

Doküman Kodu: BGYS-0004

BGYS - RİSK YÖNETİM SÜRECİ KILAVUZU

SÜRÜM 1.00

17.08.2007

Hazırlayan: Doğan Eskiyyörük

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliği Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali Dinkan, Burak Bayođlu ve Hayrettin Bahşı'ye teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ	6
1.1 Amaç ve Kapsam.....	6
1.2 Kısaltmalar.....	6
2. RİSK ANALİZİ	7
2.1 Kapsam Belirlenmesi.....	7
2.2 Varlıkların Belirlenmesi	7
2.2.1 Anketler.....	8
2.2.2 Birebir görüşmeler	8
2.2.3 Dokümantasyonun incelenmesi	8
2.2.4 Otomatik tarama araçları.....	8
2.3 Tehditlerin Belirlenmesi	8
2.4 Açıklıkların Belirlenmesi.....	10
2.5 Mevcut ve Planlanan Kontrollerin Belirlenmesi	12
2.6 Olasılık Değerlendirmesi	13
2.7 Etki Analizi.....	13
2.8 Risk Derecelendirmesi.....	14
2.8.1 Risk Derecelendirme Matrisi	15
2.8.2 Risk Derecelerinin Tanımı.....	15
2.9 Uygun Kontrollerin Belirlenmesi	16
2.9.1 Kontrol Kategorileri.....	16
2.9.1.1 Teknik Güvenlik Kontrolleri.....	17
2.9.1.2 Yönetimsel Kontroller.....	19
2.9.1.3 Operasyonel Kontroller.....	20
2.10 Sonuçların Dokümantasyonu.....	21
3. RİSK İŞLEME.....	22
3.1 Risk İşleme Yöntemleri	22
3.2 Kontrollerin Uygulanması	22

3.3 Kontrollerin Uygulanmasında İzlenecek Yaklaşım.....	24
3.3.1 Risklerin Önceliklendirilmesi	24
3.3.2 Uygun Kontrollerin Değerlendirilmesi	24
3.3.3 Kontrollerin Seçilmesi	24
3.3.4 Sorumluların Atanması	24
3.3.5 Kontrol Uygulama Planının Hazırlanması.....	24
3.3.6 Seçilen Kontrolün Uygulanması	25
3.4 Artık Risk	25
4. DEĞERLENDİRME VE TAKİP.....	26
KAYNAKÇA	27

1. GİRİŞ

“TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler” standardına göre risk yönetimi bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak tanımlanmıştır.

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

1.1 Amaç ve Kapsam

Bu dokümanın amacı risk yönetim süreci oluşturacak kurumlara risk yönetimi sürecinin planlanması, kurulması ve işletilmesi konularında yol göstermektir. Başarılı bir risk yönetimi süreci oluşturmak için gerekli safhaların nasıl ele alınacağı, risk yönetimi sürecinin nasıl sürekli bir süreç haline getirileceği anlatılmaktadır.

1.2 Kısaltmalar

- BGYS** : Bilgi Güvenliği Yönetim Sistemi
BT : Bilişim Teknolojileri
ISO : International Standards Organization
UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

2. RİSK ANALİZİ

Risk analizi TS ISO/IEC 27001:2005 standardında kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmıştır. Risk analizi süreci kapsam belirlenmesi ile başlar. Belirlenen kapsamda bulunan varlıklar belirlendikten sonra, tehditler, açıklıklar ve mevcut kontroller belirlenir. Daha sonra olasılık değerlendirmesi ve etki analizi gerçekleştirilir. Son olarak bulunan riskler derecelendirilerek dokümente edilir.

2.1 Kapsam Belirlenmesi

Risk analizinin ilk adımı kapsam belirlenmesidir. Kapsamın ilk aşamada doğru ve kurum hedeflerine uygun olarak belirlenmesi ileride gereksiz çaba harcanmasını önler ve risk analizinin kalitesini artırır. Kapsamda risk analizine tabi her şey açık olarak belirlenmelidir. Örneğin risk analizinde dikkate alınacak tüm BT varlıkları(yazılım donanım gibi), personel, tesisler, operasyonlar açıkça belirtilmelidir. Örnek bir kapsam şu şekilde olabilir. “Bu risk analizi kurumun muhasebe işlemlerinde kullanılan tüm donanım, yazılım ve personeli kapsar.” Bu durumda muhasebe işlemleri için kullanılan tüm sunucular, kullanıcı bilgisayarları, işletim sistemleri, veri tabanı yazılımları, uygulamalar ve tüm bunları kullanan ve yöneten kurum personeli risk analizi içerisinde yer alır.

2.2 Varlıkların Belirlenmesi

Varlık, sistemin bir parçası olan ve kurum için değeri olan her şeydir. Varlık kurum için değer taşıdığından korunması gerekir. Bir BT sisteminde sadece yazılım ve donanımlar varlık olarak düşünülmemelidir. Aşağıdaki örnekler varlık olarak nitelendirilebilecek değerlerdir.

- bilgi (satış bilgilerini içeren dosyalar, ürün bilgileri)
- donanım (kişisel bilgisayarlar, yazıcılar, sunucular)
- yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları)
- haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları)
- dokümanlar(stratejik toplantıların tutanakları, sözleşmeler)
- üretilen mallar
- servisler
- mali değerler (çekler, para, fonlar)

- personel
- kurumun prestiji / imajı

Varlıkların belirlenmesinde kullanılabilecek bazı bilgi toplama teknikleri mevcuttur. Aşağıdaki tekniklerden biri veya birkaçı varlıkların belirlenmesinde kullanılabilir.

2.2.1 Anketler

Varlıkların belirlenmesinde ve risk analizi için gerekli bilgilerin toplanmasında anketler kullanılabilir. Anketler BT sistemini kullanan, tasarlayan ve destekleyen tüm personele uygulanabilir.

2.2.2 Birebir görüşmeler

BT sistemini yöneten ve bu sisteme destek sağlayan personel ile yapılacak görüşmeler sistemin nasıl işlediği ve nasıl yönetildiği konularında yararlı bilgiler edinilmesini sağlar. Bu görüşmeler sırasında operasyonun işleyişi ile ilgili edinilen bilgiler sayesinde gözden kaçabilecek bazı varlıklar daha rahat belirlenir.

2.2.3 Dokümantasyonun incelenmesi

Politikaların, sistem dokümantasyonunun (işletme talimatları ve ağ diyagramı gibi), önceki risk değerlendirme raporlarının incelenmesi varlıkların çoğunun hızlı ve doğru bir şekilde belirlenmesini sağlar.

2.2.4 Otomatik tarama araçları

Ağ tarama araçları gibi otomatik tarama araçları büyük bir sistemde bulunan varlıkların belirlenmesini kolaylaştırır ve bazı varlıkların gözden kaçırılmasını engeller.

2.3 Tehditlerin Belirlenmesi

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları şunlardır:

Doğal tehditler: Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler.

Çevresel tehditler: Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.

İnsan kaynaklı tehditler: İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs.

Tehdit değerlendirmesi sırasında hiçbir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir.

Tehdit değerlendirmesi için gerekli girdi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden elde edilebilir. Ayrıca tehditlerin belirlenmesinde tehdit katalogları da kullanılabilir. Aşağıdaki tablo BT sistemlerinde sıklıkla karşılaşılan tehditleri ve bunların kaynaklarını içermektedir (tehdidin kaynağı bölümünde kullanılan kısaltmalar B: İnsan kaynaklı ve bilerek, K: İnsan kaynaklı ve kazayla, D: Doğal, Ç: Çevresel).

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

Tehdit	Tehdidin kaynağı
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K
Hat kapasitelerinin yetersiz kalması	B, K
Ağ trafiğinin dinlenmesi	B
İletim hatlarının hasar görmesi	B, K
İletişimin dinlenmesi	B
Mesajların yanlış yönlendirilmesi	K
Mesajların yetkisiz kişilere yönlendirilmesi	B
İnkâr etme(repudiation)	B
Kaynakların yanlış kullanımı	K
Kullanıcı hataları	K
Personel yetersizliği	K

Tablo 2.1 – BT sistemlerinde karşılaşılan tehditler ve kaynakları

2.4 Açıklıkların Belirlenmesi

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir.

Açıklık değerlendirmesi, tehditler tarafından gerçekleştirilebilecek açıklıkları ve bu açıklıkların ne kadar kolay gerçekleştirilebileceğini ele alır. Açıklıkların belirlenmesinde de varlık belirlemede anlatılan anket, birebir görüşme, dokümantasyon ve otomatik tarama araçları gibi yöntemler kullanılabilir. Ayrıca aşağıdaki kaynakların kullanımı da önerilmektedir.

- Açıklık listeleri ve açıklık veritabanları (Örneğin <http://nvd.nist.gov/> , <http://www.us-cert.gov/cas/techalerts/> , <http://www.securityfocus.com/vulnerabilities>)
- Önceki BT sistemi denetim raporları, test raporları, hata raporları
- Önceki risk değerlendirme dokümanları
- Üreticiler tarafından yayınlanan uyarılar
- Güvenlikle ilgili web sayfaları ve e-posta listeleri
- Yazılım güvenlik analizleri
- Sistem güvenlik taramalarının ve sızma testlerinin sonuçları

Aşağıdaki listede bazı örnek açıklıklar ve bu açıklıkları gerçekleyebilecek tehditler verilmiştir.

- Altyapı ve çevreyle ilgili açıklıklar

- Binada yeterli fiziksel güvenliğin bulunmaması (hırsızlık)
- Binalara ve odalara girişlerde yetersiz fiziksel kontrol (kasten zarar verme)
- Eski güç kaynakları (güç dalgalanmaları)
- Deprem bölgesinde bulunan yapılar (deprem)
- Herkesin erişebildiği kablosuz ağlar (hassas bilginin açığa çıkması, yetkisiz erişim)
- Dış kaynak kullanımında işletilen prosedür ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği (yetkisiz erişim)
- Donanımlarla ilgili açıklıklar
 - Periyodik yenilemenin yapılmaması (saklama ortamlarının eskimesi, donanımların bozulması nedeniyle erişimin durması)
 - Voltaj değişikliklerine, ısıya, neme, toza duyarlılık (güç dalgalanmaları, erişim güçlükleri vs.)
 - Periyodik bakım eksikliği (bakım hataları)
 - Değişim yönetimi eksikliği (kullanıcı hataları)
- Yazılımlarla ilgili açıklıklar
 - Yama yönetimi eksikliği/yetersizliği (yetkisiz erişim, hassas bilginin açığa çıkması)
 - Kayıt yönetimi eksikliği/ yetersizliği (yetkisiz erişim)
 - Kimlik tanımlama ve doğrulama eksiklikleri (yetkisiz erişim, başkalarının kimliğine bürünme)
 - Şifre yönetimi yetersizliği (yetkisiz erişim, başkalarının kimliğine bürünme)
 - Şifre veritabanlarının korunmaması (yetkisiz erişim, başkalarının kimliğine bürünme)
 - Erişim izinlerinin yanlış verilmesi (yetkisiz erişim)
 - İzinsiz yazılım yüklenmesi ve kullanılması (zararlı yazılımlar, yasal gerekliliklere uyum)
 - Saklama ortamlarının doğru silinmemesi ve imha edilmemesi (hassas verinin ortaya çıkması, yetkisiz erişim)

- Dokümantasyon eksikliği/yetersizliği (kullanıcı hataları)
- Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi (yazılım hataları)
- Yazılımların yeterli test edilmemesi (yetkisiz erişim, yazılımların yetkisiz kullanımı)
- Haberleşmeyle ilgili açıklıklar
 - Korunmayan haberleşme hatları (haberleşmenin dinlenmesi)
 - Hat üzerinden şifrelerin açık olarak iletilmesi (yetkisiz erişim)
 - Telefon hatlarıyla kurum ağına erişim (yetkisiz erişim)
 - Ağ yönetimi yetersizliği/eksikliği (trafiğin aşırı yüklenmesi)
- Dokümanlarla ilgili açıklıklar
 - Dokümanların güvensiz saklanması (hırsızlık)
 - Dokümanların kontrolsüz çoğaltılması (hırsızlık)
 - Dokümanların imha edilmemesi (hırsızlık, hassas bilginin açığa çıkması)
- Personel ile ilgili açıklıklar
 - Eğitimi eksikliği (personel hataları)
 - Güvenlik farkındalığı eksikliği (kullanıcı hataları)
 - Donanımların veya yazılımların yanlış kullanılması (personel hataları)
 - İletişim ve mesajlaşma ortamlarının kullanımını düzenleyen politikanın eksikliği/yetersizliği (yetkisiz erişim)
 - İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması (kasten zarar verme)

2.5 Mevcut ve Planlanan Kontrollerin Belirlenmesi

Yukarıda belirlenen tehditlerin, açıklıkları gerçekleştirme olasılıklarını azaltacak veya ortadan kaldıracak kontrollerin halihazırda uygulanıp uygulanmadığı veya bu kontrollerin uygulanmalarının planlanıp planlanmadığı incelenmelidir. Uygulanan veya uygulaması planlanan kontroller açıklıkların gerçekleştirme olasılıklarını düşüreceği için olasılık değerlendirmesinde ve dolayısıyla risk derecelendirmesinde önem kazanacaktır.

Kontrollerle ilgili detaylı bilgi Uygun Kontrollerin Belirlenmesi başlıklı bölümde yer almaktadır.

2.6 Olasılık Değerlendirmesi

Risk analizinde bir açıklığın gerçekleşme olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm açıklıklar için olasılık değerlendirme yapılmalıdır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, açıklığın cinsi, mevcut kontrollerin varlığı ve etkinliği göz önünde bulundurulmalıdır.

Olasılık değerlendirme için kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir olasılık değerlendirme için aşağıdaki örnek tablo kullanılabilir.

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

Tablo 2.2 – Üç seviyeli bir olasılık değerlendirme için olasılık tanımları

2.7 Etki Analizi

Risk derecelendirmesi yapabilmek için olasılık değerlendirmesinden sonra gelen adım etki analizidir. Etki analizinde herhangi bir açıklığın gerçekleşmesi halinde yaşanacak olası olumsuz etki seviyesi belirlenir. Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalıdır. Bu bilgiler daha önceden yapılmış iş etki analizi raporlarından alınabilir. Eğer daha önce yapılmış böyle bir çalışma yoksa sistemin kritiklik seviyesi sistemin (ve sakladığı veya işlediği verinin) bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli koruma göz önüne alınarak niceliksel olarak çıkarılabilir. Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde göz önüne alınabilir.

Niceliksel bir etki analizinde olasılık değerlendirmesinde olduğu gibi kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir etki değerlendirmesi için aşağıdaki örnek tablo kullanılabilir.

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

Tablo 2.3 – Üç seviyeli bir etki değerlendirmesi için etki tanımları

2.8 Risk Derecelendirmesi

Bu adımın amacı, varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelere göre yapılır. Risk bir tehdidin bir açıklığı gerçekleştirme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır.

Risklerin ölçülebilmesi için risk sınıflandırma matrisi oluşturulmalıdır ve bu sınıflandırma için tanımlamalar yapılmalıdır.

2.8.1 Risk Derecelendirme Matrisi

Yukarıda örnek olarak verilen üç seviyeli olasılık değerlendirme ve etki analizi için şu şekilde bir risk derecelendirme matrisi oluşturulabilir.

		Etki seviyesi		
		Düşük	Orta	Yüksek
Olma olasılığı	Düşük	Düşük	Düşük	Düşük
	Orta	Düşük	Orta	Orta
	Yüksek	Düşük	Orta	Yüksek

Tablo 2.4 – Örnek risk derecelendirme matrisi

Bu matristeki değerleri kurum kendisi belirlemelidir. Bunun için istenirse sayısal değerler kullanılabilir. Örneğin olma olasılıklarına 0 ile 1 arasında, etki seviyesine ise 0 ile 100 arasında değerler atanır. Risk dereceleri için aralıklar belirlenir. Olma olasılığı ve etki seviyesi çarpımının düştüğü aralık risk derecesini belirler. Örneğin bu matrise göre olma olasılığı “Orta” ve etki seviyesi “Yüksek” olan bir açıklığın risk derecesi “Orta” olarak sınıflandırılmıştır.

2.8.2 Risk Derecelerinin Tanımı

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçekleşmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir.

Yukarıdaki risk seviye matrisine uygun olarak aşağıdaki tanımlamalar örnek olarak gösterilebilir.

Risk derecesi	Risk açıklaması ve yapılması gerekenler
Yüksek	Düzeltilici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl

	uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltilici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusuna tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Tablo 2.5 – Risk dereceleri ve tanımları

2.9 Uygun Kontrollerin Belirlenmesi

Yapılan risk derecelendirme çalışmalarının sonucunda risklerin azaltılmasını veya ortadan kaldırılmasını sağlayacak kontrol önerileri belirlenmelidir. Önerilecek kontrollerin amacı riski kurumun kabul edebileceği bir değere düşürmek olmalıdır. Önerilecek kontrollerde kontrollerin etkinliği, yasalar ve düzenlemeler, iş yapma biçimine getireceği değişiklikler, kurum politikaları ve güvenlik konuları dikkate alınması gereken başlıca konulardır.

Uygulanabilecek olası kontroller belirlenirken başvurabilecek kaynaklardan biri “TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler” standardıdır. Bu standart, güvenlik politikası, bilgi güvenliği organizasyonu, varlık yönetimi, insan kaynakları güvenliği, fiziksel ve çevresel güvenlik, haberleşme ve işletim yönetimi, erişim kontrolü, bilgi sistemleri edinim, geliştirme ve bakımı, bilgi güvenliği ihlal olayı yönetimi, iş sürekliliği yönetimi ve uyum ana başlıkları altında pek çok kontrol önerisi içermektedir. Ayrıca bu kontrollerin gerçekleştirilmesine ait öneriler ve en iyi uygulamalar için TS ISO/IEC 27002:2005 standardına başvurulmalıdır.

2.9.1 Kontrol Kategorileri

Açıklıkların gerçekleşmesini önlemek veya gerçekleşen ihlallerin takibini yapabilmek için uygulanabilecek kontroller teknik, yönetsel ve operasyonel kontroller olarak üçe ayrılabilir. Uygun kontroller belirlenirken bu kontrol kategorilerden birkaçı veya hepsi kullanılabilir. Uygun kontrole yine kurumun kendisi karar vermelidir. Örneğin teknik bir kontrolün uygulanması daha pahalı ve daha bir zahmetli iş olabilir fakat yönetsel kontrollere göre daha etkin olacaktır.

2.9.1.1 Teknik Güvenlik Kontrolleri

Teknik güvenlik kontrolleri risk önlemede oldukça etkin kontrollerdir. Bu kontroller yazılım, donanım, sistem mimarisi vb. gibi çözümleri içerir. Teknik güvenlik kontrolleri destekleyici, önleyici, tespit edici ve düzeltici olmak üzere dört çeşittir.

2.9.1.1.1 Destekleyici Teknik Kontroller

Destekleyici kontroller diğer kontrollerin uygulanmasını sağlayan temel kontrollerdir. Bu kontroller şu şekilde tanımlanabilir.

Kimlik tanımlama: Bu kontrol bir kullanıcının, sürecin veya sistemin eşsiz/benzersiz olarak tanımlanmasında kullanılır. Diğer kontrollerin uygulanabilmesi için (örneğin erişim kontrol listeleri) kimlik tanımlaması şarttır.

Kriptografik anahtar yönetimi: Diğer kontrollerde kriptografik işlemlerin güvenli bir şekilde gerçekleştirilebilmesi için kriptografik anahtar yönetiminin güvenli bir şekilde gerçekleştirilmesi gerekir. Anahtar üretimi, saklanması, dağıtımı ve bakımı kriptografik anahtar yönetiminin içerisindedir.

Güvenlik yönetimi: Bir BT sisteminin güvenlik özellikleri kurumun ihtiyaçlarını karşılayacak şekilde ayarlanabilmelidir. Örneğin bir veritabanındaki bilgileri kimin okuyacağı, kimin oluşturacağı ve kimin güncelleyebileceği ayarlanabilmelidir. Böylece gereğinden fazla yetki verilmemiş olur.

Sistem koruma kontrolleri: Bu kontroller bir sistemin güvenliğinin sağlanabilmesi için gerekli temel konuları içerir. Örneğin bilmesi gereken prensibi, süreçlerin ayrımı, objelerin tekrar kullanılması, katmanlı yapılarda çalışma, güvenilecek nesne sayısının en aza indirgenmesi gibi prensipler bu tip kontrollerdir.

2.9.1.1.2 Önleyici Teknik Kontroller

Bu kontroller güvenlik ihlallerinin gerçekleşmesini önleyici kontrollerdir

Kimlik doğrulama: Bu kontrol kullanıcının belirttiği kimlik tanımlamasını doğrulamaya yarar. Bunun için şifre, PIN numarası, akıllı kart gibi mekanizmalar kullanılmaktadır.

Yetkilendirme: Yetkilendirme bir sistemde izin verilen işlemlerin belirlenmesini ve yönetimin alt birimlere dağıtılabilmesini sağlayan kontroldür.

Erişim kontrolü: Verinin gizliliği ve bütünlüğü erişim kontrolleri ile sağlanır. Bir kaynağa erişim için yetkilendirme yapıldıktan sonra uygun politikalara göre erişim kontrolü sağlanmalıdır. Gizlilik derecesi etiketleri, dosya izinleri, kullanıcı profilleri erişim kontrolünde kullanılan mekanizmalardan bazılarıdır.

İnkâr edememe: Bilgiyi gönderenin gönderdiğini, alanın da aldığını inkâr edememesi sistemin izlenebilirliği açısından önemlidir.

Güvenli iletişim: Günümüzde sık kullanılan dağıtık yapılarda güvenliğin korunmasındaki en önemli faktörlerden biri iletişim sırasında verinin gizliliğinin ve bütünlüğünün korunabilmesidir. Bunun için iletişim sırasında çeşitli şifreleme metotları ve kriptografik önlemler kullanılarak hat dinlemesi, paket dinleme, tekrar gönderme gibi saldırılara karşı önlem alınabilir.

İşlem gizliliği (Transaction privacy): Kişisel işlemlerin gizliliği gittikçe önem kazanmaktadır. Secure Socket Layer(SSL) ve Secure Shell(SSH) gibi teknolojiler kişilerin yaptığı işlemlerin gizliliğinin kaybolmasını engellemek amacıyla kullanılır.

2.9.1.1.3 Tespit Edici Teknik Kontroller

Tespit edici kontroller güvenlik ihlalleri gerçekleştikten sonra nelerin, kimin tarafından, ne zaman ve nasıl yapıldığını bulmak için kullanılır.

Denetleme: Güvenlikle ilgili olayların ve sistemdeki anormalliklerin izlenmesi, güvenlik ihlallerinin tespitinde ve olası bir ihlalden geri dönmede en önemli kontroldür

Saldırı tespiti: Ağ sızmaları ve şüpheli olaylar gibi güvenlik ihlali olabilecek durumların tespiti, uygun kontrolün alınması ve gerekli düzeltmelerin yapılabilmesi için çok önemlidir.

Bütünlük: Sistemin veya verinin bütünlüğünün takip edilmesi, ihlallerin tespit edilmesi açısından önemlidir. Örneğin işletim sisteminin kullandığı dosyalar sadece gerekli işlemler için okunurlar ve bu dosyaların üzerinde değişiklik yapılmaz. Bu dosyaların bütünlüğü virüs veya zararlı bir yazılım tarafından değiştirilirse anti virüs programları bunu tespit edebilir.

2.9.1.1.4 Düzeltici Teknik Kontroller

Güvenlik ihlalleri tespit edildikten sonra sistemi eski haline getirmek için kullanılan kontroller bu kategoride incelenebilir.

Yedekleme: Kaybedilen veya bütünlüğü bozulan veri yedeklerden geri dönülerek eski haline getirilebilir.

2.9.1.2 Yönetimsel Kontroller

Yönetimsel kontroller kurumda uygulanan politika, prosedür, standart gibi kuralların uygulanmasını sağlayacak kontrollerden oluşur ve önleyici, tespit edici ve düzeltici olmak üzere üç kategoriye ayrılır.

2.9.1.2.1 Önleyici Yönetimsel Kontroller

Önleyici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- BT sistemlerinde güvenliği sağlamak üzere kişilere sorumluluklarının atanması.
- Mevcut ve planlanan kontrollerin dokümante edilmesini sağlayacak sistem güvenlik planlarının geliştirilmesi ve uygulanması.
- Görevlerin ayrılığı, gerekli en düşük yetkilerin verilmesi, hakların tahsis edilmesi ve sonlandırılması gibi personelle ilgili güvenlik kontrollerinin uygulanması
- Güvenlik farkındalığı ve teknik eğitimlerinin verilerek sistem kullanıcı ve yöneticilerinin bilgi seviyelerinin artırılması.
- Güvenlik politikalarında belirtilen kuralların çalışanlar tarafından bilinmesinin sağlanması.
- Çalışanların özgeçmişlerinin doğrulanması, geçmişlerinin incelenmesi.

2.9.1.2.2 Tespit Edici Yönetimsel Kontroller

Tespit edici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- Güvenlik önlemlerinin periyodik olarak test edilmesi.
- Risk yönetiminin uygulanması ve risk işleme için gerekenlerin yapılması.
- Periyodik olarak sistemlerin denetlenmesi.

2.9.1.2.3 Düzeltici Yönetimsel Kontroller

Düzeltici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir

- Sistemlerinin devamlılığının sağlanması ve acil durumlarda veya felaket anlarında BT sisteminin tekrar kullanılabilir hale getirilmesini sağlayacak planların, prosedürlerin ve testlerin yapılmasının sağlanması.
- Acil durum müdahale ekiplerinin kurulması ve yetkin hale getirilmesinin sağlanması.

2.9.1.3 Operasyonel Kontroller

Kurumun güvenlik politikalarının BT varlıklarının kullanılması sırasında doğru şekilde uygulanmasını sağlamak için operasyonel kontrollerin geliştirilmesi ve yönetim tarafından takip edilmesi gerekir. Operasyonel kontroller kurumdaki işlerin yapılması sırasında kasten veya bilmeden yapılabilecek hataları engeller. Bunun için operasyonel kontrollerin nasıl uygulanacağını adım adım açıkladığı dokümanların bulunması ve bu dokümanların kontrolleri uygulayanlar tarafından biliniyor olması gerekmektedir. Önleyici ve tespit edici operasyonel kontroller için bazı örnekler aşağıda verilmiştir.

2.9.1.3.1 Önleyici Operasyonel Kontroller

- Veri ortamlarına erişimin ve veri ortamlarının yok edilmesinin kontrol edilmesi (fiziksel erişim kontrolü uygulanması, veri saklama cihazlarının uygun şekilde imha edilmesi)
- Verinin yetkisiz kişilerin eline geçmesinin engellenmesi (veri sınıflandırma etiketlerinin kullanılması)
- Zararlı yazılım içerebilecek veri kaynaklarının kontrol edilmeden kullanılmasının engellenmesi
- Ziyaretçilere refakat edilmesi, kimlik kartı taşınması, anahtarların dağıtımının kontrolü gibi fiziksel güvenliği sağlayıcı operasyonel kontroller
- Yedeklerin alınmasını ve güvenli bir yerde saklanmasını sağlayacak operasyonel adımları içeren kontroller
- Mobil bilgi işleme cihazlarının kullanım şartlarının belirlenmesi ve güvenliğinin sağlanması
- Varlıkların yangın, yanlış kullanım vb. sebeplerden etkilenmemesi için uygulanan kontroller (sistem odasında yiyecek ve içecek bulundurulmaması, yangın tespit ve söndürme sistemlerinin kullanılması, kesintisiz güç kaynakları gibi)

2.9.1.3.2 Tespit Edici Operasyonel Kontroller

- Güvenlik kameraları, hareket algılayıcıları ve alarm sistemleri gibi tespit edici fiziksel kontrollerin uygulanması
- Çevresel etkilerin takip edilmesi (duman ve yangın detektörlerinin kullanılması)

2.9.1.3.3 Düzeltici Edici Operasyonel Kontroller

- Yapılan işlerin dokümante edilmesi olası değişikliklerde doğru ayarlamaların tekrar yapılabilmesini sağlar.
- Yapılan değişikliklerin dokümante edilmesi ve bir sorun halinde değişiklik yapılmadan önceki duruma geri dönülebilmesi, yapılan değişikliklerden dolayı oluşabilecek sorunların düzeltilmesini sağlar.

2.10 Sonuçların Dokümantasyonu

Sonuçların dokümantasyonu risk analizi sürecinde en önemli adımlardan biridir. Bu dokümanlar mevcut risk ve kontrollerin herkes tarafından bilinmesini sağlarlar. Ayrıca bu dokümanlar daha sonraki risk analizlerine girdi teşkil ederler.

Risk analizi süreci tamamlandığında sonuçlar bir rapor olarak dokümante edilmelidir. Bu rapor yönetimin ve süreç sahiplerinin politikalarda, prosedürlerde, bütçede ve sistemin kullanımında veya yönetiminde yapılacak değişikliklerde karar verirken kullanacağı yönetsel bir rapordur. Yönetimin riskleri rahat bir şekilde anlayabilmesi için açık ve sistematik olmalıdır. Belirlenen riskler için uygulanacak kontrollere bu rapor göz önünde bulundurularak karar verilecektir.

3. RİSK İŞLEME

Risk yönetiminde ikinci aşama risk işleme aşamasıdır. Bu aşama risk analizinde belirlenen risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek uygulanmasından oluşur.

Risklerin tamamen ortadan kaldırılması için bütün kontrollerin uygulanması çoğu zaman mali açıdan imkansızdır. Risk işleme için burada belirtilen risk işleme yöntemlerini kullanılır. Yönetim, riski azaltmak istediğinde sisteme gelebilecek zararı en aza indirmek için “en düşük maliyetli” ve “en uygun” kontrolü seçmekle sorumludur. Bu bölüm “en düşük maliyetli” ve “en uygun” kontrolün nasıl seçilmesi gerektiğini anlatmaktadır.

3.1 Risk İşleme Yöntemleri

Risk işleme yöntemleri kurumun iş hedeflerine ve misyonuna uygun olarak seçilmelidir. Riski azaltmak için kullanılacak yöntemler şu şekilde sıralanabilir.

Riskin Kabulü: Riskin var olduğunu kabul ederek BT sistemlerini kullanmaya devam etmektir.

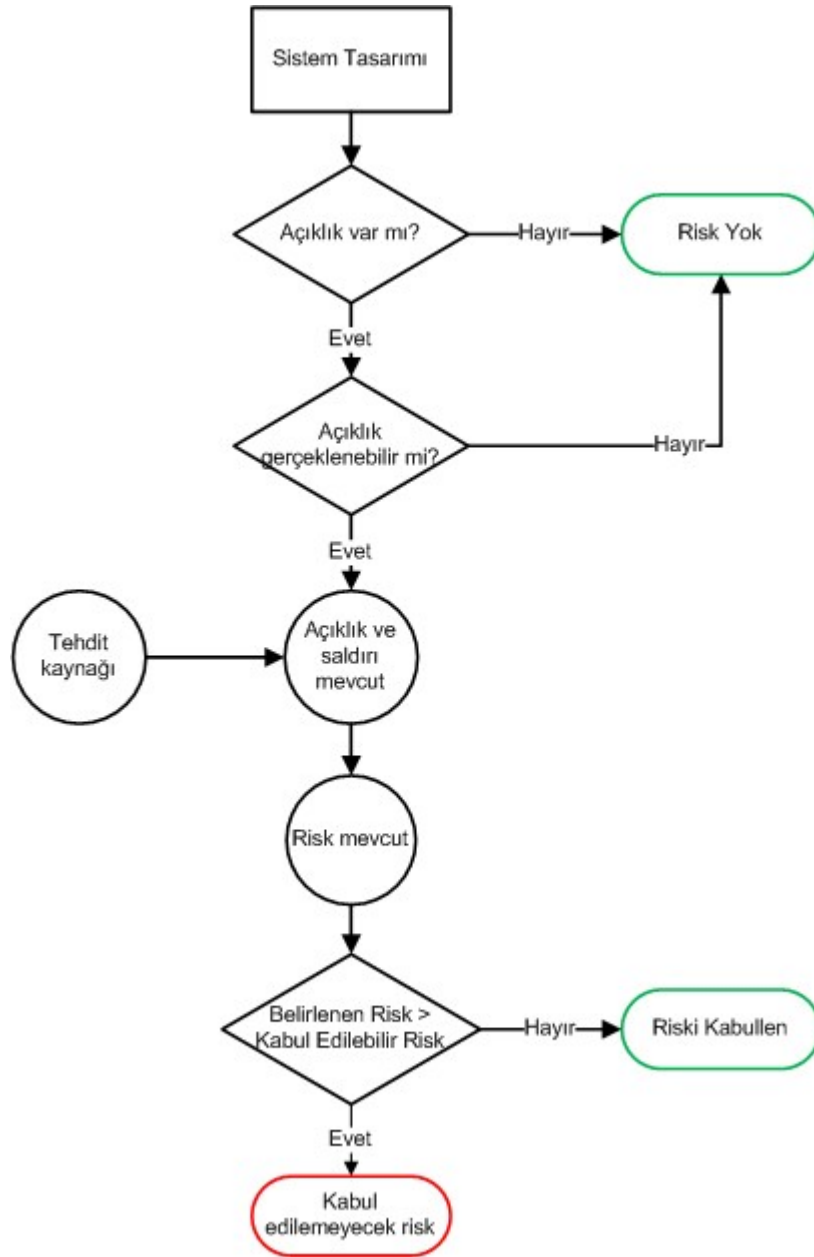
Riskten Kaçınma: Riski yaratan sebebi ortadan kaldırmaktır (örneğin bir yazılımın risk yaratan kısmının yüklenmemesi ve kullanılmaması gibi)

Riskin Azaltılması: Açıklığın gerçekleşmesi halinde oluşacak etkinin uygulanan kontroller ile azaltılması.

Riskin Transferi: Riskin gerçekleşmesi durumunda oluşabilecek zararı karşılayacak çözümler bularak (örneğin sigorta yaptırmak) riskin başkalarına aktarılmasıdır.

3.2 Kontrollerin Uygulanması

Risk analizi sonrasında sistemdeki mevcut riskler ve bu risklere karşı kullanılacak olası kontroller belirlenmektedir. Fakat her risk önlem almaya değecek bir risk olmayabilir. Bu durumda hangi riskler için önlem alınacağı ve olası kontroller içerisinde hangisinin kullanılacağını belirlemek kurumun maliyetleri açısından çok önemlidir. Bunu belirlemek için iki önemli nokta vardır. Saldırganın kazancının saldırı maliyetinden düşük olduğu veya tahmini kaybın belirlenen eşik değerinden küçük olduğu durumlarda risk için önlem almak yerine risk kabul edilebilir. Yani kısacası mevcut risk daha önce belirlenen kabul edilebilir riskten küçükse risk kabul edilebilir, aksi takdirde riski azaltacak uygun kontroller uygulanmalıdır. Bu süreç aşağıdaki akış diyagramında daha detaylı olarak açıklanmıştır.



Şekil 3.1 – Önlem alınacak risklerin belirlenmesinde kullanılacak süreç

Ayrıca yukarıdaki akış diyagramında bulunan riskle ilgili karar adımları ile ilgili uygulanabilecek bazı yaklaşımlar şunlardır.

- Eğer açıklık mevcutsa açıklığın uygulanma olasılığını azaltacak kontroller uygulanabilir.
- Eğer açıklık gerçekleştirilebiliyorsa kademeli güvenlik anlayışı, güvenli mimariler ve yönetsel kontroller kullanılarak risk azaltılabilir
- Saldırının maliyeti saldırı sonucu elde edilecek kazançtan fazlaysa saldırganın maliyetlerini arttıracak ve motivasyonunu düşürecek önlemler alınabilir.

- Tahmini kayıp çok büyük olduğunda doğru tasarım prensipleri, güvenli mimariler, teknik ve teknik olmayan kontroller kullanarak saldırının yaratacağı kayıp azaltılabilir.

3.3 Kontrollerin Uygulanmasında İzlenecek Yaklaşım

Kontroller, en büyük risklerden başlayarak, kurumun süreçlerine en az zarar verecek, riski en aza indirecek ve en düşük maliyetli olacak şekilde seçilmelidir. Bu süreçte aşağıdaki adımlar izlenebilir.

3.3.1 Risklerin Önceliklendirilmesi

Risk analizinde belirlenen risk seviyelerine göre riskler önceliklendirilmelidir. Risk işleme için kaynak aktarımı yapılırken öncelik yüksek risk dereceli risklere verilmeli, bu riski oluşturan açıklıklar ve tehditlere karşı önlemler daha önce alınmalıdır.

3.3.2 Uygun Kontrollerin Değerlendirilmesi

Riskler önceliklendirdikten sonra bu riskler için daha önceden belirlenmiş kontroller değerlendirilmelidir. Belirlenen her kontrol en efektif veya en az maliyetli kontrol olmayabilir. Bir fizibilite çalışması yapılarak riski en aza indirecek en uygun kontrol belirlenmelidir. Bu aşamada kontroller için maliyet-fayda analizi yapmak uygun olacaktır.

3.3.3 Kontrollerin Seçilmesi

Fizibilite çalışmasının ve maliyet-fayda analizinin sonuçlarına göre riski en aza indirecek en uygun kontroller, risk analizinde belirlenen kontroller arasından yönetim tarafından seçilir. Seçilen kontroller teknik, yönetsel ve operasyonel kontrollerin bir araya getirilmesinden oluşturulmalıdır.

3.3.4 Sorumluların Atanması

Seçilen kontroller uygulanması için bu kontrolleri uygulama yetkinliğine sahip kişiler belirlenmeli ve bu kişilere sorumluluk atanmalıdır.

3.3.5 Kontrol Uygulama Planının Hazırlanması

Seçilen kontrolün nasıl uygulanacağını, uygulamanın hangi adımları içereceğini ve ne kadar süreceğini belirleyen bir kontrol uygulama planı oluşturulmalıdır. Bu plan en az:

- riskleri ve risk seviyelerini
- risk analizi sonucunda belirlenen kontrol önerilerini

- önceliklendirmeleri
- seçilen kontrolleri
- gerekli kaynakları
- kontrolü uygulamakla yetki ve sorumluluğu verilen kişileri
- kontrolün uygulanması için belirlenen başlama ve bitiş tarihlerini

içermelidir.

3.3.6 Seçilen Kontrolün Uygulanması

Hazırlanan kontrol uygulama planına uygun olarak seçilen kontroller uygulanmalıdır. Uygulanması uzun zaman alabilecek kontroller için uygulamanın gidişini değerlendirmek üzere uygun aralıklara toplantılar yapıp sonuçlar raporlanabilir.

3.4 Artık Risk

Uygulanan kontroller var olan riski tamamen ortadan kaldırmak zorunda değildir. Risk işleme sonrası kalan riske artık risk adı verilir. Uygulanan kontroller sonrası artık risk belirlenmelidir. Eğer bulunan risk seviyesi kabul edilebilir risk seviyesinin üzerinde ise risk analizi ve risk işleme tekrar yapılmalıdır, eğer bulunan artık risk seviyesi kabul edilebilir riskin altında ise artık risk dokümante edilmeli ve varlığı yönetim tarafından onaylanıp kabul edilmelidir.

4. DEĞERLENDİRME VE TAKİP

Risk yönetimi bir döngüdür ve burada belirtilen risk analizi ve risk işleme süreçleri periyodik olarak uygulanmalıdır. Bu sayede uygulanan kontrollerin amacına ne kadar ulaştığı belirlenmiş olur. Ayrıca bilişim teknolojileri çok hızlı değişmektedir. Kurum sistemine yeni dahil olan varlıkların risk yönetimine dahil edilmesi önem arz etmektedir. Bunlara ek olarak zaman içerisinde kurumun iş hedefleri, iş yapma şekli ve önem verdiği konular değişebilir. Bütün bu değişiklikler varlıklarda, varlıkların değerlerinde, açıklıklarda ve tehditlerde değişiklik olmasına neden olur. Risk yönetim döngüsünün sürekli olarak işletilmesi tüm bu değişikliklerin getirdiği risklerin yönetim tarafından farkına varılmasını ve ele alınmasını sağlayacaktır.

KAYNAKÇA

- [1]. TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler
- [2]. ISO/IEC 27002:2005 Information technology – Security techniques - Code of practice for information security management
- [3]. “The Security Risk Management Guide” , Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence
- [4]. ISO/IEC 13335-3 Information technology — Guidelines for the management of IT Security, Part 3: Techniques for the Management of IT Security
- [5]. NIST SP 800-30, Risk Management Guide for Information Technology Systems