RİSK YÖNETİM PROSEDÜRÜ

1. AMAÇ

Bu prosedürün amacı, Bilgi İşlem Daire Başkanlığı Bilgi Güvenliği Yönetim Sistemi kapsamında iş sürekliliği açısından varlık değeri olan iş bileşenlerine iç veya dış kaynaklı olarak gelebilecek tehlikeler ve bu tehlikelerin vuku bulması durumunda ortaya çıkabilecek maddi veya manevi iş kayıplarını tespit edecek yöntemler ve gerekli önlemlerin planlanması için izlenecek yolu belirlemektir.

1.1. Varlıkların Belirlenmesi

Bilgi Güvenliği Yönetim Sistemi kapsamındaki faaliyetlerin gerçekleştirilmesi ve iş sürekliliği için gerekli olan tüm varlıklar KTÜ varlıklarını oluşturur. Bu varlıklar kulanım amaçları, işe etkileri, konumları itibarı ile zayıflıklara karşı tehdit altında olabilirler. KTÜ 'da varlıklar **Varlık Belirleme, Sınıflandırma ve Etiketleme Talimatına** göre yapılır.

1.2. Varlıkların Değerlendirilmesi

1.2.1. Kuruluş içerisindeki tüm varlıklar Varlık envanterinde belirtilir. Varlıkların keşfi yapılırken her türlü iç ve dış kaynaklı tehditler düşünülür. Bunun için **Tehdit Listesi** kullanılır.

1.2.2. Belirlenen tehditlerin hangi zayıflıklardan kaynaklanabileceği tespit edilir. Kuruluşumuzun yapısı ve iş süreçlerinin gereği olarak ortaya çıkan zayıflıklar **Zayıflık Listesi** ile belirlenir.

1.2.3. Varlık değeri belirlenirken Bilgi Güvenliği Yönetim Sisteminin temeli olan *Gizlilik, Bütünlük* ve *Erişilebilirlik* açısından değerlendirme yapılır. Bu değerlendirme aşağıdaki yöntem ile belirlenir ve 3 Aylık periyodlarda gözden geçirilmesi sağlanır.

Gizlilik Etki Seviyeleri (G)

VARLIĞIN GİZLİLİK DERECESİ		
Çok Yüksek	5	Çok Gizli Bilgileri içeren varlık.
Yüksek	4	Gizli Bilgiler içeren bir varlık.
Orta	3	Şirket personelinden ilgili personelin bu bilgilere sahip olabileceği varlık.
Düşük	2	Tedarikçi ve taşeronların bilebileceği ya da ziyaretçilerle paylaşılması sıkıntı olmayacak bilgi varlıkları.
Çok Düşük	1	Halkın bilgisi dâhilinde olabilecek veya herkesle paylaşılabilecek seviyedeki bilgi varlığı.

Bütünlük Etki Seviyeleri (B)

VARLIĞIN BÜTÜNLÜK DERECESİ		
Çok Yüksek	5	Bilginin %100 bütün halinde ulaşılması gereken bilgi varlığı.
Yüksek	4	Bilgi bütünlüğünde yaşanan aksaklığın kuruluşumuza etki ettiği, işin durmasına, işin aksamasına veya itibar kaybına sebep olan bilgi varlıkları.
Orta	3	Bilgi bütünlüğünde yaşanan aksaklığın kuruluşumuza kısmen etki ettiği, işin gecikmesine sebep olabilecek fakat kritik seviyede etki etmeyecek bilgi varlıkları.
Düşük	2	Bilgi bütünlüğünün olmaması sonucu kuruluşa etki etmeyen fakat başka varlıklarla ikame edilebilecek bilgi varlıkları.
Çok Düşük	1	Bilginin bütünlüğü önemli olmayan varlıklar.

Erişilebilirlik Etki Seviyeleri (E)

VARLIĞIN ERİŞİLEBİLİRLİK DERECESİ		
Çok Yüksek	5	Bilgiye %100 erişilmesi gerekli bilgi varlıkları.
Yüksek	4	Bilgiye erişilemediğinde yaşanan aksaklığın kuruluşumuza etki ettiği, işin durmasına, işin aksamasına veya itibar kaybına sebep olan bilgi varlıkları.
Orta	3	Bilgiye erişimde yaşanan aksaklığın kuruluşumuza kısmen etki ettiği, işin gecikmesine sebep olabilecek fakat kritik seviyede etki etmeyecek bilgi varlıkları
Düşük	2	Bilgiye erişimin olmaması sonucu kuruluşa etki etmeyen fakat başka varlıklarla ikame edilebilecek bilgi varlıkları.
Çok Düşük	1	Bilgi erişiminin önemli olmadığı varlıklar.

Varlık değer aralığı aşağıdaki formülle belirlenir.

VARLIK DEĞER ARALIĞI = Ort (G x B x E)

Varlık değeri hesaplanan varlıklar aşağıdaki tabloda verilen değer aralıklarından hangi aralığa ait ise varlık değeri 1 ile 5 arasında seçilerek risk hesaplaması yapılır.

VARLIK SINIFI	VARLIK DEĞERİ (V)
Çok Kritik	5
Kritik	4
İç kullanım	3
Halka açık	2
Önemsiz Bilgi	1

1.3. Risk Analiz Metodolojisi

Belirlenen tüm bilgi varlıkları için tehditler, zayıflıklar, var olan kontroller ile önerilen kontrollerin bu formda yazılması istenir. Toplanan verilerde her bir varlık için tanımlanan tehditlerin ortalaması alınarak o varlık için belirtilen ve BGYS Ekibi tarafından onaylanan iş etki değeri ile çarpılır ve Varlık Listesi formundaki Risk Değeri bölümüne çıkan puan işlenir.

Varlıkların özellikleri olabildiğince detaylı yazılır. Varlığın bulunduğu yer (lokasyon olarak tam adres) bu formda belirtilir.

Her bir varlık için varlık bilgisi veya varlık keşif formlarından gelen tehditler ve zayıflıkların ortalaması alınarak hesaba dâhil edilir. Kontrol seçiminde ise her varlığın karşılaştığı tehditler tek tek göz önüne alınır. Puanlamada çıkan değer ve derecelendirme yüksek risklere öncelikli müdahale için kullanılmaktadır.

Açıklıkların kapatılması için varlıkların üzerlerindeki tehditler ve standardın öngördüğü kontroller risk işleme için öncelikle dikkate alınır.

1.4. Risk Değerlendirme Metodolojisi

İş etkisi değerlendirilirken varlığın iş üzerindeki kesinti etkisi, yerine koyma maliyeti, bilginin gizliliği, imaja olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zarar (personele ait bilgi gibi) konuları ele alınmalıdır.

Olasılık aralığı tespit edilirken zayıflıkların çokluğu ve var olan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, tehdit biçiminin uygulanma kolaylığı, bilginin rakipler için cazibesi, personelin psikolojisi, uygulamanın hassas ve kontrol edilemeyen (politikaya uymama-kuralın etrafından dolaşma) çalışan davranışı gibi unsurlar değerlendirilmelidir.

RİSK BÜYÜKLÜĞÜNÜN HESAPLANMASI

Olasılık Dereceleri (O)

OLASILIK DERECESİ		
Ayda bir	5	Olması kesin veya sık sık gerçekleşmiş.
Üç ayda bir	4	Olması oldukça muhtemel veya zaman zaman gerçekleşmiş.
Altı ayda bir	3	Olması muhtemel veya seyrek olarak gerçekleşmiş.
Yılda bir	2	Olması muhtemel değil.
Yılda bir den daha az	1	İmkânsız veya olması hiç muhtemel değil.

Etki Dereceleri

Etki dereceleri üç boyutta değerlendirilir. Bu üç boyut finansal, operasyonel ve itibar etkileridir. Belirlenen üç etki boyutuna ilişkin kullanılan ölçütler ve derecelendirme seviyelerinin açıklamaları aşağıda listelenmiştir.

Gizlilik Etki Boyutu

GİZLİLİK ETKİ DERECESİ		
Çok Yüksek	5	Kuruluşta gizlilik açısından çok yüksek tehdit oluşturmaktadır. Kurum itibarını, iş kaybını ve iş sürekliliğini ciddi ölçüde etkilemektedir.
Yüksek	4	Kuruluşta gizlilik açısından yüksek tehdit oluşturmaktadır. Kurum itibarını ve iş sürekliliğini ciddi ölçüde etkilemektedir.
Orta	3	Kuruluşta gizlilik açısından tehdit oluşturmaktadır. İş sürekliliğini etkilemektedir.
Düşük	2	Kuruluşta gizlilik açısından düşük tehdit oluşturmaktadır.
Çok Düşük	1	Kuruluşta gizlilik açısından tehdit oluşturmamaktadır.

Bütünlük Etki Boyutu

BÜTÜNLÜK ETKİ DERECESİ		
Çok Yüksek	5	Kuruluşta bütünlük açısından çok yüksek tehdit oluşturmaktadır. Kurum itibarını, iş kaybını ve iş sürekliliğini ciddi ölçüde etkilemektedir.
Yüksek	4	Kuruluşta bütünlük açısından yüksek tehdit oluşturmaktadır. Kurum itibarını ve iş sürekliliğini ciddi ölçüde etkilemektedir.
Orta	3	Kuruluşta bütünlük açısından tehdit oluşturmaktadır. İş sürekliliğini etkilemektedir.
Düşük	2	Kuruluşta bütünlük açısından düşük tehdit oluşturmaktadır.
Çok Düşük	1	Kuruluşta bütünlük açısından tehdit oluşturmamaktadır.

Erişebilirlik Etki Boyutu

ERİŞEBİLİRLİK ETKİ DERECESİ		
Çok Yüksek	5	Kuruluşta erişilebilirlik açısından çok yüksek tehdit oluşturmaktadır. Kurum itibarını, iş kaybını ve iş sürekliliğini ciddi ölçüde etkilemektedir.
Yüksek	4	Kuruluşta erişilebilirlik açısından yüksek tehdit oluşturmaktadır. Kurum itibarını ve iş sürekliliğini ciddi ölçüde etkilemektedir.
Orta	3	Kuruluşta erişilebilirlik açısından tehdit oluşturmaktadır. İş sürekliliğini etkilemektedir.
Düşük	2	Kuruluşta erişilebilirlik açısından düşük tehdit oluşturmaktadır.
Çok Düşük	1	Kuruluşta erişilebilirlik açısından tehdit oluşturmamaktadır.

Etki değer aralığı aşağıdaki formülle belirlenir.

ETKİ DEĞER ARALIĞI = ORT (GxBxE)

Risk Derecesi (R) = V x O x E

V: Varlık Değeri **O:** Olasılık Değeri **E:** Etki Değeri

RİSK ETKİ BÜYÜKLÜKLERİNİN SINIFLANDIRILMASI VE DEĞERLENDİRİLMESİ

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

Bulunan iş etki değeri ile risk puanı yüksek orta ve düşük seviyelerde **Risk Değerlendirme Tablosu** üzerinde ilgili aralıkta puanlanır. Kabul edilebilir risk seviyesinden yukarı çıkması durumunda önleyici tedbirler alınarak yeniden risk değerlendirmesi yapılır ve kabul edilebilir risk seviyesine düşürülür. Kabul edilebilir risk seviyesine çekilemeyen riskler artık risk olarak değerlendirilir ve artık risk onayıyla firma yetkilisi tarafından onaylanır.

1.5. Risk İşleme Metodolojisi

Risk değerlendirme sonucunda tüm varlıklarla ilgili risk değerleri tespit edilir. Bu değerlendirme sürekli olarak yapısal, organizasyonel ve uygulama değişiklikleri çerçevesinde izlenir ve değişken risk sürekli yeniden hesaplanır. Risk işleme seçenekleri şunlardır: Risk kabul, riskten kaçınma, riski azaltma ve kontrol etme, riski yok etme, riskin transferi.

Kabul edilebilir risk seviyesi yönetim tarafından 1-27 puan arası riskler olarak tanımlanmıştır. Tüm varlıklar için hedefimiz riskleri bu seviyeye çekmektir.
Aksi belirtilmedikçe bütün risklerin azaltılması ve kontrol edilmesi birincil aksiyondur.
Bazı riskler bu seviyeye çekilemediğinde bunların göze alınması ve riskin kabulü yönetim tarafından yapılabilir.
Uygulama düzeyinde riski azaltamadığımız ve yönetimce kabul edilemez riskler için riskten kaçınma opsiyonu geçerlidir. Riske neden olan uygulamadan vazgeçilmesi ve iş sürecinin ve prosedürünün farklılaştırılması risk işleme seçeneklerinden biridir.

Riskin kuruluşumuz kontrollerini aştığı durumlarda (yangın, deprem, sabotaj, afet, soygun vb.) emniyet güçleri, kamu acil durum kurumları, sigorta kurumlarına risk transfer edilir.
Risk işlemede birincil aksiyon kontrollerin seçilmesidir. Kontroller; uygulayıcısının ve bu uygulamayı izleyip ölçecek ilgili amirin görüşlerinin alınması, konuyla ilgili teknik iç-dış

uzmanların ve danışmanların görüşlerinin alınması ile seçilir. Seçilen kontroller ISO 27001 Standardının EK-A bölümündeki 18 başlıktan ve 114 alt maddeden seçilmeye çalışılır. Burada kontrol amaçları ve kontrollerin ifadesi yer alır. Bu kontrollerin teknik düzeyde nasıl uygulanacağı konu uzmanları ve kontrolü uygulayacak kişilerin seçimiyle oluşturulur. Seçilen en uygun kontrolün maliyeti tespit edilir ve riski azaltılacak varlıkla ilgili yapılan varlık değerlemesi ve iş etkisinden dolayı potansiyel mali zararla kıyaslaması yapılır. Maliyet fayda analizi sonucu seçilen kontrolün uygulanabilir (feasible) olup olmadığına karar verilir. Uygulanabilir kontroller hayata geçirilir. Uygulanabilir olmayan kontroller için tekrar gözden geçirme yapılarak maliyet fayda dengesi sağlanana kadar araştırma süreci devam eder.

Uygulanan kontrol ile ilgili kayıtlar risk işleme planında belirtilir. Maliyetler ve alınan sonuçlar BGYS forumlarında görüşülür ve riskin yeni durumda ölçüm sonucu risk işleme planındaki ilgili yere yazılır.

Risk puanı kabul edilebilir seviyeye çekilene kadar gerekiyorsa yeni kontroller uygulanır ve ölçümlere devam edilir.