MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

RİSK YÖNETİMİ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu doküman, Kapsam Analizi Dokümanı'nda belirtilen bilgi varlıklarının maruz kalabileceği risklerinin süreç bazında belirlenmesi, değerlendirilmesi ve önceliklendirilmesi amacı ile hazırlanmıştır.

2 Kapsam

Bu doküman, Kapsam Analizi Dokümanı'nda belirtilen birimlerde yer alan tüm bilgi varlıklarını kapsar.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
Birim BGYS Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/ Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
GBE	Gizlilik, Bütünlük, Erişilebilirlik
Gizlilik	Bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğidir.
Bütünlük	Varlıkların doğruluğunu ve tamlığını koruma özelliğidir.
Erişilebilirlik	Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir.

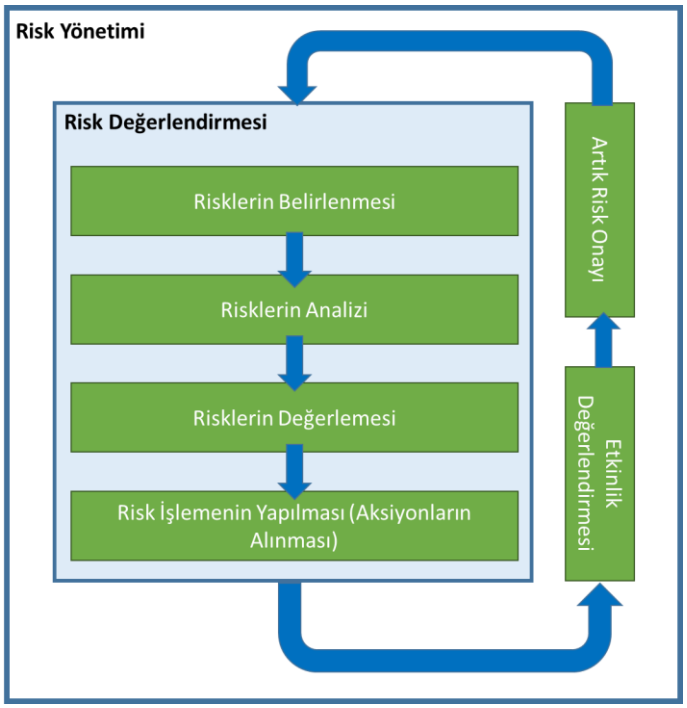
Terim	Tanım/ Açıklama
İş Etkisi	Bir varlığa ait gizlilik, bütünlük ve erişilebilirlik değerlerinin en büyüğüdür.
Risk	Bilgi ve bilgi işleme varlıklarının gizlilik, bütünlük ve erişilebilirlik bileşenlerine olumsuz etki edebilecek bir olayın sonuçlarının ve karşılık gelen olma ihtimalinin birleşimidir.
Risk Değerlendirmesi	Bilgi ve bilgi işleme varlıklarının gizlilik, bütünlük ve erişilebilirlik bileşenlerine etki edebilecek risklerin tanımlanması, analiz edilmesi ve değerlemesidir.
Risk Değerlemesi	Bilgi ve bilgi işleme varlıklarının gizlilik, bütünlük ve erişilebilirlik bileşenlerine etki edebilecek risklerin büyüklüğünün kabul edilebilir veya tahammül edilebilir olup olmadığını belirleme için risk analizi sonuçlarının risk kriterleri ile kıyaslanmasıdır.
Risk Tanımlama	Bilgi ve bilgi işleme varlıklarının gizlilik, bütünlük ve erişilebilirlik bileşenlerine etki edebilecek risklerin bulunması, tanınması ve açıklanması.
Risk İşleme Bilgileri	Gap analizi/ risk analizi sonucu risklerin minimuma indirilmesi, mevcuttaki politika, prosedür ve standartlara uyum sağlanabilmesi ve/veya denetim faaliyetleri sonucu tespit edilen bulguların düzeltilmesi amacı ile yapılacak işlemler/çalışmalardır.
Risk Yönetimi	Riskin tanımlanmasından artık risk kabulüne kadar gerçekleştirilen sistematik faaliyetlerin tümü.
Risk Analizi	Bilgi ve bilgi işleme varlıklarının gizlilik, bütünlük ve erişilebilirlik bileşenlerine etki edebilecek risklerin seviyesinin belirlenmesi.
Risk Sahibi	Bir riski yönetmek için sorumluluk ve yetki sahibi kişi veya birim.
CVSS	Genel Açık Derecelendirme Sistemi (CVSS, Common Vulnerability Scoring System), güvenlik açıklarının önem ve

Terim	Tanım/ Açıklama
	önceliklerinin belirlenmesi açısından risk seviyelerinin belirlenebilmesinde kullanılan açık bir standarttır.

5 İşlem Detayı

Bilgi Güvenliği Yönetim Sistemi kapsamında yapılan Risk Yönetimi Süreci, ISO 27001'in gereklilik şartları referans alınarak kurgulanmıştır ve Üst Yönetim Temsilcisi tarafından onaylanmış ortam ile uyumlu bir Risk Analizi Metodolojisi benimsenmiştir.

Kullanılan analiz metodu aşağıdaki şekilde belirtilmiştir:



Risk Yönetimi Süreci yılda en az bir kez ve önemli değişiklikler önerildiğinde veya meydana geldiğinde tekrar edilir.

Risk değerlendirme yapılırken kullanılan metodun detayları aşağıda açıklanmıştır.

6 Risk Değerlendirme

6.1 Risklerin Belirlenmesi

6.1.1 Bilgi Varlıklarının Tespiti

Kapsam Analizi Dokümanı'nda belirtilen birimlerle yapılacak toplantılar ve/veya birimlere gerçekleştirilerek ziyaretlerde birebir görüşme yöntemi ile "Varlık Yönetimi Prosedürü" ne uygun olarak bilgi varlıkları tespit edilir.

6.1.2 Teknik Risklerin Belirlenmesi

Zafiyet ve sızma testleri sonucunda teknik açıklar bulunur ve bunların sebep olabileceği riskler belirlenir.

6.1.3 Kavramsal Risklerin Belirlenmesi

Kapsam dâhilindeki birimlerde tespit edilen varlıklar üzerindeki risklerin belirlenmesi için, varlıklar ile eşleştirilmiş süreçlerin ISO 27001 standardının Ek-A kontrol maddelerine göre yeterlilikleri; varlık ve süreç sahipleri ile yapılan birebir görüşmeler ve gözlemler ile değerlendirilir. Gerek görülür ise Ek-A kontrol maddeleri haricinde yeni kontroller de belirlenebilir.

6.2 Risk Analizi

Risk belirleme aşamasında tespit edilen risklerin kök nedenlerinin belirlenmesi ve risk değerlendirme sonuçlarının geçerli ve karşılaştırılabilir sonuçlar üretmesinin sağlanması için risk puanlaması bu aşamada yapılmaktadır.

Risk puanı varlık değeri, olasılık ve etki değerlerinin çarpımı ile hesaplanır.

Risk Puanı = (Varlık Değeri) x (Olasılık) x (Etki)

6.2.1 Etki Derecesinin Hesaplanması

Etki değeri hesaplaması aşağıdaki şekilde gerçekleştirilir.

Puan	Seviye	Açıklama
5	**Çok Yüksek**	Kurumun çok ciddi itibar kaybına veya iş kaybına uğramasına, yasal yükümlülük altına girmesine, yüksek ek maliyetlerin doğmasına, çalışan motivasyonun iş kesintisine neden olacak şekilde etkilenmesine neden olabilecek durumlar. Ör: Kurumun sözleşme ile hüküm altına alınmış gizlilik ilkelerini ihlal etmesi, işlerini tamamen durmasına neden olacak bir kesinti
4	**Yüksek**	Kurumun yasal yükümlülük hariç itibar kaybı veya iş kaybına uğramasına, yüksek ek maliyetler doğmasına ya da çalışanların

Puan	Seviye	Açıklama
		motivasyonu üzerinde ciddi olumsuz etkiye yol açan durumlar Ör: Kritik iş uygulamalarının erişilebilirlik, bütünlük ve
3	**Orta**	İtibar kaybı ve yasal yükümlülük açısından bir zarara yol açmayan ancak iş kaybına, ek maliyetlerin doğmasına ya da çalışanların motivasyonu üzerinde bir miktar olumsuz etkiye yol açan durumlar Ör: E-posta sistemlerinde erişilebilirlik, bütünlük, gizliliği; İnternet erişilebilirliği; herhangi bir iş konusunda uzman
2	**Düşük**	İş, itibar kaybı, yasal yükümlülük ya da çalışanların morali açısından bir zarara yol açmayan ancak yapılan işi bir miktar etkileyen / gecikmesine neden olan durumlar Ör: Bir birime özgü ve kurumun asli fonksiyonlarına yönelik olmayan sistemlerin erişilebilirliği
1	**Çok Düşük**	İş, itibar kaybı, yasal yükümlülük ya da çalışanların morali açısından ciddi bir zarara yol açmayan ancak yapılan iş üzerinde az da olsa etkisi olabilecek / bir miktar gecikmeye neden olabilecek durumlar Ör: Bir çalışanın kişisel bilgisayarı gibi araçların erişilebilirliği

6.2.2 Olasılık Değerinin Belirlenmesi

Tespit edilen risklerin olasılık değerleri;

1. Teknik risklerde uluslararası standartlara uygun CVSS Score (v2) modeli temel alınarak,
2. Kavramsal risklerde ilk yıl tecrübelerden elde edilenler, sonraki yıllarda ise DİF, olay kayıtları, vb. kayıtlar dikkate alınarak belirlenir.

Olasılık değerlerinin ölçeği aşağıda verilmiştir:

Puan	Seviye	Açıklama
5	**Çok Yüksek**	• Risk kaynağı çok kabiliyetlidir. • Risk kaynağının motivasyonu çok yüksektir. • Riskin gerçekleşmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir.

Puan	Seviye	Açıklama
		• Ayda en az bir defa gerçekleşebilir.
4	**Yüksek**	• Risk kaynağı çok kabiliyetlidir. • Risk kaynağının motivasyonu çok yüksektir. • Riskin gerçekleşmesini engelleyecek kontroller yetersizdir. • Ayda bir defadan seyrek fakat en az üç ayda bir defa gerçekleşebilir.
3	**Orta**	• Risk kaynağı kabiliyetlidir. • Risk kaynağının motivasyonu yüksektir. • Riskin gerçekleşmesini engelleyecek mevcuttur. • Üç ayda bir defadan seyrek fakat en az altı ayda bir defa gerçekleşebilir.
2	**Düşük**	• Risk kaynağı kabiliyetsizdir. • Risk kaynağının motivasyonu yüksektir. • Riskin gerçekleşmesini engelleyecek veya zorlaştıracak kontroller mevcuttur. • Altı ayda bir defadan seyrek fakat en az yılda bir defa gerçekleşebilir.
1	**Çok Düşük**	• Risk kaynağı kabiliyetsizdir. • Risk kaynağı motivasyonsuzdur. • Riskin gerçekleşmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur. • Yılda bir defadan daha seyrek gerçekleşebilir.

6.3 Risklerin Değerlemesi

Hesaplanan risk puanlarının değerlemesi aşağıda yer alan tablodaki açıklamalara göre yapılır.

Risk Büyüklüğü (R)	Risk Derecesi	Değerlendirme	Renk
125-100	Çok Yüksek Risk	Acil Önlem Alınmalı	KIRMIZI
99-60	Yüksek Risk	Hemen Çalışma Yapılmalı	MOR
59-28	Dikkate Değer Risk	Mümkün Olduğunca Çabuk Müdahale Edilmeli	MAVİ
27-1	Kabul Edilebilir Risk	Acil Tedbir Gerektirmeyebilir, Dikkatli Olunmalı	SARI

Kabul edilebilir risk seviyesi 1-27 arası riskler olarak belirlenmiştir. Bununla birlikte Dikkate Değer seviyedeki bazı riskler için de yapılacak değerlendirme sonucunda kabul kararı verilebilir. Diğer tüm riskler için risk işleme gerçekleştirilmesi gerekir.

6.4 Risk İşlemenin Yapılması

Bu aşama, risk değerlendirme sırasında belirlenen risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek faaliyetlerin uygulanmasından oluşur.

Kurum, bilgi güvenliği risklerinin işlenmesi için öncellikle kabul edilebilir risk seviyesini belirler. Bu seviyenin üzerinde bulunan riskler için risk işleme yöntemlerini kullanır.

Risk sahibi, riski azaltmak istediğinde sisteme gelebilecek zararı en aza indirmek için "en uygun" kontrolü seçer. BGYS Yöneticisi risk sahip(ler)i tarafından yapılan çalışmaları gözden geçirir. Risk işleme ile ilgili rol ve sorumluluklar "Roller ve Sorumluluklar Kılavuzunda" tanımlanmıştır.

Bu süreçte planlanan kontrollerin uygulanıp/uygulanmadığı takip edilir. Riskler karşılığında tespit edilmiş kontroller başarılı bir şekilde tamamlandıysa onaylanarak Risk İşleme Planı sonucu belirlenen aksiyonlar doğrultusunda risk seviyesi güncellenebilir.

Aşağıda Risk İşleme Planı'nın hazırlanması amacıyla uygulanan adımlar ve metodolojiler detayları ile açıklanmaktadır.

6.4.1 Risk Kabul Kriterleri

Risk değerlendirmesi sırasında kurumun karşı karşıya olduğu riskler belirlenmektedir. Belirlenmiş olan risklerin tamamı için önlem almaya çalışmak hem mali açıdan, hem de zaman açısından uygun bir teknik değildir. Belirli bir seviyenin altındaki risklerin işlenmesi için

ayrılacak vakit ve mali kaynak kurumun kabul edemeyeceği seviyedeki riskler için alınacak tedbirlerin gecikmesine neden olabilir.

Bu nedenle kurum etkin bir risk işleme gerçekleştirebilmek amacıyla kabul edilebilir risk seviyesini belirler ve bu seviyenin altındaki riskleri kabul eder. Kabul edilebilir risk seviyesinin üzerindeki riskler için risk işleme yöntemleri kullanılır.

Kurum bünyesinde kullanılan risk yönetim metodolojisine uygun olarak kabul edilebilir risk seviyesinin aşağıda belirtilen riskler dışındaki tüm riskler için ***1-27*** arasında olduğu belirlenmiştir. Kabul edilebilir seviyenin altında kalan riskler için kurumun tercih etmesi halinde risk işleme yöntemleri uygulanabilir.

Bir riskin gerçekleşmesi neticesinde kurumun göreceği zararın maliyeti, riski ortadan kaldırmak için uygulanacak kontrolün maliyetinden düşük olduğu durumlarda önlem almak yerine risk kabul edilebilir. Aşağıdaki maddelerde belirtilen kriterler için de kurumsal bir önlem geliştirilmeyebilir ve riskler kabul edilebilir:

1. Paydaşlarımıza karşı yükümlülüklerimizi hiçbir şekilde etkilemeyecek iş kesintileri ve iç yetersizlikler,
2. Paydaşlarımız ve genel halk nazarında itibarımızı etkilemeyecek iş kesintileri ve tüm istenmeyen durumlar,
3. Çalışan aidiyetinin etkilenmediği, memnuniyetsizliklere sebep olabilecek kayıplar ve iç yetersizlikler,
4. Faaliyetleri aksatmayacak seviyede ve yasal uyumsuzluğa sebep olmayacak eksiklikler.

6.4.2 Risk İşleme Yöntemleri

Yöntem	Açıklama
Riskin Kabulü	Riskin var olduğunu kabul ederek sistemin kullanılmaya devam edilmesidir. Kurum yönetimi kabul edilebilir risk seviyesinden düşük riskleri doğrudan kabul eder ve bu riskler için gayret harcamaz. Risk kabulü için 6.4.1'de belirtilen kabul kriterleri kullanılır. Kurum yönetimi kabul edilen risklerini bilir ve riskin gerçekleşmesi durumunda kurumun göreceği zararın farkındadır. Kabul edilen riskler gözden geçirilir ve yönetim tarafından onaylanır. Kabul edilebilir risk seviyesinden

Yöntem	Açıklama
	yüksek olmasına rağmen kabul edilen riskler gözden geçirilir ve riski azaltıcı bir kontrol uygulama/ uygulamama konusunda karar verilir.
Riskin Azaltılması	Bu yöntem seçildiğinde riskin, mevcut seviyesinden kabul edilebilir risk seviyesine getirilmesi amaçlanır. Riskin azaltılması için uygulanan kontroller aşağıdaki şekildedir; **Önleyici kontroller**; hataların veya uygunsuzlukların oluşmasının önüne geçmek üzere alınan proaktif tedbirlerdir. **Tespit edici kontroller**; hataları ve uygunsuzlukları tespit etmek amacı ile kullanılan kontrollerdir. Bu kontroller yetkisiz veya istenmeyen olayların tespit edilmesi ve raporlanmasını sağlar. **Düzeltici kontroller**; hataların ve uygunsuzlukların oluştuktan sonra düzeltilmesi için kullanılan kontrollerdir. Bu kontroller bir güvenlik olayı meydana geldikten sonra çalışır ve uygunsuzluğun düzeltilmesini sağlar. Düzeltici kontroller aynı zamanda saldırıdan kaynaklanan hasarın veya etkinin sınırlandırılması için kullanılır. Birçok durumda düzeltici kontroller tespit edici kontroller tarafından uyarılarak çalıştırılır. **Telafi edici kontroller**; uygulanması gereken bir kontrolün herhangi bir sebeple gerçekleştirilememesi nedeni ile kullanılan ve riski hafifletici etki gösteren kontrollerdir. **Yönlendirici kontroller**; kurumun hassas bilgilerini korumak amacıyla yapılması gereken faaliyetlerin tanımlanmasıdır. Yönlendirici kontroller politika, prosedür ve talimat türünde kontrollerdir. **Caydırıcı kontroller**; güvenlik ihlallerinin önüne geçmek amacıyla kullanılırlar.
Riskten Kaçınma	Riskin bulunduğu sistemi kullanmaktan vazgeçerek riskten kaçınmak mümkündür. Bu yaklaşım sonucunda riski yaratan sebep ortadan kalkar. Riskten kaçınma seçeneği düşünülürken iş gereksinimleri ve güvenliğin sağlanması konusunda bir denge sağlanmalıdır. Kullanılmaması durumunda iş

Yöntem	Açıklama
	süreçlerinde ciddi değişiklikler getirecek ve/veya kurumun çalışmasını olumsuz etkileyecek şekilde riskten kaçınma metodu uygulanmamalıdır.
Riskin Transferi	Riskin kabul edilebilir risk seviyesinin altına düşürülmesi mümkün olmadığında veya bunu gerçekleştirmek için gereken kontrollerin uygulanması yüksek maliyet gerektirdiğinde, riskin sigorta gibi başka bir organizasyona transferi ele alınır. Riskin transferi için kullanılan bir diğer yol üçüncü parti firma veya dış kaynak kullanımıdır. Bu yöntem tercih edildiğinde güvenlik ihtiyaçlarının, kontrol hedeflerinin ve ilgili kontrollerin sözleşmelerde yer almasına dikkat edilir.

Riskin azaltılması amacıyla uygulanan kontroller riski tamamen ortadan kaldırmaz, kabul edilebilir seviyenin altına inmesi için puanını düşürücü etkide bulunur. Alınan aksiyonlar/kontroller sonrasında kalan ve yönetilemeyen, yönetim tarafından risk seviyesinin daha fazla düşürmek için alınabilecek aksiyon bulunmayan veya risk seviyesi kabul edilebilir seviyeye çekilemeyen riskler artık risk olarak değerlendirilir.

6.5 Risk İşleme Yaklaşımı

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

Risklerin Önceliklendirilmesi: Risk değerlemesinde belirlenen risk seviyelerine göre riskler önceliklendirilir. Risk işleme için kaynak aktarımı yapılırken öncelik yüksek seviyeli risklere, aynı seviyedeki riskler için ise öncelik olasılık değeri yüksek olan risklere verilir, bu riski oluşturan zafiyetler ve tehditlere karşı kontroller daha önce uygulanır.

Risk Seviyesi	Açıklama
125-100	Acil Öncelikli Risk
99-60	Yüksek Öncelikli Risk
59-28	Orta Öncelikli Risk
27-1	Düşük Öncelikli Risk

Uygun Kontrollerin Değerlendirilmesi: Riskler önceliklendirildikten sonra bu riskler için daha önceden belirlenmiş kontroller değerlendirilir. Belirlenen her kontrol en efektif veya en az maliyetli kontrol olmayabilir. Bir fizibilite çalışması yapılarak riski en aza indirecek en uygun kontrol belirlenir. Bu aşamada kontroller için fayda-maliyet analizi yapılmalıdır.

Kontrollerin Seçilmesi: Fizibilite çalışmasının ve fayda-maliyet analizinin sonuçlarına göre riski en aza indirecek uygun kontroller, risk değerlendirmesinde belirlenen kontrol önerileri arasından yönetim tarafından seçilir.

Sorumluların Atanması: Seçilen kontrollerin uygulanması için, bu kontrolleri gerçekleştirebilecek yetkinliğe sahip kişiler belirlenir ve bu kişilere sorumluluk atanır.

Risk İşleme Planının Hazırlanması: Seçilen kontrolün nasıl uygulanacağını, uygulamanın hangi adımları içereceğini ve ne kadar süreceğini belirleyen bir risk işleme planı oluşturulur. Planlama sırasında kısa sürede gerçekleştirilebilecek ve seviyesi yüksek olan riskleri kabul edilebilir seviyeye çekecek kontrollere öncelik verilir.

Risk İşleme planı en az:

1. Riskin tanımı,
2. Riskin etkilediği süreç,
3. Risk puanı,
4. Risk işleme kararı,
5. Kontrol önerilerini,
6. Önceliklendirmelerini,
7. Kontrolü gerçekleştirecek kişi veya grubu,
8. Kontrolün gerçekleştirilmesi için tahmini bitiş süresini,
9. Kontrolün tamamlandığı tarihi ve
10. Kontrol sonrasındaki yeni risk puanını içerir.

Seçilen Kontrolün Uygulanması: Hazırlanan risk işleme planına uygun olarak seçilen kontroller uygulanır. Uygulanması uzun zaman alabilecek kontroller için uygulamanın gidişini değerlendirmek üzere uygun aralıklara toplantılar yapılıp sonuçlar yönetime raporlanır. Risk yönetimi adımlarına dair bilgiler süreçlerin istenildiği gibi yürüdüğünden emin oluncaya kadar yazılı (elektronik veya basılı doküman) bilgi olarak saklanır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					