1- AMAÇ

Bu prosedürün amacı, Bilgi Güvenliği Yönetim Sistemi dahilinde yapılan Risk Değerlendirmesi ve Risk Analizi faaliyetlerinin belirlenmesidir

2- KAPSAM

Tüm Bilgi Güvenliği varlıklarını ve onlara yönelik riskleri kapsar

3- SORUMLULUK

Bu prosedürün uygulanmasından Bilgi Güvenliği Ekibi başta olmak üzere tüm personel sorumludur

4- UYGULAMA

4.1. Tehditlerin ve Zayıflıkların Belirlenmesi

4.1.1 Varlık Listesi üzerinde bulunan tüm varlık grupları için varlıkların üzerindeki tehdit ve varlıklara ait zayıflıklar belirlenir. Belirlenen Tehdit Listesi ve (PR.09 FR.02) Zayıflıklar Listesi'ne (PR.09 FR.03) eklenir.

4.1.2 Tehditler belirlendikten sonra her tehdit için tehdidin gerçekleşme ihtimali, Gerçekleştiği zaman kuruma verebileceği zarar (İş Etkisi) ve gerçekleştiğinin , risk değerlendirmesi 1,2,3 rakam sınıflandırması ile sınıflandırma yaparak anlaşılma olasılığı üzerinden bir risk değerlendirmesi yapılır

4.1.3 Yeni bir tehdit belirlendiğinde tehdit belirleyen personel (PR.09 FR.05) Risk Sahibi Onayı Formu ile ilgili tehdidi (Riski) Bilgi Güvenliği Ekip Lideri'ne bildirir.

4.2 Risk Metodolojisi

BGYS' yi etkileyen bütün alanlarda riskler analiz edilerek alınacak tavır belirlenir.

Bunun için Risk Analizi ve Varlık Envanteri formu kullanılır.

Formun üzerinde yer alan tanımlamalar ayrıca bir talimata gerek bırakmayacak şekilde hazırlanmıştır.

Form üzerinde, Muhtemel Tehlike, Sahibi, Varlık Grubu, Varlık Değeri, Tehdidin olasılığı, Şiddet, Şiddetin gizlilik, bütünlük ve erişebilirliğe etkisi, Risk Büyüklüğü, Toplam Risk, Risk Derecesi, Risk İşleme Planı kısmında (Önlem Alındıktan sonra) ise Riski Azaltmak İçin Önleyici Faaliyet, Maliyet, Planlanan Tarih, Tamamlanma Durumu, Tehdidin olasılığı, Şiddet, Şiddetin gizlilik, bütünlük ve erişebilirliğe etkisi, Risk Büyüklüğü, Toplam Risk, Risk Derecesi ve Durum bölümleri belirlenmiş olup sayısal olarak tanımları da formun yan Sheet lerinde yer almaktadır.

Öngörülen risklerin kabul edilebilir düzeyde tutulabilmesi için alınması gereken önlemler belirlenir e fırsat durumu belirlenir.

Varlık kavramı için örnekler:

a) Bilgi varlıkları: Kurumun tüm bilgi sistemlerinde, çalışanlarında, tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir;

b) Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları;

c) Fiziksel varlıklar: Bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar,

modemler, sunucular, switchler), manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri), mobilya, yerleşim düzeni;

d) Servisler (Hizmetler): Bilgi işleme ve haberleşme servisleri (web servisi, ftp servisi), genel faydalar; örneğin ısınma, ışıklandırma, elektrik, havalandırma. v.b.

e) İnsan: Personel, Tedarikçiler v.b.

Olarak sınıflandırılır.

Bilgi Güvenliği Komitesi, belli bir riskin yönetiminde gereken kabul edilebilir risk derecelerini değerlendirirken aşağıdaki hususları dikkate alır:

Varlık Değeri: Varlıklara kurum içerisindeki kritiklik derecesine göre 1 ile 3 arasında bir değer verilir. Varlık için belirlenen tehdidin olma olasılığı belirlenir.

Olasılık: Tehdidin olma olasılığı belirlenir. (Bkz. Tablo – 1)

Şiddet: Tehdidin varlıklar üzerinde gizlilik, bütünlük ve erişebilirliğine ne kadar etkisi olduğu 1 ile 5 arasında bir değer girilerek belirlenir. (Bkz. Tablo 2)

Risk Büyüklüğü: Gizlilik, bütünlük ve erişebilirlik sütunlarından oluşur. Tehdidin Olma olasılığı ve Gizlilik, bütünlük ve erişebilirlik değerlerinin tek tek çarpılmasıyla belirlenir.

Toplam Risk: Ortaya çıkan Risk Büyüklüklerinin toplamı ile Varlık değerinin çarpılmasıyla elde edilir. (Risk Değerlendirme Formu (PR.09-FR.01) üzerinde formüllendirilmiştir.)

**RİSKLER YILDA 1GÖZDEN GEÇİRİLİR.

BİR OLAYIN GERÇEKLEŞME OLASILIĞI	
OLASILIK	**DERECELENDİRME BASAMAKLARI**

1	ÇOK KÜÇÜK	HEMEN HEMEN HİÇ
2	KÜÇÜK	ÇOK AZ (YILDA 1 KEZ), SADECE ANORMAL DURUMLARDA
3	ORTA	AZ (YILDA BİR KAÇ KEZ)
4	YÜKSEK	SIKLIKLA (AYDA BİR)
5	ÇOK YÜKSEK	ÇOK SIKLIKLA (HERGÜN, HAFTADA BİR) NORMAL ÇALIŞMA ŞARTLARINDA

Tablo – 1

ŞİDDET TABLOSU		
1	ÇOK HAFİF	İŞ SAATİ KAYBI YOK
2	HAFİF	İŞ GÜNÜ KAYBI YOK, KALICI ETKİSİ OLMAYAN
3	ORTA	KAYBI ORTA SEVİYEDE OLUP, MÜDAHALE GEREKTİREN
4	CİDDİ	İŞ SÜREKLİLİĞİNİ ETKİLEYECEK, MÜDAHALE GEREKTİREN
5	ÇOK CİDDİ	İŞ SÜREKLİLİĞİNİ CİDDİ AÇIDAN ETKİLEYECEK

Tablo – 2

Risk Metodolojisi: Risk Analiz Metodolojisinde ;

TOPLAM RİSK = Varlık Değeri * Olasılık*Risk Büyüklüğü Toplamı formülü kullanılır.

Bu formüle göre teorik olarak elde edilebilecek en yüksek değer 225 puandır. {3*[5*(5+5+5)]}

Mevcut risk analiz çalışmaları neticesinde maksimum kabul edilebilir risk puanı 71 olarak belirlenmiştir.(Bkz. Tablo – 3 ve Tablo - 4)

İndirgenmiş risk puanının, kabul edilebilir seviye olan 71 puanın üzerine çıkması halinde (Bilgi Güvenliği Ekip Lideri tarafından üst yönetime risk durumu (Bilgi İşlem Daire Başkanı) e-mail ile bildirilir.

Üst yönetim ile yapılacak değerlendirme neticesinde; risk üst yönetim tarafından kabul edilir ve gerekli iyileştirme çalışmalarının başlatılması için onay verilir. Onay verilmesi halinde, ilgili varlık sahibi bölüm yönetimi öncülüğünde iyileştirici faaliyetler planlanarak hayata geçirilir.

İyileştirici faaliyet neticesinde risk değerlendirmesi tekrarlanır. Söz konusu risk puanın kabul edilebilir seviyenin üzerinde kalması durumunda aynı süreç tekrarlanır.

Risk analizi sonucunda aynı varlık için, farklı tehditlere karşın farklı risk puanları oluşabilir. Dolayısıyla risk analizi sonucunda hangi varlığın ne kadar korunacağı değil, hangi varlığın, hangi tehdit karşısında ne kadar korunacağına dair sonuçlar oluşturulur.

RİSK MATRİSİ

OLASILIK	ÇOK CİDDİ 5	CİDDİ 4	ORTA 3	HAFİF 2	ÇOK HAFİF 1
ÇOK YÜKSEK 5	YÜKSEK 225	YÜKSEK 180	YÜKSEK 135	ORTA 90	DÜŞÜK 45
YÜKSEK 4	YÜKSEK 180	YÜKSEK 144	ORTA 108	ORTA 72	DÜŞÜK 36
ORTA 3	YÜKSEK 135	ORTA 108	ORTA 81	DÜŞÜK 54	DÜŞÜK 27
KÜÇÜK 2	ORTA 90	ORTA 72	DÜŞÜK 54	DÜŞÜK 36	DÜŞÜK 18
ÇOK KÜÇÜK 1	DÜŞÜK 45	DÜŞÜK 36	DÜŞÜK 27	DÜŞÜK 18	DÜŞÜK 3

Tablo – 3

SONUÇ	EYLEM
135-225	KABUL EDİLEMEZ RİSK Bu risklerle ilgili hemen çalışma yapılmalı
72-134	DİKKATE DEĞER RİSK

	Risklere mümkün olduğunca çabuk müdahale edilmeli
3-71	**KABUL EDİLEBİLİR RİSK Acil tedbir gerekmeyebilir**

Tablo - 4

4.3 Artık Risk

Risk analizi tamamlandıktan sonra fark edilen ve değerlendirilmemiş riskler artık risk olarak değerlendirilir. Artık riskler (PR.09 FR.05) Risk Sahibi Onayı Formu ile bildirilir ve eğer risk gerçekten var ise risk işleme tablosuna eklenerek risk işleme tablosu revize edilir.

4.4 Risk Analizi

Bilgi varlıkların karşılaşabilecekleri risklerin değerlendirildiği, bu risklerin kabul edilebilir düzeyde tutulması için alınması gereken önlemlerin değerlendirildiği çalışmalar "Risk Analizi" olarak adlandırılır.

Risk analizleri Bilgi Güvenliği Ekip Lideri tarafından gerçekleştirilir.

Risk analizi; BGYS kapsamındaki varlıklar, bu varlıkların sahipleri, bu varlıklara yönelik tehditler, bu tehditler tarafından suiistimal edilebilecek zayıflıklar, gizlilik, bütünlük ve kullanılabilirlik kaybının varlıklar üzerinde oluşturabileceği etkiler değerlendirilerek yapılır.

Öngörülen risklerin kabul edilebilir düzeyde tutulabilmesi için alınması gereken önlemler belirlenir.

Risk analizleri, Bilgi Güvenliği Ekibi Toplantıları kapsamında ele alınır.

Varlık
Kurumun kurumsal müşterilerine sağlamak ile yükümlü olduğu iş süreçlerinin uygun ve kesintisiz olarak yerine getirilebilmesi için kullanılan varlıklar bilgi varlığı olarak ele alınır. Yokluğu veya olumsuz etkilenmesi durumunda hizmeti maddi olarak etkileyecek varlıklar risk analizinde değerlendirilir.
Varlık Sınıflandırması;

- **Bilgi varlıkları:** Veritabanları, veri dosyaları, sistem dokümanları, operasyon ve destek süreçleri, eğitim materyalleri vb.
- **Kağıt dokümanlar:** Kontratlar, kurum dokümanları, kritik bilgiler içeren dokümanlar vb.
- **Yazılım varlıkları:** Uygulama yazılımları, sistem yazılımları vb.
- **Fiziksel varlıklar:** Bilgi işlem ekipmanları, manyetik ortamlar, diğer teknik teçhizat, mobilyalar, fiziksel iş ortamları vb.
- **İnsanlar:** Personel
- **Kurum imaj ve itibarı:** Ticari itibar, marka değeri vb.
- **Servisler:** Bilişim hizmetleri, diğer teknik servisler vb.

Olarak sınıflandırılır.

Varlıkların "sahipleri" o varlıklar üzerinde erişim, kullanım yetkilerini belirleme yetkisine birinci dereceden sahip olan ilgili bölüm yöneticileridir. Sahipler, sahipleri oldukları varlıkların tehditlere karşı korunması süreçlerinden

birinci derecede sorumludur. Sahipler, o varlıkların değerlerinin belirlenmesi sürecinde de en etkili / doğru veriyi sağlayabilen ilgili yöneticilerdir.
Varlıkların sahipleri risk analizi tablosunda belirtilir. Sahiplere ilave olarak, varlıkların bakım ve korunmasından sorumlu kılınan "emanetçiler" ve bu varlıkları kullanarak iş gören "kullanıcılar" da tanımlanabilir.

Örneğin; Server'ların sahibi Bilgi ve İletişim Teknolojileri'dir

Karar alma sürecinde önemli olabilecek tüm bilgileri Bilgi Güvenliği Komitesine sunmak tüm Kurum çalışanlarının görevidir.

Bir bilgide gizlilik, doğruluk veya kullanılabilirlik anlamında tüm riskleri tamamen ortadan kaldırmak nadiren mümkündür (ya da uygulanabilir).Kurumun verimli ve ekonomik faaliyet göstermesi gereklidir ve bu yüzden iş süreçlerini etkileyebilecek veya Kurum bilgilerini tehlikeye atacak bir olayın olasılığına karşı alınacak güvenlik önlemlerinin zaman ve maliyet sonuçlarını dengeleyen yönetim kararları verilmektedir.

Bu konuda nihai karar, üst yönetimin tam yetki ile yetkilendirdiği Bilgi Güvenliğinden Sorumlu Yönetici (Bilgi Güvenliği Ekip Lideri) tarafından verilir.

Bilgi Güvenliği Ekip Lideri, belli bir riskin yönetiminde gereken kabul edilebilir risk derecelerini değerlendirirken aşağıdaki hususları dikkate alır:

Varlıklar, gizlilik, bütünlük, kullanılabilirlik (G,B,K) bakımından değerlendirilerek derecelendirilir. Her varlığın gizlilik, bütünlük ve kullanılabilirlik değerleri 5'li skalalar baz alınarak ayrı ayrı değerlendirilir. Varlığın nihai değerini belirleyen, gizlilik, bütünlük, kullanılabilirlik değerlerinin çarpanıdır.

Gizlilik: Birim açısından hassas olan bilgilerin, yetkisi olmayanların görmesinin engellenmesi, gizliliğinin sağlanması.

Bütünlük: Yönetim ve işletme süreçleri için kritik bilginin doğru ve eksiksiz olmasının sağlanması.

Kullanılabilirlik: Süreçlerin kesintisiz ve etkili biçimde devamı için kritik bilginin ihtiyaç anında kullanılabilirliği.

1: İhmal edilebilir
2: Düşük
3: Orta
4: Yüksek
5: Çok yüksek

	GİZLİLİK	BÜTÜNLÜK	KULLANILABİLİRLİK
5	Gizliliği ortadan kalkınca kurumun faaliyetlerini	Bütünlüğü ortadan kalkınca yerine konamaz. Kurumun	Erişilememesi en çok 60 dk. tolere edilebilir.

	tamamen sona erdirir. Kurum yasal yaptırımlara maruz kalır, kuurumun ticari itibarı çok ağır derecede zedelenir.	faaliyetlerini durdurur.	
4	Gizliliği ortadan kalkınca kurumun ticari itibarı ciddi derecede zedelenir. Ciddi oranda maddi zarar oluşur, kurumun faaliyetlerini geçici olarak uzun süreli kesintiye uğratır. Büyük oranda müşteri kaybı yaşanır	Bütünlüğü ortadan kalkınca kurumun faaliyetleri geçici olarak kesintiye uğrar, önemli maddi kayıp yaşanabilir, bilgi kayıpları olabilir, yerine konması uzun zaman alabilir.	Erişilememesi 6 saate kadar tolere edilebilir.
3	Gizliliği ortadan kalkınca kurumun imajı zedelenebilir, orta derecede maddi zarar oluşur, müşteri kaybı olmaz.	Bütünlüğü ortadan kalkınca maddi kayıp yaşanır. Yerine konması için kaynak harcanması gerekebilir.	Erişilememesi 12 saate kadar tolere edilebilir.
2	Gizliliği ortadan kalkınca kurumun faaliyetleri devam eder, imaj kaybı yaşanmaz, müşteri kaybı olmaz, küçük çapta maddi zarar oluşabilir.	Bütünlüğü ortadan kalkınca maddi kayıp yaşanmaz, imaj ve motivasyon kaybı yaşanabilir.	Erişilememesi 1 güne kadar tolere edilebilir.
1	Gizliliği ortadan kalkınca kurumun faaliyetleri devam eder, maddi kayıp yaşanmaz, hukuksal bir sorun yaşanmaz, herkesin erişimine açıktır	Bütünlüğü ortadan kalkınca kolaylıkla yerine konabilir, Kurum faaliyetleri kesintiye uğramaz	Erişilememesi 1 günden fazla tolere edilebilir.

G,B,K ' nın çarpanı yöntemiyle değerleri belirlenen varlıkların karşılaşabileceği "tehditler" ve bu tehditlerin suiistimal edebileceği "zayıflıkları" değerlendirilir.

Tehdit: Kuruma ticari açıdan zarar verebilecek istenmeyen durumların olası nedenleri.

Zayıflık: Bir varlığın bir tehdit ile suiistimal edilebilecek zayıflıkları.

Önce;

Varlık, tehdit ve zayıflık kombinasyonu düşünülerek " etki " ve " olasılık " değerleri atanır. Etki ve olasılık değerleri verilirken hiçbir önlem ve kontrolün mevcut olmadığı durum düşünülür. Hiçbir önlem ve kontrolün bulunmadığı durumda oluşan değerler ile risk puanı oluşturulur. Hiçbir önlem ve kontrolün bulunmadığı durumlar için etki ve olasılık değerleri maksimum değer olan 3 değerini alır.

Sonra;

Mevcut (alınan) önlem ve kontroller düşünülerek etki ve olasılık değerleri verilir. Önlem ve kontroller tehdidi azaltırken, zayıflığı da azaltır, dolayısıyla etki ve olasılık değerleri indirgenir. Mevcut (alınan) önlem ve kontroller düşünülerek yapılan değerlendirme sonucunda "indirgenmiş etki", "indirgenmiş olasılık" ve "indirgenmiş risk puanı" oluşur.

"Etki" ve "Olasılık" ayrı ayrı 3'lü skalalar üzerinden değerlendirilir.

1: Düşük
2: Orta
3: Yüksek

ETKİ

3 Varlığın süresiz olarak işlem yapamamasına, tamamen zarar görmesine neden olur. Tamamen baştan yapılandırılmasını gerektirir.

2 Varlık üzerinde hasar oluşur, hasarın giderilmesi için kaynak harcanmasını gerektirir

1 Tehdidin varlık üzerinde etkisi yoktur.

OLASILIK

3 Daha önce bir defadan fazla yaşanmış olabilir, bir yıl veya daha kısa sürede birkaç kez olabilir, yaşanma olasılığı yüksek.

2 Daha önce bir kez gerçekleşmiş olabilir, bir yıl ila beş yıl arasında bir veya birkaç kez olabilir.

1 Daha önce hiç gerçekleşmemiş. Beş yıldan daha uzun bir sürede bir kez olabilir veya hiç olmaz.

Risk analiz metodolojisinde;

" Varlık Değeri x Etki x Olasılık = Risk Puanı " formülü kullanılır.

Bu formüle göre teorik olarak olabilecek en yüksek risk puanı (125 x 3 x 3) 1125 puandır.

Mevcut risk analiz çalışmaları neticesinde kabul edilebilir risk puanı 250 olarak belirlenmiştir.

İndirgenmiş risk puanının, kabul edilebilir seviye olan 250 puanın üzerine çıkması halinde Bilgi Güvenliği Ekip Lideri tarafından üst yönetime risk durumu (Bilgi İşlem Daire Başkanı) e-mail ile bildirilir.

Üst yönetim ile yapılacak değerlendirme neticesinde; risk üst yönetim tarafından kabul edilir ve gerekli iyileştirme çalışmalarının başlatılması için onay verilir. Onay verilmesi halinde, ilgili varlık sahibi bölüm yönetimi öncülüğünde iyileştirici faaliyetler planlanarak hayata geçirilir.

İyileştirici faaliyet neticesinde risk değerlendirmesi tekrarlanır.Söz konusu risk puanın kabul edilebilir seviyenin üzerinde kalması durumunda aynı süreç tekrarlanır.

Risk analizi sonucunda aynı varlık için, farklı tehditlere karşın farklı risk puanları oluşabilir. Dolayısıyla risk analizi sonucunda hangi varlığın ne kadar korunacağı değil, hangi varlığın, hangi tehdit karşısında ne kadar korunacağına dair sonuçlar oluşturulur.

5- BGYS Kayıtları

GN.FR-183 2018 BGYS RİSK DEĞERLENDİRME FORMU
GN.FR-184 BGYS TEHDİT LİSTESİ FORMU
GN.FR-185 BGYS ZAYIFLIKLAR LİSTESİ FORMU
GN.FR-186 BGYS RİSK İŞLEME TABLOSU FORMU
GN.FR-187 RİSK İŞLEME TABLOSU