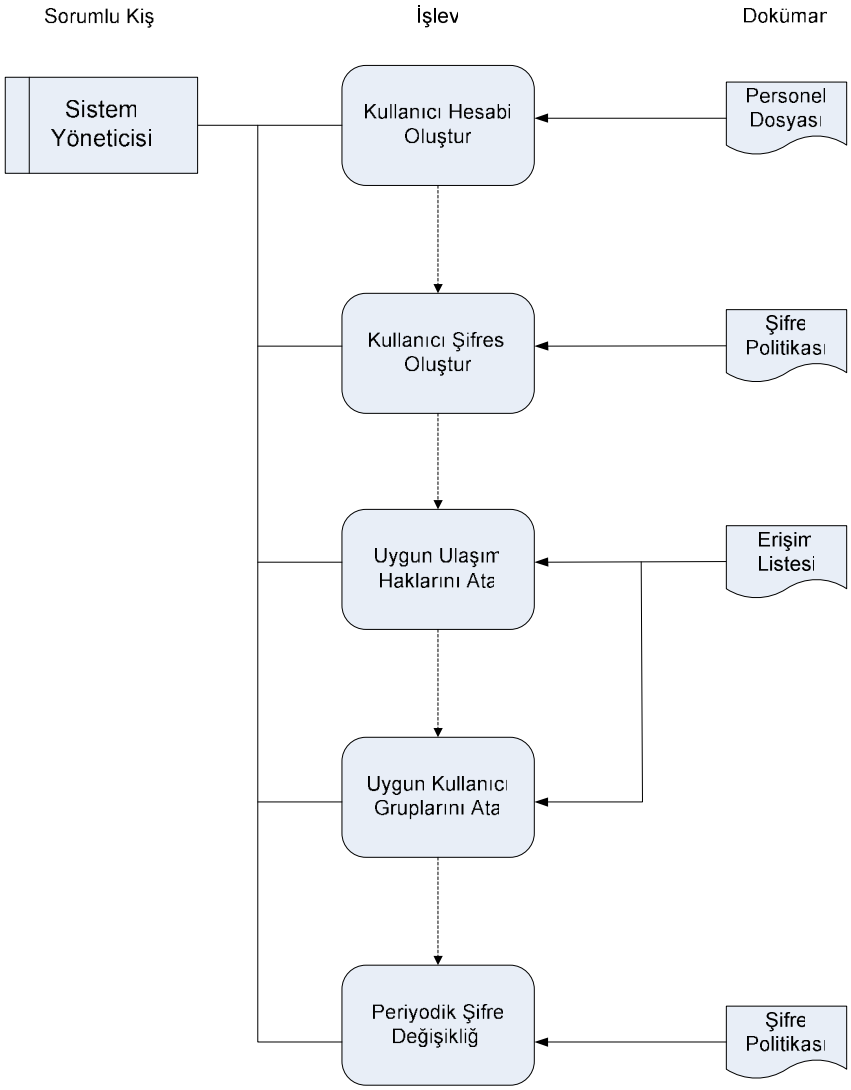
-Kullanıcı hesabı oluşturmak,

-Şifre oluşturmak,

-Uygun ulaşım haklarını atamak,

-Uygun kullanıcı gruplarını atamak,

-Düzenli şifre değişimi, yapılmasını içermektedir.



Şekil 34. Kullanıcı Erişim Prosedürü

3.1.4.3.5. Çalışanları Eğitmek

Prosedürden amaçlanan yeni çalışanların eğitimi için gereken adımların birleştirilmesi, her çalışanın ASELSAN'ın amaçlarını, çalışma prosedürlerini,

görevlerini ve Bilgi Güvenlik Sistemindeki rolünü anlamış olmasını sağlamaktır. Şekil 35'te personele verilecek eğitim kapsamı ve sorumlulukları grafiksel olarak gösterilmiştir. Bu amaçla, personele proje yöneticisi ve bilgi güvenlik yöneticisi sorumluluğunda aşağıdaki konularda eğitim verilmelidir.

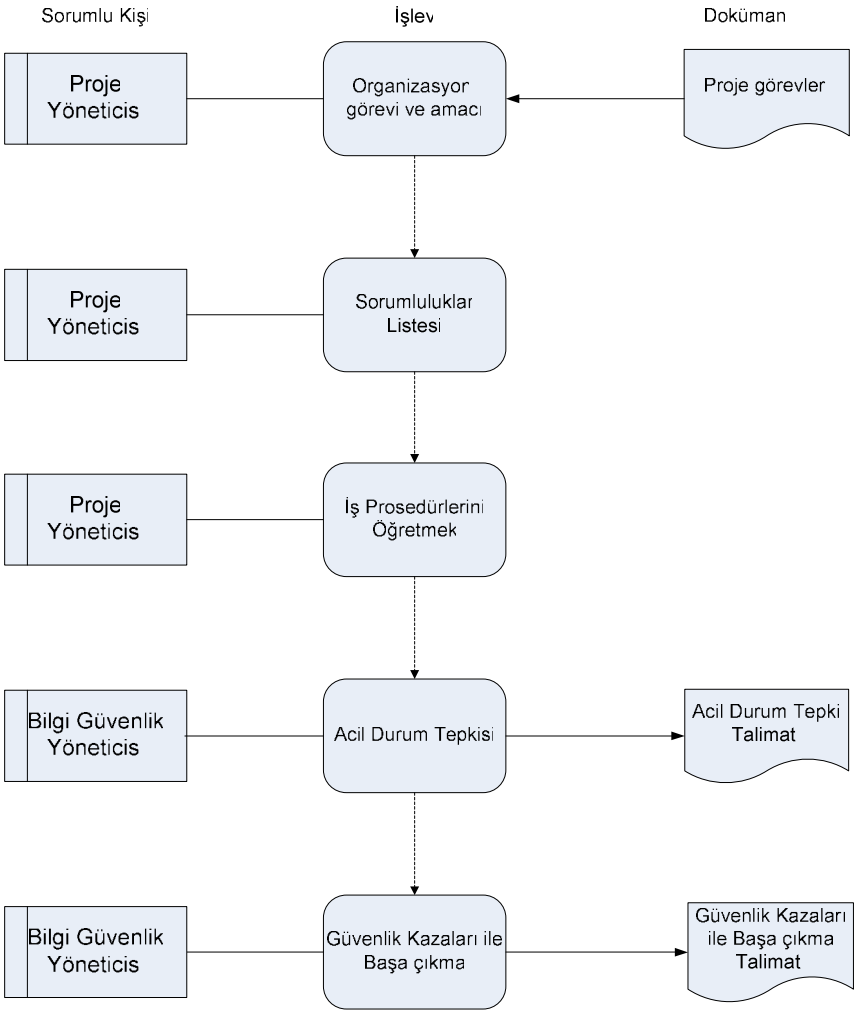
-Organizasyon, görevi ve hedefleri,

-Sorumluluk listesi,

-Çalışma prosedürlerini öğrenme,

-Acil duruma cevap verebilme,

-Güvenlik tehditlerine karşılık verebilmeyi kapsamaktadır.



Şekil 35. Personel Eğitim Kapsamı

3.1.4.3.6. Acil Duruma Cevap Verme Talimatı

Bu talimatın amacı, acil bir durumda iş kazası riskini ve bilginin hazır bulunması, güvenilirliği veya doğruluğu ile ilgili problem riskini azaltmak için uygun bir prosedürün işleme konulmasını sağlamaktır.

Risk Yönetim prosedürüne göre, bilgi güvenlik yöneticisi acil durum sayılacak tüm olayların listesini hazırlamaktan sorumludur. Daha sonra, bu listeye göre detaylı talimatlar hazırlanacaktır. Bilgi güvenlik yöneticisi listeyi ve talimatları güncel ve kolay ulaşılabilecek şekilde tutmaktan sorumludur.

Acil durum, çalışanlara veya diğer insanlara fiziksel tehlike yaratabilecek veya organizasyonların varlığını tehdit eden olaylardır. Acil olarak sınıflandırılan olaylar:

-Yangın,

-Sel,

-Bina yıkılması,

-Soygun,

-Hırsızlık,

-Stratejik bilgi kaçakçılığı,

-Büyük sistem hasarı, sayılabilir.

Her acil durum şirket içinde krize neden olabilir. Bu tür olaylar karşısında yapılacakların anlatıldığı prosedürler atılması gereken adımları tanımlar. Her acil durum cevap prosedürünün genel kuralı insanların hayatını ve sağlığını korumaktır. Eğer insanların güvenliği sağlanırsa, ikinci öncelik ASELSAN'ın varlıklarının korunmasıdır.

Her çalışan düzenli olarak acil durum prosedürleri konusunda eğitilmeli ve yangına müdahale cihazlarının kullanımı ve alarm cihazları ile ilgili eğitim almalıdır. Bilgi güvenlik yöneticisi, acil durumlarda, ASELSAN'ın beraber çalışacağı organizasyonların listesini hazırlamak ve görünür yerlere yerleştirmekten sorumludur. İtfaiye, polis, acil yardım, banka, avukatlık bürosu, hissedarlar ve yatırımcılarla paylaşılacak bilginin bulunduğu plan hazırlanmalıdır.

3.1.4.3.7. Güvenlik İhlallerine Cevap Verme Talimatı

Güvenlik ihlali, bilginin güvenilirliğini, kullanılabilirliğini ve gizliliğini tehlikeye atan olaylar olarak adlandırılır. Bu talimatın amacı her tür güvenlik

ihlalinin düzgün bir biçimde ele alınmasını sağlamaktır. Risk Analizine bağlı olarak, bilgi güvenlik yöneticisi, olabilecek tüm olayların listesini hazırlamak ve hangisinin güvenlik ihlali olduğunu belirlemek zorundadır. Buna bağlı olarak daha detaylı talimatlar hazırlamaktan ve bu listenin güncel tutulmasından sorumludur. Güvenlik ihlalleri sırasında uyulması gereken kuralları aşağıdaki gibi verebiliriz.

-Çalışmayı durdurun ve hiçbir şeyi onarmaya çalışmayın,

-Her zaman, hemen bir uzman çağırın,

-Her şeyi not alın (özellikle ekranda gözüken mesajlar),

-Daha önce yaptıklarınızı not edin,

-Uzman görüşlerinin izlenmesi, olarak sayılabilir.

3.1.4.4. Bilgisayar Sistemlerinin Sürdürülebilirliği

Bu prosedürün amacı bilgi güvenliği açısından gereken her türlü tedbirin bilgisayar sistemlerinde alınmasını sağlamaktır. Bu amaçla sistem kurulumu, ayarları, günlük faaliyetler, zorla giriş testleri, ağ testleri, yedekleme ve sistem yükseltimi kapsamında yapılacak faaliyetlerin detayları aşağıda sunulmuştur.

Sistem kurulumu: Yeni bir sistemin kurulması olsun, bir sistemin yedeğinden yüklenmesi olsun her sistem kurulumunda dikkat edilmesi gereken noktalar vardır. Kurulum sırasında, bilgisayar sistem bileşenlerini tanıtan, ana ayarları tanıtan ve yüklenen programların listelendiği bir "Sistem Dokümantasyonu" dokümanı hazırlanmalıdır. Bu tip bir doküman sistem tekrar kurulumunu için yardımcı olur. Kurulumdan sonra, Sistem Yöneticisi kurtarma diskleri yaratmalı ve tüm CD'lerin, kurulum disklerinin, lisansların ve kullanım kılavuzlarının uygun şekilde saklandığından emin olmalıdır.

Sistem ayarları: Sistem Yöneticisi, tüm sistemin düzgün çalışması için ayar yapmaktan başka tüm sistemin güvenli olduğundan emin olmalıdır. Örneğin tüm şifre korumasız hesaplar bloke edilmeli, gereksiz programlar devre dışı bırakılmalıdır. Ağ hızlı ve güvenli çalışacak şekilde ayarlanmalıdır. Tüm ayar bilgileri "Sistem Dokümantasyonu" içine eklenmelidir

Sistem "günlük" işleri: "Günlük" iş hesap yaratma, şifre değiştirme gibi aktivitelerden oluşur. Sistem Yöneticisi, Güvenlik Temsilcisi ile beraber, tüm yazılımın ve donanımın düzgün kullanıldığından ve korunduğundan emin olmalıdır. "Günlük" işin çok önemli

bir parçası, olay raporlarının analizi ve bu raporlardan hataların öğrenilmesidir. Olay, ne yazık ki "günlük iş olarak tanımlanabilecek kadar sık olan sistemin kilitlenmesi ve daha sonra tekrar başlatılmasıdır. Bu tekrar başlatma işleminin düzgün bir biçimde yapılması için talimatlar hazırlanmalıdır.

Zorla giriş testleri: Kontrol Planına göre, sistemin güvenlik seviyesini ölçmek için zorla giriş testleri yapılmalıdır. Sistem Yöneticisi, dâhili uzmanlar (eğer gerekli ise harici profesyonellerin yardımı) ile beraber sistemin bilinen tüm saldırılara (Tehdit kataloguna bağlı olarak) hazır olduğundan emin olmalıdır.

Ağ testleri: Kontrol Planına göre, ağ testleri, ağın performans seviyesini kontrol etmek için yapılmalıdır. Kesintisiz bilgi alışverişini garanti altına almak için yerel ağları hızlı ve güvenilir tutmak önemlidir.

Yedekleme: Tüm gerekli bilgilerin yedeklerinin düzgün bir şekilde alındığını ve bu işlemlerin düzgün bir şekilde sonlandırıldığından emin olmak Sistem Yöneticisinin görevidir. Ayrıca, tüm yedeklerin uygun şekilde şifrelenip paketlenmesinden, güvenli bir biçimde saklanmasından ve gerektiğinde bu yedeklere uygun çalışanların kolayca erişebildiğinden emin olmalıdır. Bu işlem Bilgi güvenlik yöneticisi uygun bir şekilde gerçekleştirildiğini kontrol etmelidir.

Sistem yükseltimi: Sistem yükseltmesi sadece gerçekten buna değer ise yapılmalıdır. İlk olarak tüm gerekli donanım, yazılım, eklentiler ve sürücüler toplanmalıdır. Daha sonra, tüm değişiklikler ağa bağlı olmayan bir makinede yapılmalıdır. Eğer sistem yükseltildi ise, dahili hata olmadığının kontrolü için, bir seri test yapılmalıdır. Zorla giriş testide bu kontrolün bir parçası olabilir. Yükseltmeden önce, herhangi bir problem durumunda geri dönebilmek için, tüm sistemin yedeğini almak zorunludur. Yükseltmeden sonra bir seri test daha yapılmalıdır. Sistem yükseltişinden hemen sonra, "Sistem kurulumunda" belirtildiği gibi, sistem dokümantasyonunda gerekli düzenlemeler yapılmalıdır.

3.1.4.5. Risk Yönetim Prosedürü

Bu prosedürün ana amacı doğru risk yönetimi yapmak için talimatlar vermektir. Risk Analizi sonuçlarına göre belirginleşecek olan tehditler ve Bilgi Güvenlik Sistemini tehdit eden dahili ve harici riskler, Risk Yönetimi prosesine taban

oluşturacaktır. Bu prosedürün ana elemanları Şekil 36'da detaylı olarak vurgulanmakla birlikte, aşağıdakilerden oluşmaktadır:

-Tüm bilgi varlıklarının tanımlanması,

-Zayıflık analizi,

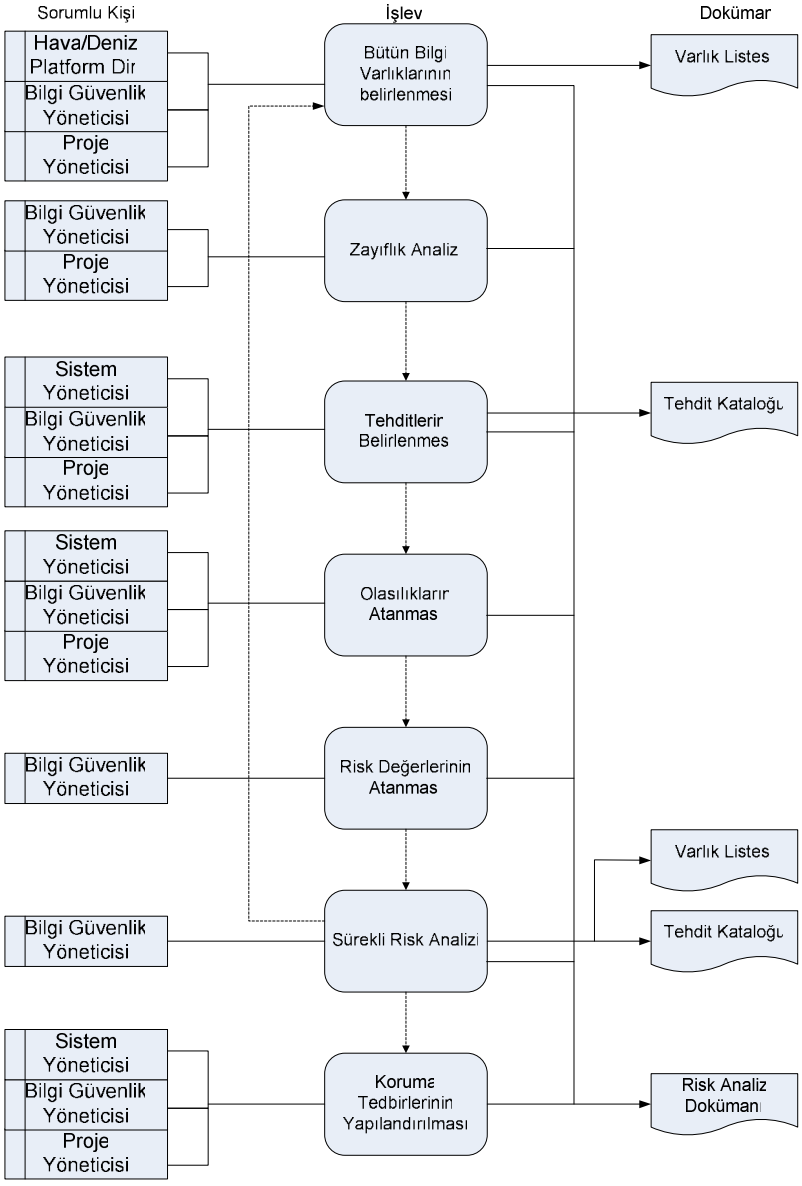
-Tehdit tanımlaması,

-Olasılıkların atanması,

-Risk değerinin atanması,

-Korumaların gerçekleştirilmesi,

-Kritik Olasılık Planı.



Şekil 36. Risk Yönetim Prosedürü

3.1.4.5.1. Tüm Bilgi Varlıklarının Tanımlanması

ASELSAN sürekli evrim geçirmektedir. Tüm varlıklar çok kısa bir süre içinde değişebilir ve tüm bilgi varlıklarının sürekli izlenmesi çok önemlidir. Proje yöneticileri, bilgi güvenlik yöneticisi talimatları ile ASELSAN'ın bilgi varlıklarının listesini oluşturmakla yükümlüdür. Bu liste bilgi güvenlik yöneticisi tarafından saklanacak ve daha sonra, risk analizi ve koruma veya kontrol önerme amacı ile kullanılacaktır. Varlık listesi bilgi, yazılım, fiziksel ve servis şeklinde bölünecek ve bu bölümün 3. maddesinde belirtildiği şekilde sınıflandırılacak, her varlık bu gruplardan sadece birine atanacaktır.

3.1.4.5.2. Zayıflık Analizi

Varlık listesine göre bilgi güvenlik yöneticisi, proje yöneticileri ile birlikte, varlıkların zayıflık listesini hazırlamak durumundadır. Liste hem teknik hem de organizasyon seviyesinde zayıflıkları içermelidir. Zayıflıklar, temel olarak varlıkların özelliklerine bağlı tehditlerin unutulmamasına karşı bir koruma sağlar.

3.1.4.5.3. Tehdit Tanımlaması

Varlık listesi ve zayıflık listesi bilgi güvenlik yöneticisine, bir muhtemel tehditler listesi oluşturmak için taban oluşturur. Bu görev zayıflık analizi ile paralel olarak yürütülmelidir. Bu görevlerin sonuçları proje yöneticisi ve sistem yöneticisinin yakın işbirliği ile toplanmalıdır. Bu aşamadaki hatalar tüm sistemin güvenliğini etkiler. Tehdit tanımlamasının sonuçları, daha ileri Risk Analizlerinde taban oluşturmak açısından, ayrı bir "Tehdit Katalogu" dokümanında toplanır. Tehdit katalogundaki bilgiler, ilgili herkesin doğru güvenliğini sağlamak için, müşteriler ve üçüncü taraflar ile paylaşılabilir.

3.1.4.5.4. Olasılıkların Atanması

Her tehdide bir gerçekleşme olasılığı atanmalıdır. Bu görev, kendi uzman bilgisine dayanarak, bilgi güvenlik yöneticisi, kendi uzmanlıklarına dayanarak, proje yöneticisi ve sistem yöneticisi tarafından gerçekleştirilir. Olasılıkların

atanmasında, Tablo 13.'ten yararlanılır ve olasılıkları imkansız olanı 0'dan başlayarak devamlı olanı ise 5'e kadar olacak şekilde aralardakilere rakam karşılıkları atanır.

Tablo 13. Olasılık Değerleri

0	İmkansız	20 yılda 1
1	Muhtemel değil	5 yılda 1
2	Az olası	Yılda 1
3	Olası	Ayda 1
4	Sık sık	Günde 1
5	Devamlı	Günde 1'den fazla

3.1.4.5.5. Risk Değerinin Atanması

Risk değeri, varlık değeri ve olasılığın çarpımıdır. Şekil 37'de risk değerlerinin alabileceği sınır değerler verilmiş olup, eğer risk değeri 8'e eşit veya daha yüksek ise veya varlık değeri 4 ise veya olasılık değeri 5 ise hemen önlem alınması gerekir. Güvenlik marjındaki bölgeler(4–6) güvenlik altına alınmalıdır ama düşük önceliklidir. Eğer risk değeri 3'ün altında ise güvenlik önlemine gerek yoktur ama sürekli kontrol, ani durum değişiklikleri için gereklidir.

		Olasilik					
		0	1	2	3	4	5
Varlık Değerleri	0	0	0	0	0	0	0
	1	0	1	2	3	4	5
	2	0	2	4	6	8	10
	3	0	3	6	9	12	15
	4	0	4	8	12	16	20

Şekil 37. Risk Değerleri

3.1.4.5.6. Sürekli Risk Analizi

Sürekli ortam değişimleri, varlık değerlendirmesi, yeni zayıflıkların eklenmesi ve yeni tehditlerden dolayı, sürekli risk analizi yapmak önemlidir. Geç kalmış hareketler kötü sonuçlar doğurabilir. Bilgi güvenlik yöneticisi ana görevi Risk Analizi prosesini sürdürmektir.

3.1.4.5.7. Korumaların Gerçekleştirilmesi

Risk değerine göre bir sıra içinde, organizasyon belirli görevlere korumalar gerçekleştirmelidir. Her yüksek seviyeli risk uygun koruma ile azaltılmalıdır. Diğer elemanlar için risk değerini dikkate alan kontroller gerçekleştirilmelidir. Proje yöneticisi, sistem yöneticisi ve bilgi güvenlik yöneticisinin önerilerine göre, tüm gerekli korumaları gerçekleştireceklerdir.

3.1.4.5.8. Kritik Olasılık Planı

Risk analizi, ASELSAN'ın faaliyetini sürdürebilmesi için, hangi varlıkların önemli olduğunu kontrol eder. Bilgi güvenlik yöneticisi, Risk Analizi sonuçlarına dayanarak, Kritik Olasılık Planları oluşturmak zorundadır. Böyle bir plan, en zor zamanlarda faaliyeti sürdürmeyi ve tekrar işe dönmeyi sağlayacak tüm hareketleri içerir. Günlük işler için gerekli önemli bilgilerin listesi, muhasebe için gereken bilgi ve en önemli varlıkların bir listesi yapılmalıdır.

Kritik Olasılık Planı, Kriz Haberleşme listesini (Tüm gerekli kişilerin bilgileri ve kriz durumunda haberleşme sırası) içermelidir. Güvenlik temsilcisi tüm gerekli varlıkları toplamak zorundadır ve uygun saklama yerini belirleyip, uygulamaya geçirir. Bu yer, güvenli, hırsızlığa ve varlıkların hasar görmesine karşı dayanıklı, şirkete erişim engellendiği durumlara karşı, ASELSAN'ın dışında bir yer olmalıdır. Kritik Olasılık Planı, ASELSAN'ın kriz bitinceye kadar hayatta kalmasını sağlamalıdır.

3.1.4.6. Kontrol Prosedürü

Bu prosedürün amacı tüm sistemin planlanan şekilde çalıştığına emin olmaktır. Bunu yapmak için kontrol sistem bileşenlerinden bir liste oluşturulur. Kontrol, ASELSAN'ın BGYS'deki hataları, bu hataları kullanan bir olay meydana gelmeden, bulmasını sağlamaktır. Bu amaçla kontrol prosedürün ana elemanları;

-Kontrol edilecek sistem bileşenlerinin tanımlanması,

-Kontrol,

-Raporları oluşturma,

-Raporları cevaplama,

şeklinde sıralanabilir.

3.1.4.6.1. Sistem Bileşenlerinin Tanımlanması

Faaliyetleri sürdürebilmek için gerekli sistem bileşenlerinin düzgün bir biçimde bakılması ve sistemin prosedürlere uygun olarak yürütüldüğünü kontrol etmek için bir kontrol planı oluşturulmalıdır. Güvenlik temsilcisi, kurul üyeleri ile birlikte kontrol için gereken elemanlardan oluşan bir liste yaratır. Böyle bir liste, bileşen isimlerini, kontrol sıklığını, kontrol yapacak kişiyi ve prosedürü tanımlar. Liste, sık kontrol gerektiren varlıkları ve sistem elemanlarını da içermelidir.

3.1.4.6.2. Kontrol

Tüm kontroller detaylı prosedürlere göre yapılmalıdır. Bunların yapılıp yapılmadığının kontrol edilmesinden sorumlu olan kişi güvenlik temsilcisidir. Görev tanımında kontrol raporlarını kontrol etmek ve bulunan problemleri gidermek için gereken adımların yapılıp yapılmadığının kontrolü de vardır.

Kontrolden sorumlu her çalışan güvenlik temsilcisine raporları verir. Güvenlik temsilcisi bu raporların doğruluğunu kontrol eder ve kurul üyeleri ile yatırımcılara bunları rapor eder.

3.1.4.6.3. Raporları Oluşturma

Her kontrol bir raporla sonuçlanmalıdır. Böyle bir rapor, hazırlanma tarihli, kontrol amacını belirten, tüm problemleri sıralayan ve sistemi daha iyi hale getirmek için öneriler içermelidir. Kontrolde yer alan tüm çalışanlar raporu imzalamalıdır. Her rapor uygun şekilde saklanmalıdır, ancak güvenlik temsilcisi bu raporların kolay erişimini sağlamalıdır.

3.1.4.6.4. Raporları Cevaplama

Her kontrol ciddi ve düzgün hazırlanmış bir sonuç ile bitmelidir. Sadece sistem zayıflıklarını aramak değil aynı zamanda sistemi daha efektif yapacak değişiklikler önermek kontrol yapan ve rapor hazırlayan her personelin görevidir. Aktivitelerden sorumlu proje yöneticisi, sistem yöneticisi ve güvenlik yöneticisi rapor sonuçlarına en kısa zamanda karşılık vermek zorundadırlar.

3.1.5. Risk Yönetimi

Proje kapsamındaki bilgi, yazılım, fiziksel varlıklar ve hizmetlerden oluşan varlıklar üzerinde Bölüm 3'te detayları verilen ve 4. Bölümün 3. maddesinde belirtilen prosedüre göre risk analiz sonuçları ve önerilen korumalar Tablo 14'te sunulmuştur.

Tablo 14. Proje Risk Analiz ve Değerlendirme Sonuçları

No	Varlık İsmi	Etki Değeri	Zayıflıkları	Tehditler	Olasılık	Risk	Önerilen Koruma
Bilgi Varlıkları							
1	Kullanıcı Veri Tabanı	3	Erişim Gerektiriyor	Silinebilir	3	9	Yönetici Tarafından Sahiplenmeli
				Değiştirilebilir	3	9	
				İçeriği Öğrenilebilir	3	9	Tek Yönlü Şifrelenmeli
				Kullanıcılar Bilgilerini Unutabilir	4	12	İş Süresince Yönetilmeli
2	Yazılım Lisansları	3	Sistem Bakımında Gereklidir (online yardım, yükseltme, vs.)	Kaybetmek / Yok etmek	2	6	Özel Bir Yerde Saklanmalı
							Kopyaları Çıkarılmalı
3	Bilgisayar Sistem Doküman-tasyonu	3	Sistem Bakımında Gereklidir (sorun giderme, yükseltme, vs.)	Kaybetmek / Yok etmek	2	6	Özel Bir Yerde Saklanmalı
							Kopyaları Çıkarılmalı
4	Sistem Doküman-tasyonu	4	Sistemin Düzgün Çalışması İçin Gerekli	Kaybetmek / Yok etmek	3	12	Özel Bir Yerde Saklanmalı
				Uygun Olmayan Prosedürleri İzlemek	3	12	Kopyaları Çıkarılmalı

Yazılım Varlıkları							
5	IBM AIX v. 4.3	4	Boot etmek	Yanlış Deamon/Program Yüklemesi	3	12	Kayıtları Analiz Etmeli
				Yanlış Bileşen Tanımlaması	3	12	
				Yanlış Aygıt Kontrolü	3	12	
			Kullanıcı Erişimi	Şifrenin açığa çıkması	4	16	Şifre Politikası Kullanmalı
						16	Her şifre kullanımı kayıtlanmalı
				Şifreyi Unutmak	4	16	Şifre Politikası Kullanmalı
				Uygun olmayan kullanıcı hakları	3	12	Erişim Listesi Kullanılmalı
				etc/bin/shadow	3	12	Root tarafından sahiplenilmeli
							"guest" ve "nobody" hesapları silinmeli
							hesapları yönetmek için "aduser" ve "rmuser" gibi sistem araçların kullanılmalı
			Uygunsuz Sistem Kapanışı	Uygunsuz Servis Sonlandırılması	3	12	Her zaman uygun komutları kullanılmalı (shutdown, reboot)
							Kesintisiz Güç Kaynağı kullanılmalı
			Başlangıç Skriptleri	Yanlış çok kullanıcı ayarı	2	8	Root tarafından sahiplenilmeli
							Kayıtlar Analiz Edilmeli
			acl	Çok düşük veya çok yüksek erişim hakları	4	16	Gerekli Erişim Listesine göre gerçekten gerekli ise kullanmalı
			Sticky Bit				Find komutu kullanmalı
			SUID&SGID				Ps komutun kullanmalı
			root	Kazara sistem hasarı riski	3	12	Hesaba sadece yönetim için bağlanmalı
							Herhangi bir değişiklik yapmadan sistem yedeklenmeli
				Kök hesabın hacklenme riski	3	12	Gereksiz özellikler kullanım dışı bırakmalı
							Güncellemeler yüklenmeli
							Şifre kullanmalı

							Netstat komutunu sık kullan
			netstat	Değiştirilebilirler ve yanlış bilgi verebilirler	5	20	Köke ayrıcalıklı silme ve değişiklik yapma yetkisi vermeli
			ps				
			df				
			du				File control-sum'ı kontrol etmeli
			top				
			ls				
			Find	Değiştirilebilir ve yanlış bilgi verebilir	5	20	File control-sum'ı kontrol etmeli
							Köke ayrıcalıklı silme ve değişiklik yapma yetkisi vermeli
				Çok fazla disk zamanı kullanıyor	3	12	Yüklenmiş dosya sistemleri içinde bilinen dosyaları aramak için (s)locate komutunu kullanmalı
							Köke ayrıcalıklı silme ve değişiklik yapma yetkisi vermeli
6	Apache Daemon 1.3.20	4	Web sayfasını kontrol eder	Servis dışı	2	8	v.1.3.22 sürümünü güncellemeli
				Bilgi sızıntısı	2	8	
				Web saldırısı	2	8	
7	Domain Name Server 8.2.2	4	Bağlamak	Uzak kök verme	5	20	v.8.2.5 veya v.9.1.3'e geçmeli
				Geçersiz ayar	5	20	Zone transfer'i devre dışı bırak
			Pek çok TCP servis için gerekiyor (e-mail, WWW, chat, SMTP)	Eğer server devre dışı kalırsa tüm bu servisler devre dışı kalır	3	12	Uygun DNS server ayarları kullan
8	FTP Daemon	2	Güvenli değil, kaynak kodunda hatalar mevcut	Bilgi transferini korumadan zayıf kimlik tespiti	5	10	Tüm dosyaları www üzerinden gönder
				Sık sunucu kök ayrıcalıklara sahip	5	10	
				Her "anonymous" kullanıcı bazı dosyaları alabilir	5	10	
				Bazen anonymous kullanıcı ayrıcalığı varmış gibi katalog yazabilir	4	8	
			Dosya alma ve gönderme	Yetkisiz dosya transferi	4	8	Netstat komutunu kullanmalı
				Kötü amaçlı dosyaların transferi	4	8	Bilgi Transfer Planı yapmalı
							Anti virüs yazılımı kurmalı ve sürekli güncel tutmalı
9	SendMail	2	Güvensiz	Mail iletme	5	10	Dahili çalıştırmalı

	Daemon 8.11.0						8.12.1 sürümünü güncellemeli
							Yazılım değiştirmeli
				Kötü amaçlı dosyaların transferi	4	8	Anti virüs yazılımı kurmalı ve sürekli güncel tutmalı
							Bilgi Transfer Planı yapmalı
				Zayıf kimlik tespiti	3	6	Bilgi Transfer Planı yapmalı
			SUID	Yetkisiz kullanıcılara yetki verebilir	4	8	Dahili çalıştırmalı
							Yazılım değiştirilmeli
			Popüler Protokollerde (SMTP, POP3) tekst temizlemek	Bilgi sızıntısı	3	6	Dahili çalıştırmalı
							Program Değiştirilmeli
							Mesajları Şifrelenmeli
			Mesaj Güvenliği	Değiştirilebilir	3	6	e-imza kullanmalı
				İzinsiz okunabilir	3	6	Şifreleme yapılmalı
			Unix servis loglarını yollamak için SendMail kullanıyor	Diğer servisleri rahatsız edebilir	4	8	Tüm değişiklikler iki kez kontrol edilmeli
10	Telnet INETD	2	Koddaki Yanlışlar	Zayıf Yetkilendirme	3	6	SSH v2 kullanmalı yazılım yüklenmeli
			Güvensiz	Buffer Taşması	5	10	Silinmeli
				Yetkisiz dosya transferi riski	4	8	Netstat komutu kullanmalı
				Zaralı Yazılım indirme riski	4	8	Bilgi Transfer Politikası Kurmalı
							Güncel anti virüs yazılımı kurmalı ve güncelliğini korumalı
			Tekst Temizleme	Veri Hackleme	3	6	Şifreleme yapılmalı
				Bilgilere yetkisiz Ulaşım	3	6	Bilgi Transfer Politikası Kurulmalı
							Uzaktan çalışmalar için SSH v2 programı kullanmalı
11	Chargen INETD	1	Güvensiz	Dos atakları (echo ile)	5	5	Silinmeli
			Gereksiz	Sunucu ataklarında kullanılabilir	5	5	
12	Echo INETD	1	Güvensiz	Dos atakları (echo ile)	5	5	Silinmeli
			Gereksiz	Sunucu ataklarında kullanılabilir	5	5	
13	Finger INETD	1	Bilgi yayınlamak	Hackerlar bilgisayar sistemi ve kişisel bilgileri ele geçirebilir	5	5	Silinmeli
			Gereksiz	Buffer Taşması	5	5	
			Güvensiz	Format String	5	5	

				saldırısı			
14	Windows NT 4.0	4	Kullanıcı Logini	Şifrenin açığa çıkması	4	16	Şifre Politikası Kullanmalı
				Şifreyi Unutmak	4	16	
				Uygun olmayan kullanıcı hakları	3	12	Erişim Listesi Kullanmalı
			Boot etmek	Yanlış sunucu / program kullanımı	3	12	NTFS Bölümlendirme kullanmalı
				Yanlış Bileşen Tanımlaması	3	12	
				Yanlış Aygıt Kontrolü	3	12	
			Uygunsuz Sistem Kapanışı	Uygunsuz Servis Sonlandırılması	2	8	Her zaman uygun komutları kullanmalı (shutdown, reboot)
				Bilgi Kaybı	2	8	Kesintisiz Güç Kaynağı kullanmalı
				Uç durumlarda insan desteksiz sistemi yeniden açamama	3	12	
			NetBios	Bilgi Yayınlanması	4	16	NetBios'u filtrelemeli
				Kaynaklara ulaşım verilmesi	4	16	
				Ağ üzerinden disk paylaşımı (güvenliği tam sağlanmamış, uygun olmayan erişimlere ve sistem kataloglanmasına izin veriyor olabilir)	4	16	İptal etmeli
			NTFS	Yanlış yedekleme	3	12	Tüm yedeklerin doğruluğunu kontrol etmeli
				Çok düşük veya çok yüksek erişim hakları vermek	3	12	Erişim Listesine gerekli hakları eklemeli
15	Service Pack 6a	4	Güvensiz	Yamaları Yüklemeyi Unutma Riski	4	16	SP6a Erolment Pack'i ertelememeli
16	Exchange Server 5.5	4	Mail Server	Bilgi sızıntısı	3	12	Şifrelemeli
							e-imza kullanmalı
				E-mektup iletimi	5	20	e-mektup iletimi devre dışı bırakmalı
			Sürekli disk dolumu	Sabit diskin dolum tehlikesi, program durması ve sistem tamirinin imkansızlığı	4	16	Disk alanını günlük olarak kontrol etmeli
							Artan şekilde yedekleme yapmalı
			Admin mod dışında çöp klasörünün silinmemesi	Sabit disk yerinin olmaması durumunda program çalışmayacak veya veri silmeyecek	4	16	Disk alanını günlük olarak kontrol etmeli
							Yedek sabit disk almalı
			Mailbox veri tabanı yönetimi	Veri tabanı bozulması	3	12	Yedeklemeli
				Ağ bağlantısı yok	3	12	Veri tabanını

				iken kullanıcıların mesajlarına ulaşamaması			birleştirmeli
				Veritabanının antivirüs programı ile taranması ile ilgili sorunlar	3	12	Workstation a anti virüs yazılımı kurmalı
			Mesaj güvenliği	Değiştirilebilir	3	12	E-imza kullanmalı
				İzinsiz okunabilir	3	12	Şifreleme yapılmalı
			Güvenlik modeli (OS parçası olarak ACL)	Kendi ayarları yanlış	4	16	ACL değiştirilmeli (erişim kontrol listesi)
				Büyük karışıklık, bir kısım işler Exchange bir kısım işler NT tarafından yapılmış			
17	Microsoft Domain Name Server	4	Bağla	Uzak noktaya root verme	5	20	v.8.2.5'den v.9.1.3'e geçilmeli
				Yanlış ayar	5	20	Zone transferi devre dışı bırakmalı
			Pek çok TCP servis için gerekiyor (e-mail, WWW, chat, SMTP)	Eğer server devre dışı kalırsa tüm bu servisler devre dışı kalır	3	12	Uygun DNS server ayarı kullanmalı
18	Telnet Server	2	Kod hatası	Zayıf kimlik kontrolü	3	6	Yazılımı SSH v2 protokolü kullanarak kurmalı
			Güvensiz	Buffer taşması	5	10	Kaldırmalı
				İzinsiz dosya transferi riski	4	8	GUI'ye ulaşmak için terminal services (firewalldan geçmiş) kullanmalı
				Zararlı yazılım indirme riski	4	8	Anti virüs yazılımı kurmalı ve güncel tutmalı
							Bilgi Transfer Planı yapmalı
			Teksti siliyor	Verilere zarar verme	3	6	Şifrelemeli
				Bilgiye izinsiz erişim	3	6	Bilgi Transfer Planı yapmalı
							Uzaktan erişim için SSH destekli bir yazılım kullanmalı
19	LAN Manager	4	Uzaktan erişim	Bilgiye izinsiz erişim	3	12	Bilinen iyi bir çözümü yok
							Uzaktan erişimi devre dışı bırakmalı
			Zayıf şifre ile şifreleme	Şifre kırma	3	12	Syskey kurmalı
Fiziksel Varlıklar							
20	AIX Server	4	Fiziksel olarak ulaşılabilir	Yok etme / parça çalma	2	8	Yedek bir tane almalı
							Sigortalamalı
							Kısıtlı erişim sağlanmalı

							Acil durumda yeni bir tane almak için para ayrılmalı
				Bilgiye yetkisiz ulaşım	4	16	Şifre koruması sağlanmalı
							Kısıtlı erişim sağlanmalı
			Yok edilebilir	Bilgiye ulaşım yok	2	8	Yedeklenmeli
							Kısıtlı erişim sağlanmalı
			Çalınabilir	Bilgiye ulaşım yok	2	8	Şifreleme yapılmalı
				Bilgi sızıntısı	2	8	Kısıtlı erişim sağlanmalı
21	Hard Drive	4	Sınırlı Kapasite	Bilgi için yer yok	3	12	Disk alanını günlük gözden geçirmeli
							Bilgi Transferi Politikası Kurmalı
			Çalınabilir	Bilgi sızıntısı	2	8	Şifreleme yapılmalı
				Bilgiye ulaşım yok	2	8	Kısıtlı Erişim sağlanmalı
			Yok edilebilir	Bilgiye ulaşım yok	2	8	Sık yedekleme yapılmalı
							Kısıtlı Erişim sağlanmalı
22	Ağ Kartı	2	Yok edilebilir	LAN ve Internet bağlantısı yok	2	4	Yedek bir tane almalı
23	Disket Sürücü	1	Yok edilebilir	yedekleme ve geri yükleme imkanının olmaması	3	3	Yedek bir tane almalı
				Veri iletimi imkanının olmaması	3	3	
				Sistem bileşenlerinin yüklenmesini bölebilir	2	3	
			Veri Transferi için kullanılabilir	Bilgi çalmak için kullanılabilir	4	4	Erişim Listesi Kullanmalı
							Bilgi Transferi Politikası Kurmalı
24	CD-Rom Sürücü	1	Yok edilebilir	Yedekleme ve geri yükleme imkanının olmaması	2	2	Yedek bir tane almalı
				Yazılım yüklemek imkansızlaşabilir	2	2	
			Yasal olmayan yazılım yüklemek için kullanılabilir	Lisans anlaşmasının bozulması	4	4	Bilgi Transferi Politikası Kurmalı
							CD'den yüklemeyi yasaklamalı, sadece yöneticiye izin vermeli
25	NT Server	4	Fiziksel olarak erişilebilir	Yok etme / Parça çalma	2	8	Yedek bir tane almalı
							Sigortalamalı
							Kısıtlı Erişim sağlanmalı

							Acil durumda yenisini almak için para ayrılmalı
				Bilgiye Yetkisiz Ulaşım	3	12	Şifre ile korumalı
							Kısıtlı Erişim sağlanmalı
			Yok edilebilir	Bilgiye erişimin kesilmesi	2	8	Sık yedekleme yapmalı
							Kısıtlı Erişim
			Çalınabilir	Bilgiye erişimin kesilmesi	2	8	Şifreleme yapılmalı
				Bilgi Sızıntısı	2	8	Kısıtlı Erişim sağlanmalı
26	Sabit Disk	4	Sınırlı Kapasite	Bilgi için yer yok	3	12	Disk alanını günlük gözden geçirmeli
							Bilgi Transferi Politikası Kurmalı
			Exchange 5.5 aktiviteleri yüzünden dolabilir	Değişimin bekletmesi	4	16	Disk alanını günlük gözden geçirmeli
				Mail kutularına erişimin olmaması	4	16	Yedek bir disk almalı
				Dosyaları Boşaltma imkanının olmaması	4	16	
			Çalınabilir	Bilgi sızıntısı	2	8	Şifreleme yapılmalı
				Bilgiye ulaşım yok	2	8	Kısıtlı Erişim sağlanmalı
			Yok edilebilir	Bilgiye ulaşım yok	2	8	Sık yedekleme yapmalı
							Kısıtlı Erişim sağlanmalı
27	Streamer	3	Yok edilebilir	Bilgiyi yedekleme ve geri yükleme şansı yok	2	6	Yedek bir tane almalı
28	Switch	4	Yok edilebilir	LAN veya internet erişimi yok	3	12	Yedek bir tane almalı
29	Router Cisco 2600	4	Ağ trafiğini düzenler	Bilgilerin bozulması	3	12	Düzgün Router ayarı yapılmalı
			Zor düzgün ayarlar				
			Standart zayıf şifre	Şifre tahmini	3	12	Şifre politikası uygulanmalı
			Yok edilebilir	LAN veya internet erişimi yok	2	8	Yedek bir tane almalı
30	Ağ kabloları	2	Yok edilebilir	LAN veya internet erişimi yok	2	4	Düzgün yerleştirmeli
31	Yazılım kurulum diskleri	3	Fiziksel olarak ulaşılabilir	Kaybetme / yok etme / çalınma	4	12	Erişimi kısıtlanmalı
			Yok edilebilir	Bilgisayar sistem bakımı için gerekebilir	4	12	Yedeklerini almalı
32	Yedekleme diskleri	3	Fiziksel olarak ulaşılabilir	Kaybetme / yok etme / çalınma	4	12	Erişimi kısıtlanmalı
			Yok edilebilir	Bilgi sızıntısı	4	12	Erişimi kısıtlanmalı

							Şifrelenmeli
			Çalınabilir	Bilgisayar sistem bakımı için gerekebilir	4	12	Yedeklerini almalı
Hizmetler							
33	Elektrik	4	Kısa devre	Donanıma zarar verebilir	2	8	Kesintisiz Güç Kaynağı kullanmalı
			Kesinti	Önlem alınmamış bilgisayarların elektriğini kesebilir, sisteme zarar verebilir	3	12	Yedek güç kaynağı
							Kesintisiz Güç Kaynağı kullanmalı
				İş proseslerini bloke edebilir	2	8	İş Devam Programı başlatmalı
			Yangın	Şirketi, tüm varlıkları ve bilgiyi yok edebilir	2	8	Yangın koruma sistemi kurmalı
							Çalışanları yangından koruma programı oluşturmalı ve eğitim vermeli
							Yedekler almalı
							Yedekleri düzün saklamalı
				Donanımı yok edebilir	2	8	Yangın koruma sistemi kurmalı
				Yazılımı yok edebilir	2	8	Yedekleri düzün saklamalı
				İş proseslerini bloke edebilir	2	8	Yedek güç kaynağı kullanmalı
34	Su	1	Sel	Donanımı yok edebilir	2	2	Donanımı ve kabloları yerden yükseğe yerleştirmeli
				Yazılımı yok edebilir	2	2	Kurulum disklerini düzgün yerleştirmeli
				Yedekleri yok edebilir	2	2	Yedekleri düzgün yerleştirmeli
				İş proseslerini bloke edebilir	2	2	İş Devam Programı başlatmalı
35	Klima	1	Donanımın havalandırılması	Donanıma zarar verebilir	2	2	Bilgisayar odalarının iklimlendirilmesine dikkat etmeli
				Yangına neden olabilir	2	2	Düzgün kurulum yapmalı

3.1.6. Uygulamanın Denetimi ve Kontrol Listeleri

Güvenlik denetimi, bir kurumun güvenlik altyapısının, güvenlik politikasının, prosedürlerinin ve personelinin ayrıntılı bir biçimde ele alınması, zayıf yönlerin tespiti ve bu zayıflıkların giderilmesi için öneriler sunulması anlamı taşımaktadır. Bu nedenle başarılı bir denetim, tüm ilgili tarafların işbirliği ile

gerçekleştirilebilir. Genelde güvenlikle ilgili bir denetim söz konusu olduğunda, birçok insan olumsuz bir önyargıya kapılır ve rahatsız olur. Bununla birlikte, güvenlik denetimi kurum içinde güvenlik politikasına uygun çalışılıp çalışılmadığının tespitinde kullanılabilecek tek yoldur.

Bilgi Güvenliği Politikası ve Prosedürleri'ndeki hata ve eksiklikler gerekirse birçok kullanıcı grubu ile yüz yüze görüşmeler yapılarak, bilgi güvenliği politikasının ne kadar gerçek yaşama yansıdığını değerlendirmek amacı ile aşağıda Tablo 15'te verilen denetimler belirtilen aralıklarda ve kişilerin sorumluluğunda yapılmakta, sonuçları raporlanmaktadır.

Denetimleri iki tip kapsamında değerlendirebiliriz. Biri kurumun kendi personeli tarafından gerçekleştirilen "İç Denetim", diğeri ise kurum dışı, bağımsız bir kuruluş tarafından gerçekleştirilen "Dış Denetim"dir.

Tablo 15. Uygulama Denetim Tablosu

Denetimler	Sıklık	Sorumlu Kişi	Rapor Verilecek Kişi
Tüm Sistem	Yılda 2 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Politikayı Gözden Geçirmek	Yılda 2 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Prosedür Doğruluk Denetimi	Yılda 2 Kere	Proje Yöneticisi	Bilgi Güvenlik Yöneticisi, MGEO Başkanı
Prosedür Eğitimi	Yılda 2 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Prosedür Denetimi	3 Ayda 1 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Risk Analiz Metotları	Yılda 2 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Yeni Varlıklar	Haftada 1 Kere	Proje Yöneticisi	Bilgi Güvenlik Yöneticisi
Üçüncü Partiler	Ayda 1 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Tüm Sistemin Yedeklenmesi	Ayda 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Sürekli Sistem Yedeklenmesi	Haftada 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Yeni Anti virüs	Ayda 2 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Sistem Yamaları	Ayda 2 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Diskteki Boş Alan Miktarı	Günde 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Kritik Süreklilik Planı	3 Ayda 1 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı

Ağ Testi	3 Ayda 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Sızma Testi	3 Ayda 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Sistem Yükseltmesi	Yılda 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Yükleme Disklerinin, Lisansların, Sistem Dokümantasyonunun, Yedeklerin Depolanması	Ayda 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
Sistemi Gruplamak	3 Ayda 1 Kere	Proje Yöneticisi	Sistem Yöneticisi
Şifre Değişimi	3 Ayda 1 Kere	Sistem Yöneticisi	Bilgi Güvenlik Yöneticisi
E-imza anahtar değişimi	Yılda 2 Kere	Sistem Yöneticisi	MGEO Başkanı
Erişim Listesi	Günde 1 Kere	Sistem Yöneticisi	Proje Yöneticisi
Kişisel Dosya	Haftada 1 Kere	Proje Yöneticisi	İnsan Kaynakları Yöneticisi
Yangın Koruma Sistemi	Yılda 2 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Diğer Acil Durum Prosedürleri	Yılda 2 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı
Kaza Prosedürleri	3 Ayda 1 Kere	Bilgi Güvenlik Yöneticisi	MGEO Başkanı

Denetimlerde kullanılacak kontrol listeleri, TS ISO 27001 standardının Ek-A'sında uygun olanların belirlenip, uygulamaya konulması ile sağlanmaktadır. Söz konusu ekte, işletmeler için yaygın şekilde uygun olduğu düşünülen kapsamlı bir kontrol amaçları ve kontroller listesi içerir. Bu standardın kullanıcıları, hiçbir önemli kontrol seçeneğinin gözden kaçmamasını sağlamak amacıyla kontrol seçimi için bir başlangıç noktası olarak Ek-A'yı incelemelidirler. Eğer kapsam yeterli gelmiyorsa kapsamı genişletilebilir. 11 temel konu başlığında altında toplam 39 adet kontrol amacı içeren liste Tablo 16'da sunulmuştur.

Tablo 16. Kontrol Temel Başlıkları ve Amaçları

Kontrol Başlığı	**Kontrol Amacı**
A.5 Güvenlik politikası	
	A.5.1 Bilgi güvenliği politikası
A.6 Bilgi güvenliği organizasyonu	
	A.6.1 İç organizasyon
	A.6.2 Dış taraflar
A.7 Varlık yönetimi	
	A.7.1 Varlıkların sorumluluğu
	A.7.2 Bilgi sınıflandırması
A.8 İnsan kaynakları güvenliği	
	A.8.1 İstihdam öncesi
	A.8.2 Çalışma esnasında
	A.8.3 İstihdamın sonlandırılması veya değiştirilmesi
A.9 Fiziksel ve çevresel güvenlik	
	A.9.1 Güvenli alanlar
	A.9.2 Teçhizat güvenliği
A.10 Haberleşme ve işletim yönetimi	
	A.10.1 Operasyonel prosedürler ve sorumluluklar
	A.10.2 Üçüncü taraf hizmet sağlama yönetimi
	A.10.3 Sistem planlama ve kabul
	A.10.4 Kötü niyetli ve mobil koda karşı koruma
	A.10.5 Yedekleme
	A.10.6 Ağ güvenliği yönetimi
	A.10.7 Ortam işleme
	A.10.8 Bilgi değişimi
	A.10.9 Elektronik ticaret hizmetleri
	A.10.10 İzleme
A.11 Erişim kontrolü	
	A.11.1 Erişim kontrolü için iş gereksinimi
	A.11.2 Kullanıcı erişim yönetimi
	A.11.3 Kullanıcı sorumlulukları
	A.11.4 Ağ erişim kontrolü
	A.11.5 İşletim sistemi erişim kontrolü
	A.11.6 Uygulama ve bilgi erişim kontrolü

	A.11.7 Mobil bilgi işleme ve uzaktan çalışma
A.12 Bilgi sistemleri edinim, geliştirme ve bakımı	
	A.12.1 Bilgi sistemlerinin güvenlik gereksinimleri
	A.12.2 Uygulamalarda doğru işleme
	A.12.3 Şifreleme kontrolleri
	A.12.4 Sistem dosyalarının güvenliği
	A.12.5 Geliştirme ve destekleme proseslerinde güvenlik
	A.12.6 Teknik açıklık yönetimi
A.13 Bilgi güvenliği ihlal olayı yönetimi	
	A.13.1 Bilgi güvenliği olayları ve zayıflıklarının rapor edilmesi
	A.13.2 Bilgi güvenliği ihlal olayları ve iyileştirmelerin yönetilmesi
A.14 İş sürekliliği yönetimi	
	A.14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları
A.15 Uyum	
	A.15.1 Yasal gereksinimlerle uyum
	A.15.2 Güvenlik politikaları,standartlarla teknik uyum
	A.15.3 Bilgi sistemleri denetim hususları

3.1.7. Gözden Geçirme ve İyileştirme

ASELSAN BGYS'sini 6 ayda bir aralıklarda, sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için MGEO başkanı, bilgi güvenlik yöneticisi ve proje yöneticisi tarafından gözden geçirilmektedir. Bu gözden geçirme, güvenlik politikası ve güvenlik amaçları dahil BGYS'nin iyileştirilmesi ve gereken değişikliklerin yapılması için fırsatların değerlendirilmesini içermektedir. Gözden geçirme sonuçlarına göre gerekirse risk değerlendirme, prosedür değişikliği, kaynak ihtiyacı ve kontrol ihtiyaçları gözden geçirilerek, dokümante edilmekte ve kayıt altına alınmaktadır. BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici eylemlerin gerçekleştirilmesini bilgi güvenlik yöneticisi tarafından sağlanmaktadır.

3.2. Teknik Faaliyetler

Bu bölümde ASELSAN'da proje kapsamında alınan teknik güvenlik önlemleri anlatılmıştır. İlk olarak genel güvenlik yapıtaşları açıklanmış daha sonra yazılım uygulaması yardımıyla oluşturulan güvenlik yapısı açıklanmıştır. Kullanılan güvenlik önlemleri;

-Fiziksel Güvenlik,

-Güvenlik Duvarı,

-Kullanıcı Tabanlı Oturum İçerik Kontrolü,

-Oturum İçerik Kontrolü,

-Saldırı Tespit Sistemi,

-Virüs Koruma Sistemi,

-Ağ Güvenliği, başlıkları altında toplanmış ve konuların detaylarına ilişkin bilgiler aşağıda sunulmuştur.

3.2.1. Fiziksel Güvenlik

Fiziksel güvenlik, ASELSAN kaynaklarını ve değerli bilgilerini tehdit eden açıklarını kapatmakta kullanılan en önemli yöntemlerden biridir. Fiziksel güvenliğin ilk adımı olarak çalışma alanlarının fiziksel güvenlik gereksinimleri belirlenmiştir. Bunlar temel olarak; şirket binası, kısıtlı bölgeler, çalışma alanları ve ziyaretçi alanları olarak üçe ayrılabilir. Risk analizi ile hangi bölgenin ne derecede güvenlik gereksinimine ihtiyaç duyduğu belirlenerek, bu bölgelere girişte nasıl bir yöntem izleneceğine karar verilmiştir. ASELSAN tesislerine girişte akıllı kart adı verilen giriş kartları kullanılmaktadır.

Diğer önemli bir konu ise şirkete gelen ziyaretçilerin şirket içindeki hangi bölgelere girilebileceği ve yanlarında eşlik edecek kişinin özellikleri belirlenmiştir. Ayrıca ziyaretçi giriş çıkışlarının düzenli olarak kaydının tutulması çok önemlidir. Bu konuda ziyaretçilere verilecek ve adlarına kayıt yapılacak kartlar kullanılacaktır.

Bina güvenliğinde güvenlik görevlilerinin de önemli bir yeri vardır. Girişlerde bulunan görevliler giriş çıkışların düzenli olmasını ve takibinin yapılmasını sağlamaktadırlar. Fakat burada önemli bir konu görevlilerin şirketin politikası doğrultusunda eğitilmeleri sağlanmış ve hangi konularda hassasiyetle hareket

edecekleri belirlenmiştir. Ayrıca kullanılacak güvenlik kameraları ile bina güvenliğini daha etkin kılınmıştır.

Sistem güvenliğinin en önemli adımlarından biri hiç şüphesiz sistem odanızı güvenli hale getirilmesidir. Bu odadaki sistemlerin mümkün olduğunca fiziksel olarak ayrı tutulabilecek kilitli kabinelerde veya bölümlerde bulundurulmaktadır. Bu sayede sistem odasını kullanma hakkı olan tüm kişilerin, o odada bulunan bütün sistemlere de fiziksel olarak erişme hakkına sahip olması engellenmiştir.

ASELSAN'da bilgi sistemlerinin güvenliği için çok ciddi seviyede yatırımlar yapılmıştır. Fakat ne yazık ki unutulan bazı küçük detaylar ileride büyük sorunlara neden olabilecektir. Bu duruma en güzel örnek ise sistemlerin yedeklenmesidir.

Alınan fiziksel önlemler, toplam sekiz başlık altında aşağıdaki ana faaliyetlerden oluşmaktadır. Bunlar;

-Tesisin yeri ve yapısı,

-Fiziksel erişim,

-Elektrik ve klima sistemleri,

-Su etkisi,

-Yangın önleme ve yangına karşı koyma,

-Araçların saklanması,

-Atık atma,

-Tesis dışı yedekleme, başlıklarıdır.

3.2.1.1. Tesisin Yeri ve Yapısı

ASELSAN, Ankara'nın Akyurt tesislerinde, güvenlik şartları sağlanan tüm bilgi güvenliğine yönelik saldırıları durduracak, önleyecek ve tespit edecek şekilde tasarlanmış, fiziksel olarak korunan ortam içinde faaliyetlerini yürütür.

3.2.1.2. Fiziksel Erişim

ASELSAN sistemleri, 4 fiziksel güvenlik seviyesiyle korunur ve daha yüksek bir seviyeye erişim yapılmadan önce alçak seviyelere erişilmelidir. Her bir seviyenin özellikleri ve şartları aşağıdaki Tablo 17'de verilmiştir.

Tablo 17. Fiziksel Güvenlik Seviyeleri

Seviye	Tarif	Erişim Kontrol Mekanizması
Fiziksel Güvenlik Seviyesi 1	Fiziksel Güvenlik Seviyesi 1, tesis için en diş fiziksel güvenlik duvarına karşılık gelir.	Bu seviyeye erişmek için bir personel giriş kartı kullanılması gerekir. Bu seviyeye fiziksel erişim otomatik olarak kayıtlara geçirilir ve videoya kaydedilir.
Fiziksel Güvenlik Seviyesi 2	Seviye 2, dinlenme odaları ve ortak koridorlar da dahil ortak alanları içerir.	Seviye 2, personel giriş kartı kullanılarak herkes için tesisin ortak alanlarına bireysel erişim kontrolü sağlar. Seviye 2'ye fiziksel erişim otomatik olarak kayıtlara geçirilir.
Fiziksel Güvenlik Seviyesi 3	Seviye 3, gizli operasyonunun yapıldığı ilk seviyedir. Gizli operasyonu, kimlik kontrolü, doğrulama ve düzenleme gibi sertifikalandırma prosesi periyoduyla ilgili herhangi bir faaliyettir.	Seviye 3, iki faktörlü kimlik kontrolü kullanımıyla bireysel erişim kontrolü sağlar. Güvenilir olmayan personelin veya ziyaretçilerin refakatçisiz olarak, Seviye 3 güvenli alana girmesine izin verilmez. Seviye 3'e fiziksel erişim otomatik olarak kayıtlara geçirilir.
Fiziksel Güvenlik Seviyesi 4	Seviye 4, özellikle gizli operasyonlarının yapıldığı seviyedir. İki ayrı Seviye 4 alanı vardır: çevrim içi Seviye 4 veri merkezi ve çevrim dışı Seviye 4 kod yaratma prosedürü odası.	Seviye 4 veri merkezi bireysel erişim kontrolünü, kod yaratma prosedürü odası da ikili kontrolü sağlar; bu işlevlerin her biri, iki faktörlü kimlik kontrolü kullanılarak yerine getirilir. Refakatçisiz Seviye 4 erişimi için onaylanmış bireyler Güvenilen Personel Politikasını karşılamalıdır. Seviye 4'e fiziksel erişim otomatik olarak kayıtlara geçirilir.

3.2.1.3. Elektrik ve Klima Sistemleri

ASELSAN'ın güvenli tesisleri, elektrik gücüne sürekli ve kesintisiz erişim sağlamak için elektrik sistemleri ve sıcaklığı ve nispi nemi kontrol etmek için ısıtma/havalandırma/klima sistemleri ana ve yedek sistemlerle donatılmıştır.

3.2.1.4. Su Etkisi

ASELSAN, suyun sistemlerine etkisini en aza indirecek önlemler almıştır.

3.2.1.5. Yangın Önleme ve Yangına Karşı Koyma

ASELSAN, yangınları veya hasara yol açan diğer alev veya duman vakalarını önlemek ve söndürmek için makul önlemleri almıştır. Yangın önleme ve korunma önlemleri mahalli yangın emniyet yönetmeliklerine uygun şekilde tasarlanmıştır.

3.2.1.6. Araçların Saklanması

Üretim yazılım ve verileri ile denetim, arşiv veya yedekleme bilgilerini içeren bütün araçlar ASELSAN tesislerinde veya erişimi yetkili kişilerle sınırlandıracak ve araçları kazayla hasara (örneğin, su, yangın ve elektromanyetik) karşı koruyacak şekilde tasarlanmış, uygun fiziksel ve mantıklı erişim kontrollerine sahip güvenli tesis dışı depolama tesislerinde muhafaza edilmektedir.

3.2.1.7. Atık Atma

Gizli dokümanlar ve malzemeler atılmadan önce kıyılır. Gizli bilgileri toplamak veya iletmek için kullanılan araçlar atılmadan önce okunamaz hale getirilir. Şifreleme cihazları atılmadan önce fiziksel olarak imha edilir veya imalatçının talimatlarına göre sıfırlanır. Diğer atıklar ASELSAN'ın normal atık atma şartlarına göre atılmaktadır.

3.2.1.8. Tesis Dışı Yedekleme

ASELSAN, kritik sistem verilerini, denetim kaydı verilerini ve diğer gizli bilgileri rutin olarak yedeklenmektedir.

3.2.2. Güvenlik Duvarı

Değişik noktalara konulmuş iki farklı güvenlik duvarı ile ASELSAN'ın proje kapsamındaki sınır koruma ihtiyaçları sağlanmaktadır. Bu güvenlik duvarlarından biri ağın Internete çıkış noktasında, ikincisi de veri bölgesinin girişine konumlandırılmıştır. Güvenlik duvarları, kendi aralarında kümelenmiştir ve yük paylaşımlı olarak çalışmaktadır. Kullanılan band genişliği, isteğe bağlı olarak ihtiyacı

olan uygulamaya öncelikli olarak tahsis edilmektedir. Internet üzerinden kullanıcıların dışarıya yaptıkları bağlantılar değişik parametrelere bağlı olarak sürekli izlenmektedir.

Proje kapsamında, Paket Süzmeli Güvenlik Duvarı yöntemi uygulanmaktadır. Bu yöntem yönlendirici vasıtasıyla paketlerin başlık alanlarının kontrolü ve bu kontrol sonucunun oluşturulmuş kurallar tablosuna göre yönlendirilmesi olayıdır. OSI modellemesinde 3.katmanda çalışan paket süzmeli güvenlik duvarı; alıcı ve gönderici IP adresleri, taraflarda ki port numaraları, paket türleri (UDP, TCP …) ve hizmet protokolleri (Telnet, HTTP, FTP, SMTP, IP tunnel gibi) bilgilerine bakarak gerekli yönlendirmeleri yapar.

Kurum ağını dışarıdan gelen saldırılara karşı güvenli hale getirmek için iyi tasarlanmış bir çevre ağının varlığı önemli bir etmendir. Böyle bir ağ aynı zamanda iç ağın diğer ağlara karşı saldırılarda kullanılmasını önlemeye de yarar. Çevre ağda DMZ (Demilitarized Zone) yapısı kullanılarak iç ağ ve Internet arasında korumalı bir dolaylı erişim mimarisi kullanılmaktadır. Bu yapıda ilk önemli karar DMZ içine hangi sunucuların konacağıdır. Genel bir yaklaşım, kurum dışından erişilebilen tüm hizmetleri DMZ içine koymaktır. DMZ erişimi de bir veya daha fazla güvenlik duvarı kullanılarak güvenilir hale getirilmiştir.

3.2.3. Kullanıcı Tabanlı Oturum İçerik Kontrol Sistemi

ASELSAN bünyesindeki tüm kullanıcıların kurumsal e-posta adresi mevcuttur. Bu yazılımla, e-posta sisteminden gelebilecek virüslü e-posta, istenmeyen (spam) e-posta, zincir e-posta gibi saldırılara karşı koruma sağlamaktadır. Ayrıca şüpheli görünen e-postalar, operatör tarafından gözden geçirilmek üzere göz altına alınmaktadır.

3.2.4. Oturum İçerik Kontrol Sistemi

Ağ sayfalarına erişimlerde, erişilen sayfaları sınıflandırır ve belirlenmiş sınıflardaki sayfalara erişime izin verilir. Bu şekilde, kötü amaçlı kod barındırabilecek sayfalara ve band genişliğinin etkin kullanımını engelleyecek program indirmelerin önüne geçilmiş olur. Bu yazılımla ayrıca, kullanıcıların uçtan uca dosya paylaşımı ağlarına (Örneğin Kazaa, E-Donkey, i-Mesh gibi) ve anında mesajlaşma sistemlerine (MSN, ICQ,Yahoo Messenger gibi) erişimleri engellenir.

3.2.5. Saldırı Tespit Sistemi

Sistemde, ağ tabanlı saldırı tespit yazılımları kullanılmaktadır. Bu yazılımlar sayesinde içeriden ve dışarıdan gelebilecek ve güvenlik duvarı tarafından tespit edilemeyecek saldırılara karşı korunma sağlanmış olur. Saldırı Tespit Sistemi, atak nereden gelirse gelsin önlemini almak üzere üretilmiş bir çözüm olarak, şirket içinden herhangi birisi ya da dışarıdan bir kişi veya kuruluş sisteme girdiği anda bu durumu fark etmekte ve kişinin nereden geldiği ve nereye bağlandığı sorularına ilişkin raporlamalar yapmaktadır. Ayrıca belirlenen kurallar çerçevesinde gelen saldırıları tespit ederek kısa mesaj servisi (SMS), e-posta, sistem kaydı ve veritabanı gibi uyarı ve kayıt çıktıları sağlamakta ve gerekirse Güvenlik Duvarı'na saldırı olduğuna dair uyarı sinyalleri yollayabilmektedir.

3.2.6. Virüs Koruma Sistemi

ASELSAN ağına bağlı olan tüm kullanıcı ve hizmet bilgisayarlarında virüs koruma yazılımı kuruludur. Tüm bilgisayarlarda, kullanıcı müdahalesine gerek olmaksızın günde birkaç kez virüs imzaları güncellenmektedir. Virüs koruma sunucusu yedeklenmiştir.

3.2.7. Ağ Güvenliği

ASELSAN bütün işlevlerini, yetkisiz erişimlere ve diğer kötü niyetli faaliyetlere karşı korumak amacı ile güvenliği sağlanmış ağlar kullanarak yerine getirir. Tüm gizli bilgilerin iletimini şifreleme ve dijital imzalar kullanarak korur. Ağ güvenliğinde kullanılan yöntemleri;

-Güvenlik duvarı,

-Saldırı tespit sistemi,

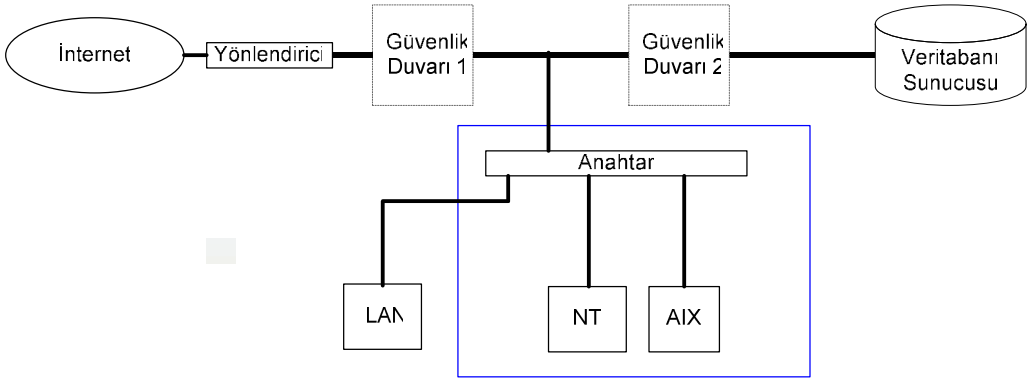
-Rol tabanlı erişim sistemi,

kullanılmaktadır.

Rol Tabanlı Erişim Sistemi, bilgi ve iletişim sistemlerine erişim haklarının yönetilmesi için geliştirilen bir güvenlik sistemidir. Bu güvenlik sistemi, çok büyük ağ uygulamaları için daha düşük maliyette ve daha az karmaşık güvenlik yönetimi oluşturmaktadır. Rol Tabanlı Erişim Sistemi, kullanıcıların rollerini ve yetkilerini

tanımlayarak güvenlik yönetimini kolaylaştırır. Burada rol, kullanıcıların gruplanması anlamında kullanılmaktadır.

Güvenlik açısından bakıldığında, ağ uygulamasının çalışması Şekil 38'de gösterildiği gibi olmaktadır. Buna göre; Internet üzerinden gelen istekler 1. Güvenlik Duvarı'ndan, SSL tabanlı olarak geçer. Kullanıcının tek muhatabı AIX uygulama sunumcusuna gelir. Sunumcu veritabanı işlemlerini, XML biçiminden SQL biçimine çevirerek, 2. Güvenlik Duvarı'ndan üzerinden veri tabanına gönderir.



Şekil 38. Ağ Uygulaması

4. ASELSAN A.Ş.'DE BGYS SÜRECİNİN DEĞERLENDİRİLMESİ

Söz konusu proje kapsamında üretilen bilgi kaynaklarının güvenliğinin sağlanmasında ve mevcut bilgisayar sistemi ile beraber sağlıklı bir Bilgi Güvenlik Sistemi yapılandırılmasında temel oluşturulmuştur. Proje öncesi bu sistem ile ilgili fikirlerin şirketin günlük aktiviteleri içinde olsa da, bir sistem olarak yapılandırılmamış olduğu anlaşılmaktadır. Tez, bilgi güvenliği politikası, bilgi güvenlik prosesleri ve risk analizi oluşturulmasına katkıda bulunmuştur. Bu uygulamadan sonra gerek yurt içi gerek ise yurtdışı şirketlerin yaptıkları şekilde ISO 27001 sertifikası için gerekli hazırlıklar gözden geçirilip, sertifikasyona yönelik başvuru yapılmalıdır.

Bu tez sonucunda, BGYS uygulama nedeni, risk yönetiminin şirketlere nasıl uygulanabileceği, BGYS'nin nelerden oluştuğu ve ISO 27001 standardının BGYS olarak seçilme nedenine yönelik dört temel araştırma sorularına cevaplar verilebilmiştir. Söz konusu soruların nasıl yanıtlandığı aşağıda sunulmuştur;

BGYS uygulama nedenleri: Son yıllarda bilginin değerinin giderek arttığını izlemekteyiz. Pek çok kişi, yasal olmayan amaçlarda kullanmak üzere, belirli bir bilgi için çok para ödemeye hazırdırlar. Bu fiyat artışı giderek daha çok kişinin bilgilerini satmak istemesine yol açmaktadır. Şirket planları, şirketin mali potansiyel analizi veya yeni geliştirilen bir ürünün mevcut durumu gibi bilgiler piyasada bulunan rakipler için çok değerli olabilir ve şirketin mevcudiyeti açısından çok önemlidir. Her organizasyon bazı stratejik verilere sahiptir ve hepsi bu verileri korumak istemektedir.

Risk yönetimi ve şirketlerde uygulanması: Risk sürekli olarak iş hayatını etkilemiştir ve etkileyecektir. Bu sebeple risk yönetimi için özel yollar bulunmuştur. Tezin ikinci bölümünde risk yönetimi prosesinin bazı kilit öğeleri tanımlanmıştır. Bunlar varlıkların tanımlanması, tehdit analizi, etki tanımları ve korumaları seçimidir. Risk yönetimi tanımlamayı yapar ve etkinliklerini kontrol etmek için yapılması gerekenleri tavsiye eder. Hatırlanması gereken en önemli nokta risk yönetimi prosesinin devamlılığıdır. Diğer bir deyişle, tüm örgütsel ortamın geliştiği ve sistemin güncel tutulması gerektiği hatırlanmalıdır. Risk yönetimi ISO 27001 bazlı sistemin motorudur ve tüm sistem için büyük değere sahiptir.

BGYS nelerden oluşur: BGYS'nin yapılması gereken bazı özellikleri mevcuttur. Bölüm üçte bu konu ile ilgili gerekli teorik bilgi altyapısı bulunmaktadır. Yazılı metinlerde bu konu ile ilgili verilen yaklaşımlarda risk analizi tabanlı sistem olması dikkat çekmektedir. Şirket, bu amaçla başlangıçta bir politika belirlemeli, şirket varlıkları tanımlamalı, güvenlik ile ilgili personelin eğitimi tamamlanarak, risk analizi prosesini tüm bilgi varlıklarına uygulamalı, değerlendirme sonuçlarına göre yönetmeli ve sistem belirli aralıklarla gözden geçirilmelidir.

ISO 27001 standardının BGYS olarak seçilme nedeni: Belirtilmesi gereken en önemli nokta, şirketlerin BGYS kurmak zorunda olduklarıdır. ISO 27001 standardı, güvenlik saldırılarını uygun noktada tutmak için gerekli yönetimsel faaliyetleri içermesi, daha etkili teknik koruma sağlaması ve uluslararası geçerliliğinin olmasından dolayı seçilmiştir. Bölüm üçte bu tür bir sistemin ana fikirleri ve bölüm dörtte nasıl yapılması ile ilgili bilgiler yer almaktadır. Tüm proses eğer eksiksiz bir şekilde uygulanır ve yönetilirse, genel bir risk azalmasına ve şirketi geleceğe hazırlamaya yardımcı olur. ISO 27001 uluslararası bir standarttır ve geniş kesimlerce tanınır ve saygı görür. Bu tanınma pratikte şirket daha önceden bilgi güvenlik sistemine sahip

şirketlerle tanışma aşamasında kullanılabilir. BS 7799 (ISO 27001'ın çıktığı kaynak) kullanıcılarından oluşan uzun liste bu standardın değeri hakkında bilgi verebilir. BS 7799 kaynaklı pek çok forumlar ve kullanıcıların toplandığı kulüpler kurulmuştur.

Oluşturulan BGYS yapısal olarak çok esnektir ve güncellemeler mümkün olduğu kadar basit yapılabilmektedir. Blok yapısından dolayı yeni elemanlar eklemek, varolanları yenilemek veya kaldırmak çok kolaydır. Analiz sonuçları göstermiştir ki, ASELSAN özel olarak iki konuya önem vermeli, tüm yazılımları, eski güvenlik açıklarından zarar görmemek için güncel tutmalı ve sisteme şifreli erişim uygulamalıdır. Önerilen güvenlik yöntemleri uygulandıktan sonra bir kez daha etkinlikleri için risk analizine tabii tutmalıdır. Yüksek riskin azaltılması, bir sistemin başarılı olduğu anlamına gelecektir.

ASELSAN en basit risk analiz yöntemini, varlık değeri ve tehdit oranı ile nitel bir ölçek kullanarak, benimsemiştir. Kurulmuş olan risk analiz prosedürü pek yakında gelişecektir. Analize yeni elemanlar ekleyerek örneğin korumaların bedeli ve potansiyel kayıplar gibi değerlerin karşılaştırılacağı şekle gelecektir. Şu anda tamamlanan prosedür sistemin en önemli parçalarına dikkat çekmeli ve ASELSAN'a sistemi güncel tutmasına yönelik deneyim fırsatı verilmelidir.

Sistemin bazı elemanları şimdiden çalışmaya başlamıştır. Şifre politikası, bilgi güvenlik politikası ve gizlilik antlaşması gibi dokümanlar günlük işin parçası olmuşlardır. Resmi bir ASELSAN bilgi güvenlik politikasının oluşturulması tüm güvenlik özelliklerinin tamamen kontrolünü, gizlilik anlaşması tüm çalışanlardan ve üçüncü parti iş ortaklarından bilgi güvenliğinin sağlanmasını yasal olarak isteme hakkını verir. Ancak, bu sistemin getirdiği avantajları hesaplamak güçtür. Burada problem firmanın bu sistem sayesinde ne kadar kontrat kazandığının, ASELSAN imajının ne kadar kazandığının ve eğer bu sistem olmasaydı firmanın kaybedeceklerinin tanımlanmasıdır. Bu son konu her Bilgi Güvenlik Sisteminin problemidir. Bunun nedeni istenmeyen olayların gerçekleşmesi riskidir. Bu olaylar oluşabilir de, oluşmayabilir de ve bu nedenle hiçbir sistem gerçek değeri veremez. Sadece belirli tarihsel verilere göre ve özel olarak uygulanan kontrollere göre tahminler yapılabilir fakat gerçek değer asla bilinemez. ISO 27001 bazlı sistem ASELSAN organizasyonuna BGYS bakış açısından bakmayı öğretir. Gelecek sistemin ne kadar başarılı olduğunu gösterecektir.

SONUÇ

Bugün en büyük güçlerden birisinin bilgi olduğu gerçeği kabul edilmiş ve dünya bu gerçek ışığında yapılanmaya ve hatta içinde yaşadığımız çağa bilgi çağı denmeye başlanmıştır. Üstün teknolojinin sağladığı inanılmaz kolaylıklara sınırları ortadan kalkan ve biri birine yaklaşan devletler, kuruluşlar ve kişilerin yarattığı küresel dünya ile birlikte bilginin önemi daha da artmıştır.

Hali hazırda, teknolojik alandaki gelişmelere paralel olarak iletişim ve bilgisayar ortamlarındaki baş döndürücü ilerlemeler çok miktarda bilginin üretilmesine, depolanmasına, süratle iletilmesine ve kullanımına imkan sağlamaktadır. Bu ise toplumun her kesimine bilginin etkin kullanımı açısından büyük faydalar sağlamakta ve bu kesimlerin her seviyesinde büyük çapta bilgi alış verişi olabilmektedir. Bugün, buna gösterilebilecek en güzel örnek 'INTERNET' tir. INTERNET haricinde de bir tuşa basılarak süratle telefon, faks irtibatları yapılabilmekte, video konferanslarla dünyanın çeşitli yerlerini bir araya getirebilmekte ve hatta süren bir savaş gerçek zamanlı olarak tüm dünyaya görüntülü olarak aktarılabilmektedir. Bugün gelinen seviyenin çok ileri bir seviye olması, bunun yakın bir gelecekte daha da gelişmiş bir seviyeye ulaşacağının delilidir. Teknoloji geliştikçe, bilgi çoğalmakta, paylaşımı artmakta ve bunun neticesi olarak da teknoloji de süratle gelişmektedir. Bu iki olgu, birbirinden ayrılmaz bir bütünün parçalarıdır. Daha fazla bilgiye sahip olanlar daha fazla güce sahip olacaklar ve istedikleri zaman ve yerde sahip oldukları bu bilgiyi kullanarak arzu ettikleri etkiyi yaratabilecek ve olaylara yön vererek geleceği kontrol altına alabilecektir. İşte bu imkan ve kabiliyet önüne geçilemez bir cazibe yaratmakta ve bilgiye sahip olma olgusunu ön plana çıkarmaktadır. Ne kadar çok bilgiye sahip olursak, o kadar çok bu bilgiyi elde etmeye çalışanlar olacaktır. Soğuk savaş bitmiş olmasına rağmen, bilginin elde edilmesi ve buna karşı yoğun bir savaş sürdürülmektedir. Bu savaşta düşmanın ve dostun kim olduğu belli değildir. Her an hiç beklemediğimiz biri tarafından saldırıya uğrayabilir ve bilgi kaybedebiliriz. Kaybettiğimiz bu bilgi karşı tarafça kazanılmış olabilir. En önemlisi de, tehdidin hangi bilgiyi ve ne kadarını elde ettiğini bilememizdir. Bir anda merkez bankası çökmüş, borsa dibe vurmuş ve ekonomi bir kaosa sürüklenmiş, bu da yetmemiş gibi metro durmuş, uçaklar kalkamamış, büyük çapta haberleşme sisteminiz felç olmuş olabilir. Öyleyse savaş söz konusudur. Bu savaşta, her savaşta olduğu gibi tehdit, silah ve kurallar mevcuttur. Teknolojideki gelişmelere

paralel olarak bu savaşta taraflar yöntemler geliştirmiş ve geliştirmeye devam etmektedirler. Saldırı konusunda, saldırıyı yapanlar her ne kadar teknolojinin kendilerine sağladığı imkânları azamî şekilde kullanıyor iseler de, savunan taraf da aynı teknolojik imkânlardan faydalanmak şansına sahip olup, bu olgu bilgi güvenliği olarak adlandırılmaktadır.

Bilgi güvenliği bilginin kendisi kadar eskidir. Bilgini insan varlığı ile aynı anda olduğu düşüncesi ile bilgi güvenliğinin de insan tarihi ile aynı anda başladığı söylenilebilir. İnsanlar ne zaman bilgiyi kaydetmeleri depolamaları ve aktarmaları ile ilgili yeni metotlar geliştirseler, bu yenilikler kaçınılmaz olarak yeni teknoloji yöntemlerini beraberinde getirirler ve işleme tâbi bilgiyi korurlar. Bilgiyi korumak için insanlık tarafından çeşitli yöntemler uygulanmış, geliştirilmiş ve daha da geliştirilmektedir. Parola sormak ve bir metnin ezberlenmesi , basit kurallar içersinde şifrelenmesi ya da bölümlere ayrılarak birkaç kişiye dağıtılması ve bir araya getirilmeden bir anlam ifade etmemesi , ayrıca önemli konuların konuşulduğu yerlere su sesi tesis ederek konuşulanların anlaşılmamasının sağlanması gibi . Bu örnekler çoğaltılabilir. Tabii olarak , günümüzde de teknolojinin verdiği olanaklar en yüksek noktada kullanılarak bilgi güvenliği sağlanmaya çalışılmaktadır.

Bilgi teknolojisine giderek artan bağımlılığın sonucu olarak devlet yönetimi, ekonomik ve toplumsal hayatın her yönün ortak bileşeni olan bilgi alt yapısını kötü niyetlilere, terörist faaliyetlere ve doğal afetlere karşı güvenliğinin sağlanması önem kazanmıştır. Bu konuda gelişmiş ülkeler kendi yapılarına uygun farklı önlemler almak mecburiyetinde kalmışlar ve bu konu ile ilgili teşkilatlarını kurmuşlardır. Bu konuda atılacak en önemli adımlardan birisi, ulusal politika ile her türlü tehdit ve hassasiyete karşı misyon ve görevleri farklı kamu ve özel sektörün kendi işlemlerinde ve karşılıklı ilişkilerinde bilgi güvenliğini tam olarak sağlayacak müşterek ilke ve önceliklerin belirlenmesidir. Devlet kuruluşları, hem gizlilik dereceli ve hem de üretim istatiskleri, para basımı bilgileri gibi gizlilik derecesi olmayan hassas bilgileri koruma altına almak zorundadırlar. Bu bilgileri hassas bilgi durumuna getiren gerçek, onların çalınması ve değiştirilmesi halinde ülke ekonomisinin bir kaosa sürüklenebileceğidir. Bu gibi durumlarda, sadece devlet kuruluşunun değil özel sektörün de gizliliğe ihtiyacı vardır. Banka fon transferleri, uçak rezervasyonları, tıbbi araştırmalar bu gibi bilgilere örnek gösterilebilir.

Ulusal savunma ve milletlerarası fonların transferi ile ilgili işlere sahip olsak bile, bir bilgi çok önemli olabilir. Şahsımıza ya da işimize ait bir bilginin çalınması ya da tehlikeye girmesi bize yönelik bir saldırıdır. Hatta, evimizde PC ile çalışırken de bilgisayar güvenliği bizi etkileyecektir. Eğer çok kullanıcı, dışa bağlantılı ve özellikle INTERNET' bağlı sistemlerde çalışıyorsak güvenlik ile yakından ilgilenmemiz ve çok ciddi bir şekilde tedbir almamız gerekmektedir. Günümüzde bu gibi çok kullanıcılı yeni sistemlere en azından parola sorma ve dosya koruma gibi güvenlik özellikleri ilave edilmiştir. Birçok teşkilat, kullanıcılarına bu özellikleri kullanmaları için ısrarlı olmaktadır.

Bu kadar geniş kapsamlı bilgi teknolojileri olan bağımlılığın artması sonucunda da güvenlik önemli bir yer işgal etmeye başlamıştır. Acaba her seviyede güvenlik alınmalımıdır ve bu güvenliğin seviyesi ne olmalıdır? Tüm bu sorulara risk yönetimi ile cevap bulunabilir. Risk yönetimi, tehditlere ve hassasiyetlere karşı alınacak potansiyel güvenlik tedbirleri, maliyet-etkin kararlarla değerlendirmeyi gerektirir. Bu maliyet-etkin kararlar, bilgi alt yapısı unsurlarına olabilecek başarılı saldırıların etkilerini değerlendirmeyi de içermelidir. Risk yönetimi yaklaşımı, yeterli olmayan kaynakların en etkin bir biçimde tahsisine imkan vermeli ve kabul edilebilir riskler karşılığında güvenliği teminat altına almalıdır.

Risk, bir tehdit analizinden çıkarılır. Resmi risk değerlendirilmesi riskler arasındaki ilişkiyi tayin etmede ve riske bağlı hasar yada kaybı hesaplamayı gerektirir. Bu ilişki, etkin karşı tedbirlerin temelini oluşturur. Tehdit, bir sistemin etkinliğini azaltabilen, etkisiz hale getirebilen ya da vazifenin başarılmasını önleyebilen bir unsur anlamındadır. Bilinen bir tehdit bulunmasa bile, düşmanca bir unsurun verebileceği zarar yinede değerlendirilmelidir.

Bilgi güvenliği tesis edilmesinde en önemli unsur olan tehdidin türlerini üç ana başlık altında toplayabiliriz. Bunlardan birincisi, sisteme yetkisiz giriş, gizlice dinleme, hırsızlık, casusluk ve yayılan radyasyonun kullanılmasından oluşan kasıtlı eylemlerdir. İkincisi, sel, yangın, elektrik kesintisi ve depremlerin toplamı olan doğal afetlerdir. Üçüncüsü ise, malzeme ve sistemin kötü ve yanlış kullanımı ve kullanıcı ile iletici hatalarının meydana getirdiği kaza sonucu oluşabilecek tehditlerdir.

Tehdidin kaynakları, bireylerden (muhbir ve yetkisiz kullanıcı gibi) karmaşık ulusal organizyonlara kadar geniş bir yelpaze olarak ortaya çıkmaktadır. Bu gruplar

arasındaki sınırlar belirsiz olduğundan; genellikle ortaya çıkan olayın kaynağını tespit etmek zordur. Örneğin, bir yetkisiz kullanıcı tarafından yapılmış gibi görünen bir iş, gerçekte yabancı bir ülkeye ait istihbarat servisinin marifeti olabilir. Tehdidin kaynakları; yetkisiz kullanıcılar, muhbir, teröristler, uyuşturucu kaçakçıları ve toplumsal eylemciler gibi devlet dışı gruplar, dış istihbarat örgütleri ve yabancı ülke silahlı kuvvetleri ya da siyasi hasımlardır.

Gelişen teknolojileri takip ederek birçok kaynak ve teknoloji kullanma imkanına sahip olan, nereden geleceğinin anlaşılması zor ve türünü bol olduğu güçlü bir tehdidin her zaman hazır beklediği, bilgi teknolojilerine bağımlılığın arttığı bu ortamda bilgi güvenli bir şekilde işlemek, depolamak ve iletimin ne kadar zor olduğu da kendiliğinden ortaya çıkmaktadır.

Tehdit kaynakları ne kadar kuvvetli ve becerikli olursa olsun bunlara karşı alınacak tedbirler de mevcuttur. Teknolojiler geliştikçe bunlara paralel olarak alınan güvenlik tedbirleri de geliştirilmelidir. Bu karşılıklı olarak yapılan bir mücadeledir ve hiç bitmeyecektir. Bitmeyecek bu mücadelenin kaçınılmaz sonuçları vardır. Bu konuda atılacak en önemli adım bilgi güvenliği için politika, prensip, yöntem ve standartların belirlenmesi, tamamen milli olarak gerçekleştirilmesi ve tüm bu faaliyetlerin yürütülecek bir teşkilatın kurulmasıdır. Milli olarak yapılmayan ve dışarıdan alınan bilgi güvenliğinin bilgiyi güvence altına alması söz konusu değildir. Tam aksine tehdidin işini kolaylaştırmaktadır.

BGYS bilgi kaynaklarını korumak için geliştirilmiştir. Değişik yaklaşımlar mevcuttur fakat hepsinin ortak bazı özellikleri vardır. Tüm yaklaşımlar proses başlangıcında organizasyonel değişiklikler gerektirir ve çoğu riskler ile uğraşmanın değerini vurgulamaktadır. Risk Analizine bağlı olarak önerilen özel korumaları ile ISO 17799 ve ISO 27001 gelişmiş en iyi sistemlerden birisidir. Uluslararası bir standart olduğundan iyi bilinmektedir ve kabul görmüştür. Bu standardı uygulayan firmalar geçmişe göre çok daha az dahili problem yaşadıklarını vurgulamışlardır.

Sunulan tez kapsamı hem ISO 17799 hem de ISO 27001 düzenleme tabanlıdır. Bilgi Güvenlik prosesi yapısını kullanarak, uygun BGYS gerçekleştirmesini sağlamaktadır. BGYS gerçekleştirilmesi prosesinde bir kaç ana unsur vardır. Başlatılması zordur, sürekli ve sabit analiz gerektirir ve hatasız kesin bir şekilde yapılmalıdır. Bu metindeki fikirler bunların altını çizmek ve uygun uygulamalarının

metotlarını vermek üzerinedir. ISO 27001 daha önceki kullanıcıların deneyimlerine göre bazı kritik başarı faktörler listelenebilir. Bunlar:

-İş amaçlarını yansıtan Güvenlik Politikası, amaçları ve aktiviteleri,

-Firma kültürü ile uyumlu bir güvenlik gerçekleştirme yaklaşımı,

-Yönetimden görülen destek ve sorumluluk,

-Güvenlik gereksinimlerinin, risk değerlendirmelerinin ve risk yönetiminin iyi algılanması,

-Tüm yönetici ve çalışanlara güvenliğin pazarlanması,

-Tüm çalışanlara ve yüklenicilere bilgi güvenlik politikası kılavuzunun dağıtımı,

-Uygun eğitim ve bilginin sağlanması,

-Bilgi güvenlik yönetimindeki performansı ölçen dengeli ve ayrıntılı ölçme sistemi ve iyileştirme için geri besleme, olarak vurgulanabilir.

Bu liste göstermektedir ki şirket yapısındaki değişiklikler fiziksel güvenlik önlemlerinden daha önemlidir. Yöneticiler, çalışanlarını, tüm sistemin anlaşılmasına hazırlamalıdırlar. Her şey sıra düzen içinde en üstten başlamalı ve çevre ile birlikte geliştirilmelidir. Her şeyin nasıl gözükeceği üst düzey yönetimin bir hareketine bağlıdır.

ISO 27001 tabanlı bir Bilgi Güvenli Sistemi oluşturmanın kendine özgü güçlü ve zayıf yönleri vardır. Güçlü yönleri, sistem düzgün bir şekilde uygulamaya geçince yönetiminin çok kolay olmasıdır. Yerleşik kontroller sayesinde tüm bilgi sistemini kapsayacaktır. Başka bir avantajı ise ISO 27001 kontrolleri tüm sistemi kapsar, hata için alan bırakmaz ve standart çok detaylı değildir. Kontroller bazı işlemler gerektirse de uygun ve kesin çözüm için çok fazla serbest alan bırakır.

Zayıf noktası ise bu konuda çok fazla yayın, sık kullanılan yöntemleri tanımlayan ve bazı durumlarda yapılması gerekenleri anlatan, olmamasıdır. Bazı durumlarda genelleme seviyesi çok yüksektir ve bu durum firma içinde uzun sürecek tartışmalara yol açabilir.

Özellikle Risk Analizi göstermiştir ki, bu faaliyetin pek çok yöntemi vardır. Analizin formunu ve kontrol edecek değerleri seçerken pek çok problem çıkabilir. Bu tez içinde vurgulanan ana noktaları taban alarak, bir BGYS sistemini uygulamaya sokarken hatırlanması gereken, üç ana sonuca varan bir liste oluşturulmuştur.

-Risk Analizi mümkün olduğu kadar kesin yapılmalıdır: İyi yapılmış bir Risk Analizi sistemin ve kendisini çevreleyen ortam ile ilişkilerin anlaşılmasına izin verir. Varlıkların tam listesi, düzgün şekilde analiz edildiğinde, gelecek olayların getireceklerini ve bunlara karşı yapılacak hazırlıkları yüksek doğrulukla verir.

-Sistem proseslerin devamlılığını sağlamalıdır: Her organizasyon çevresi ile birlikte gelişmektedir ve sistem bu değişimlere ayak uydurabilmesi için güncellenmelidir. Bu kısmın atlanması görevlerini verimli olarak yerine getiremeyen eski korumalara yol açacaktır.

-Hiçbir BGYS sürekli olarak %100 korunamaz: Bugünün bilgisayar sistemlerinde %100 güvenlik sağlamak imkansızdır. Bu sistemlerin karmaşıklığı ve BGYS'nin ele alması gereken mevcut olasılıkların fazlalığı uzun bir sürede sistemin güvenliğini imkansız kılar. Bu tip bir toplam güvenliğin maliyeti de çok yüksek olacaktır, sistemin kendi maliyetini bile aşabilir.

Bu gerçeklere rağmen, bilgi güvenliği yatırım için uygun bir alandır. Bilgi varlıkları çok önemlidir ve bir önlem alınmalıdır. Bilgi güvenliği bütçesi ve planlamaya uygun olursa dengeli ve iyi organize olmuş bir firmada başarı ile yürütülebilir.

Tüm bunlardan çıkan sonuç; Bilgi Güvenliği'nin bir teknoloji sorunu olmadığı, bunun bir iş yönetimi (sistem) sorunu olduğudur. Bu nedenle günümüzün rekabet ortamında global ekonominin içinde varolmak için bilgi kaynaklarının koruma ve güvence altına alma, bunu bir yönetim sistemi yaklaşımı içinde kurumsal düzeyde yaygınlaştırma mecburiyeti kurumları Bilgi Güvenliği Yönetim Sistemi kurmaya ve kullanmaya zorlayacaktır.

KAYNAKÇA

ASELSAN A.Ş.' nin Tanıtımı. 01 Mayıs 2006, http://www.aselsan.com.tr

Bilişim Sistemleri Güvenliği El Kitabı. Ankara: Türkiye Bilişim Derneği, Haziran 2003.

Bilişim Güvenliği. Oracle Türkiye: Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003.

Bisson Jacquelin, René Saint-Germain. **The BS 7799 / ISO 17799 Standardı ile Güvenlik Politikaları Uygulaması**, **Callio Technologies**, Şubat 2006, https://www.callio.com/files/wp_iso_en.pdf

Carlson, Tom. **Information Security Management: Understanding ISO 17799**. Lucent Technologies, Sep 2001.

Conrow, Edmund H. **Effective Risk Management**. Reston VA: AIAA, 2003.

Drucker, Peter F. **Gelecek İçin Yönetim**. Ankara:Türkiye İş Bankası Yayınları, 1993.

_____ . **Kapitalist Ötesi Toplum**. İstanbul: İnkilap Kitapevi, 1993.

_____ . **21. Yüzyıl İçin Yönetim Tartışmaları**. İstanbul: Epsilon Yayıncılık, 2000.

DURMUŞ Gürsoy. **Risk Analizi**. Mart 2006, http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/Riskanal.pdf

Edvinsson, Leif. **Şirket Boylamı**. İstanbul: Türk Henkel Dergisi yayınları, 2002

Elma Cevat, Demir Kamile.**Yönetimde Çağdaş Yaklaşımlar**. Ankara: Anı Yayıncılık, 2000.

Emiral, Fatih. **Bilgi Güvenliği Bilincinin Genele Yayılması**. 14 Nisan 2006, http://www.deloitte.com/dtt/article/0,1002,sid%253D8497%2526cid%253D53205,00.html

ERGUN, Ayhan. **Fiziksel Güvenliğinizden Emin misiniz?** 09 Mayıs 2006, http://www.acemiler.net/pc_guvenlik.phtml

Fıkırkoca, Meryem. **Bütünsel Risk Yönetimi**. Ankara: Pozatif Matbaacılık, 2003.

Filiz, Atilla. **Risk Yönetimi**. 05 Mart 2006, http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=638

George Von KROGH, Kazuo ICHIJO, Ikujro NONAKA. **Bilginin Üretimi**. İngilizce'den çeviren Günhan Günay. İstanbul: Dışbank, 2002.

Gökçen Hadi, **Yönetim Bilgi Sistemleri**. Ankara: EPİ yayıncılık, 2002.

Humphreys, Ted. " Certification News", ISMS Journal. Issue 6, Jan 2006.

International Organization for Standardization. ISO/IEC TR 13335-1, Information Technology - Security Techniques - Management of Information and Communications Technology Security. Part 1, 1996

"ISO17799 Danışmanlığı". Şubat 2006. http://www.innova.com.tr/04Hizmetler/detayli_bilgi02.htm

Karaaslan, Enis. "Güvenlik Nedir ?" 09 Mayıs 2006 http://www.birdenbire.com.tr/Guvenlikne.htm

Koç, Umut. "Komplekslik Yaklaşımı ve Bilgi Yönetimi", 3.Ulusal Bilgi Ekonomi ve Yönetim Kongresi. Eskişehir: Osmangazi Üniversitesi, 2004.

Küçükoğlu, Şule. "Uygun Güvenlik Çözümüne Yolculuk." 16 Mayıs 2006, http://www.infosecurenet.com/macroscope/macroscope6.pdf

Leroy A. , Sıgnoret J.Pierre. **Teknolojik Risk**. Çeviren Füsun Ülengin. İstanbul: İletişim Yayınları,1994.

Onur, Altay, "Bilgi Güvenliği Yönetim Sistemleri Standartları", http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=583 , Şubat 2006,

Okay M., Pekel A.,Yaman O.,Soyar D.,Kuleyın N., Mete A. "Bilişim Teknolojilerinde Risk Yönetimi". Kamu Bilişim Platformu, 20 Mart 2006 , http://kamubib.tbd.org.tr/dokumanlar/cg2.doc

ÖRNEK PINAR Nazik Nazan. İşletmelerde Bilgi Yönetimi ve ARÇELİK A.Ş.de Bilgi Yönetimi Sürecine İlişkin Uygulama Çalışması. Eskişehir: Anadolu Üniversitesi Y.Lisans tezi, 2002.

PGD-T007. ASELSAN Pazar Geliştirme Direktörlüğü Tanıtım Brifingi, Haziran 05.

Raymond McLeod, Jr., George Schell, **Management Information System**. Upper Saddle River, N.J. : Pearson Education, 2004.

Şahin, M. **Yönetim Bilgi Sistemi**. Eskişehir: A.Ü.İkt. ve İda.Bil.Fak.Yayınları, 2003.

Şamiloğlu, Famil. **Entelektüel Sermaye**. Ankara: Gazi Kitapevi,2002.

Şimşek, Şerif. **Yönetim ve Organizasyon**. Konya: Günay Ofset, 2002.

TIWANA, Amrit. **Bilginin Yönetimi**. Çeviren:Elif ÖZSAYAR. İstanbul: Dışbank, 2003.

Thomas, A. Stewart. **The Wealth of Knowledge**. New York : Currency, 2001.

Türk Standardları Enstitüsü. TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri. Ankara: 2002

Türk Standardları Enstitüsü. TS ISO/IEC 27001, Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler. Ankara: 2006

Türk Standardları Enstitüsü. TS ISO/IEC GUIDE 73, Risk Yönetimi- Terim ve Tarifler. Ankara: 2005

Türk Standardları Enstitüsü. TS IEC 62198, Proje Risk Yönetimi. Ankara: 2003

Uygulamalı BS7799 Eğitim Dokümanı. TÜBİTAK-UEKAE, 19/12/2005

Uz, Reha. **Risk Yönetimi ve Basel II'nin Kobi'lere Etkileri**. İstanbul: Türkiye Bankalar Birliği, Eylül 2004.

Yılmaz, Ayşe Küçük. Havacılıkta Emniyet Açısından Risk Yönetimi ve Havacılık Örgütlerinden Uygulama Örnekleri. Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, 2003.

_____ ,14 Mart 2006, http://isggm.calisma.gov.tr/docs/sunumlar/18.hafta/6May2004/8

_____ ,16 Mart 2006, http://www.uekae.tubitak.gov.tr/OKTEMWeb/Baglantilar/2-RiskYonetimi.htm