1. AMAÇ

Bu doküman, Bilgi Güvenliği Yönetim Sistemi için risk analizi ve değerlendirme yöntemlerini tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu prosedür, BGYS kapsamında yer alan adreslerde depolama, ithalat, ihracat, gümrükleme fonksiyonları ile bu fonksiyonları destekleyen İdari işler, Bilgi Sistemleri, İthalat ve İhracat, Muhasebe ve hizmet alınan üçüncü taraflar dahilinde tüm prosesleri kapsar. Yerine getirilen hizmetlere ilişkin bilgi varlıkları ve dış taraflardan kaynaklanan tehditler bu prosedür kapsamındadır.

3. SORUMLULAR

BGYS Temsilcisi ve diğer personelin sorumlulukları ilgili görev tanımı, politika, prosedür veya dokümanlarda belirtilmiştir.

4. UYGULAMA

4.1 Tanımlar

Varlık: Kuruluş için değeri olan herhangi bir şey. [ISO/IEC 13335-1: 2004]

Gizlilik (C): Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliği. [ISO/IEC 13335-1: 2004]

Bütünlük (I) : Varlıkların doğruluğunu ve tamlığını koruma özelliği. [ISO/IEC 13335-1: 2004]

Erişilebilirlik (A) : Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliği. [ISO/IEC 13335-1: 2004]

Risk Değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses. [ISO/IEC Guide 73]

Risk Analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı. [ISO/IEC Guide 73]

Risk Derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi. [ISO/IEC Guide 73]

Risk İşleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması prosesi. [ISO/IEC Guide 73]

Riskin Kabulü: Bir riski kabul etme kararı. [ISO/IEC Guide 73]

Artık Risk: Risk işlemeden sonra kalan risk. [ISO/IEC Guide 73]

Risk Yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler. [ISO/IEC Guide 73]

Uygulanabilirlik bildirgesi: Kuruluşun BGYS' si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirge. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını, yasal ve düzenleyici gereksinimleri, anlaşma yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır.

Tehdit: Bir varlığın / sistemin zarar görmesine veya çalışmamasına neden olan, istenmeyen bir olayın arkasındaki gizli gerçek, gerekçe, gözdağı.
Açıklık: Bir varlığın / sistemin, altyapının eksikliği, yetersizliği. Zayıflık.

Tehdit Olasılığı: Varlığın / Sistemin açıklıklarını sömüren tehdidin ortaya çıkma olasılığı

Risk Fonksiyonu: R($V_{arlık}$,T_{ehdit},$A_{çıklık}$)

İş Etki: Tehditlerin ortaya çıkması halinde varlık üstünde ortaya çıkan olumsuz durumlar, kesintiler, durmalar, bozulmalar, çalışamaz hale gelme. Tehdidin varlık üzerindeki işe etkisi gizlilik, bütünlük ve erişilebilirlik değerlerini kullanır.

4.2 Yöntem

BGYS Temsilcisi, Genel Müdür, Muhasebe Sorumlusu ,İdari İşler Sorumlusu,İthalat ve İhracat Sorumlusu, Güvenlik Görevlisi, Santral Operatörü ve ilgili süreç sahiplerinin katılımıyla ÖRNEK FİRMA bilgi varlıkları üzerindeki açıklıklar, tehditler, tehditlerin olasılığı ve işe etkisi dikkate alınarak risk seviyeleri belirlenir. Risk değerlerini azaltmak için üst yönetim desteği ile gerekli aksiyonlar alınır, yatırım ihtiyaçları tespit edilerek finansal yönetim sürecine girdi oluşturur.
Risk analizi süreci, kapsam belirlenmesi ile başlar. Kapsamda bulunan varlıklar belirlendikten sonra, tehditler, açıklıklar ve mevcut kontroller belirlenir. Daha sonra olasılık değerlendirmesi ve etki analizi gerçekleştirilir. Son olarak bulunan riskler derecelendirilerek dokümante edilir.

1. Kapsam Belirlenmesi
2. Varlıkların Belirlenmesi
3. Tehditlerin Belirlenmesi
4. Açıklıkların Belirlenmesi
5. Olasılık Değerlendirilmesi
6. Etki Analizi
7. Risk Derecelendirilmesi
8. Uygun Kontrollerin Belirlenmesi
9. Sonuçların Dokümantasyonu

Riskleri tanımlamak, çözümlemek ve derecelendirmek için kullanılan ve üretilen dokümanlar aşağıdadır:

- Varlık Envanteri
- Risk Analizi
- Risk İşleme Planı

a) Varlık Kategorileri

Risk analizine tabi tutulacak varlık kategorileri aşağıdaki gibidir:

Server : Sunucular, Sanal sunucular

Sistem odası aktif cihazlar : aktif cihazlar (switch, firewall, router, hub, modem, vb),

Access Point ve Switch :

GSM : GSM hatları , telefonlar , vb.

Printer , Fax ve Kesim Makinesi : faxlar, fotokopiler, yazıcılar, santraller, evrak imha cihazları vb.)

Bilgisayarlar : PC'ler, taşınabilir bilgisayarlar, desktoplar , vb.

Workstation : Özel amaçlı Workstation bilgisayarlar.

Diğer cihazlar – IT : Depolama birimleri, yedekleme birimleri (kasetler, hard diskler vb.)

Yazılım Veri Tabanı: Elektronik kayıtların yeraldığı veritabanları.

Yazılımlar: İşletim sistemleri, ofis uygulamaları, uygulama yazılımları, uygulama sunucuları, ağ yönetim / izleme sistemleri.

İnsan Kaynakları: Çalışanlar.

Diğer Cihazlar / Altyapı: Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, yangın bildirme, iklimlendirme, giriş / çıkış kontrol sistemleri, kamera sistemleri, yangın, su, duman, nem uyarı sistemleri, yangın söndürme sistemleri, kabinler, destek teçhizatı vb.

Binalar: Yönetim ve hizmet odaları, sunucu odaları, depolar, enerji odaları, arşiv odaları, toplantı salonları.

Bağımlılıklar: FİRMA'in temel fonksiyonlarını yerine getirirken almış olduğu ürün ve hizmet sağlayıcılar, yasal ve sözleşmeye dayanan bağımlılıklar.

Varlıkların envanteri çıkartılırken varlıkların sahipleri ve sorumluları ile bulundukları yerler ve çeşitli konfigürasyon bilgilerine yer verilecektir.

b) Varlık sınıflandırma

Varlık değerleri aşağıdaki tablodaki örnek ifadelere göre sınıflandırılabilir:

Varlık Değeri	**Varlık Değeri belirleme kriterleri için örnek ifadeler**
1	(G) Varlık açısından **gizlilik** yoktur. Bilgilerin açığa çıkmasından sistem etkilenmez. (B) Varlığın zarar görmesi veya olmaması sistemi etkilemez. Varlığın yedeği de yedeklidir. (E) Varlığın erişilebilirliği ortadan kalkmaz.
2	(G) Varlık açısından gizlilik kritik değildir. Kurum çalışmaları için açığa çıkan

	bilgilerin önemi düşüktür. (B) Sistem çalışmaya devam eder ancak varlığın yenilenmesi gerekebilir. Varlık yedeklidir. (E) Varlığın erişilebilirliği kısmen ortadan kalkabilir. Varlığın olmaması halinde başka varlıklar üzerinden işlemler devam eder.
3	(G) Varlık **gizlilik** açısından büyük öneme sahip değildir. Gizli bilgilerin açığa çıkması Kurumun imajını etkilemez. (B) Varlığın **bütünlüğü** sistem için büyük öneme sahip değildir. Varlığın zarar görmesi halinde yenilenmesi gerekebilir. Yedekler mevcuttur. (E) Varlığın **erişilebilirliği** ortadan kalkabilir ancak varlığın olmaması halinde başka varlıklar üzerinden işlemler devam eder. Sistemin zarar görmesi belirli kısımlarda yavaşlamaya neden olur.
4	(G) **Varlık gizlilik** açısından önemlidir. Gizli bilgilerin açığa çıkması Kurum imajını kötü yönde etkiler. User şifreleri ve aktif cihaz şifrelerinin açığa çıkması durumunda sistem erişebilirliği kısmen ortadan kalkar. (B) Varlığın **bütünlüğü** sistem için önemlidir. Varlığın zarar görmesi sistemin işlerliğini büyük ölçüde etkiler. Varlığın zarar görmesi tüm sistemi etkilemez belirli prosesleri çalışamaz hale getirebilir. (E) Varlığın sistemin işlemesinde önemli rolü vardır. Sistemin çok az kısmına **erişilebilir** ya da erişilebilirlik ortadan kalkar. Sistem 1 gün kullanılamaz.
5	(G) Varlık **gizlilik** açısından çok önemlidir. Gizli bilgilerin açığa çıkması kurum imajına zarar verir. Mali ve yasal kayıplara neden olabilir. Sistem çalışamaz hale gelebilir. (B) Varlığın zarar görmesi sistemi doğrudan etkiler. Varlık sistem için kritik öneme sahiptir. Sistemin yeniden çalışır hale gelmesi için zaman ve maliyet gerekir**.(bütünlük)** (E) **Erişilebilirlik** ortadan kalkar. Sistem 2 gün ve üzeri kullanılamaz.

c) Tehditler ve Açıklıklar

Tehditler : Varlıkların risk değerlendirmesi iki kademeli analize tabi tutulmaktadır.

- Özellik ve ortam koşulları olarak birbirine yakın ve aynı servis grubu içinde yer alan varlıklar üzerindeki tehditlerin ve açıklıkların ortak olması durumunda gruplandırarak analiz etmek.
- Gruplamaya müsait olmayan varlıkları tekil olarak analiz etmek.

Tehditler aşağıda listelenmiştir:

İnsan Kaynakları için:

1. İş kazası
2. İş değiştirme
3. Yetkileri kötüye kullanma
4. Hata ve unutma
5. Salgın hastalık

6. Doğal afet

Yazılım ve Donanım varlıkları için:

1. Yanlış işlem uygulanması
2. Yanlış öncelik tespiti
3. Sorumlulukları yerine getirememek
4. Kaynakları bulundurmamak
5. İş bilgisi ve deneyim eksikliği
6. Kaynak planlaması (bütçe) yapmamak
7. Taleplerin sürekli değişmesi
8. Proje zorluğu
9. Sürüm ve güncelleme kontrollerindeki problemler
10. Kodlama problemleri
11. Yetersiz antlaşmalar ve kontrol eksikliği
12. Yetkisiz erişim
13. Teknik sorunlar
14. Virüs, trojan, spyware …
15. Kullanıcı hatası ve unutkanlık
16. Satın alma süreci ile koordinasyon eksikliği
17. IT kararlarında ilgili IT personelinin bulunmaması
18. 3.taraflara bağımlılık
19. Hırsızlık
20. Donanım arızası
21. Elektriksel problemler
22. Donanım yazılım uyumsuzluğu
23. Enerji kesintisi
24. Fiziksel zarar
25. Periyodik bakımlardaki aksaklıklar
26. SLA uyumsuzluğu

3.Taraflar için:

1. Yetki çakışması
2. Planlanan işlerin zamanında bitmemesi
3. Hizmet kesintisi
4. Yetkisiz erişim
5. Erişim yetkisi oluşturmadaki gecikmeler
6. İflas
7. Yetkinlik eksikliği
8. SLA uyumsuzluğu
9. İstenen doküman veya elektronik kayıt ortamının (kartuş vs) bulunamaması
10. Güvenlik önlemlerindeki eksiklik
11. Bakım hizmetlerindeki yetersizlik
12. Değişikliklerin sistemi yavaşlatması veya durdurması
13. Yazılım kaynaklı teknik sorunlar
14. Kötüye kullanım
15. Yasal uyumsuzluk
16. Sözleşmelerin yetersizliği
17. Bilgi sızması

Binalar:

1. Yetkisiz erişim
2. Yangın
3. Fiziksel zarar
4. Su baskını
5. Deprem
6. Hata ve unutma
7. Hırsızlık
8. Patlamalar

Açıklıklar:

Açıklıklar varlıklara ilişkin olup ortadan kaldırılamazlar. Açıklıklar, varlıkların korunmasızlıklarıdır. Tehditler varlıklara zarar verecek dışsal durumlar, olaylar, araçlar ve kişilerdir. Tehditlerin ortadan kaldırılması mümkün değildir. Ancak açıklıklar yönetilerek tehdidin işe etkisi yönetilebilir. Tehditler varlıkların açıklıklarını kullanarak sisteme zarar verirler.

Açıklar;

- Varlığın niteliklerinden kaynaklı (taşınabilirlik, hafiflik gibi varlığa dair)
- Varlık yönetimine bağlı kusurlarından kaynaklı olabilir. (Tasarım, konfigürasyon, yerleşim gibi)

Açıklıklar aşağıda listelenmiştir:

1) Personel farkındalığı
2) Yetersiz ve yanlış güvenlik politikaları
3) Bakım ve servis eksiklikleri
4) Yama ve konfigürasyon yönetimi
5) Yazılımsal açıklıklar
6) Erişim yönetimi zayıflığı
7) Altyapı ve tesisat yetersizliği
8) Ortam şartlarının uygunsuzluğu
9) Sosyal şartlar
10) Yapısal açıklıklar
11) İş güvenliği eksikliği
12) Eğitim eksikliği
13) Üçüncü taraflara bağımlılık
14) İklim şartları
15) Coğrafi faktörler
16) Beşeri durumlar
17) Günlük kontrollerin yapılmaması
18) Elektrik dalgalanmaları ve ani kesinti
19) Güvenlik politikalarında açıklık
20) Organizasyon yapısı
21) Planlama problemleri
22) Standartlara uyum konusunda yaptırım ve disiplin eksikliği

d) Tehditlerin Gerçekleşme/Etkileme Olasılığı / Sıklığı

Tehditlerin oluşma, ortaya çıkma sıklıkları ya idarenin geçmiş kayıtları ya çalışanların öngörüleri ya da benzer tehditlerin genel anlamda tahminleri ile belirlenir. Tehditlerin ortaya çıkma olasılıkları / sıklıkları veya sistemi olumsuz yönde etkileme olasılıkları BGYS Ekibi tarafından kararlaştırılır.

Derece	Olasılık
1	3 yıldan seyrek
2	Birkaç yılda bir
3	Yılda birkaç kez
4	Ayda birkaç kez
5	Haftada birkaç kez

e) İş etki Analizi

Derece	Etki
1	Tehdidin varlık üzerinde etkisi yoktur.
2	Sistem durmaz fakat sistem performansı düşer ve iş sürekliliği açısından **yavaşlama** olur.
3	Sistem durur, yedeklerden geri dönüş gerekebilir, sistemin ayağa kaldırılması **5 saat sürer**. Varlıkların onarımı veya yenilenmesi için kaynak gerekebilir.
4	Sistem durur ve varlıklarda büyük ölçüde zarar ortaya çıkar. Birden fazla proses bu tehditten etkilenir. Sistemin ayağa kaldırılması **1gün sürer**. Zarar gören sistem büyük ölçüde yeniden yapılandırma gerektirebilir.
5	Sistem durur ve kullanılamaz. Zarar gören sistemin yeniden yapılandırılması gerekir. Sistemin ayağa kaldırılması **2 günden fazla** sürer.

Etki değeri = Max (Gizlilik, Bütünlük, Erişilebilirlik) fonksiyonu ile hesaplanır. En büyük değer etki faktörü olarak kabul edilir.

f) Risk analizi ve derecelendirme

Tehditlerin açıklıkları kullanmasının etkileri olasılıklar dâhilinde ortaya çıkar. Bu nedenle tehditlerin ortaya çıkma olasılıkları ile etki çarpılarak varlığın risk değeri hesaplanır.

Risk değeri = Olasılık * Etki

Ancak risk değeri tek başına bir anlam ifade etmez çünkü ortaya çıkan risk değerinin varlıkların kritikliği ile ilişkisinin sağlanması gerekmektedir. Risk değerinin varlık kritiklik değeri ile çarpılması sonucu ortaya çıkan değer Mutlak Risk Değeri olarak kabul edilmiştir.

Mutlak Risk Değeri = Varlık değeri * Risk değeri

Mutlak Risk Değeri yapılandırılması gereken risklerin sınıflandırılması için bir temel teşkil eder. Risk değerlendirmesinde varlıklar üzerinde birden fazla tehdit var ise her bir tehdit üzerinden ayrı değerlendirme yapılır. Her tehdit bir açıklığa bağlanarak hesaplama yapılır. Bir tehdit birden fazla açıklığı kullanarak ortaya çıkabilir.

g) Risk matrisi

Risk Değeri Hesaplama

Risk Değeri						
	Etki					
Olasılık		1	2	3	4	5
	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Mutlak Risk Değeri Hesaplama

Mutlak Risk Değeri					
Varlık	Risk Değeri				
1	1	2	3	4	5
2	4	8	12	16	20
3	9	18	27	36	45
4	16	32	48	64	80
5	25	50	75	100	125

Kabul edilebilir risk seviyesi aşağıdaki şekilde belirlenmiştir:

Etki Değeri 3,4 ve 5 ile Olasılık değeri 4,5 için matris çarpımı değeri alınır. Bu değerler Varlık Değeri 4 ve 5 olan varlıklar ile matris çarpımı yapılarak riskli alan belirlenir. Mutlak risk değeri matrisinde belirtilen 25-27-32 değerleri düşük risk, 36,45,48,50 değerleri orta risk , 64,75,80,100 değerleri yüksek risk ve 125 değeri çok yüksek risk olarak alınır. Kabul edilebilir risk değeri , kabul edilemez risklerin en küçük değeri olan 25 den bir düşük değer **20** dir.

20 değerinden düşük riskler için de gerekli görüldüğünde aksiyon planlanır. Ancak bu değerden düşük risklerin yönetim tarafından kabul edildiği öngörülmüştür ve bu kural risk analizi çalışmasında uygulanmıştır. 20 değerinden büyük olan riskler değerlendirilerek aksiyon planları oluşturulacaktır.

h) Risk İşleme Planının Hazırlanması

HAZIRLAYAN	ONAYLAYAN
BGYS YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR

Risk analizi dokümanında risklerin işlenmesine ilişkin varsa olası maliyetler yer alır. Üst yönetim Risk Analiz Raporunu değerlendirir.

Aşağıdaki seçeneklerden birini o risk satırı için seçer. Eğer "Kontrol" seçeneği seçilirse o seçenek için seçilmiş kontrol kriterleri ve kriterler için tanımlanmış önlemler, planlar, faaliyetler, satın alımı önerilen donanım, yazılım, ekipman veya hizmetlerin kurum tarafından dahili veya harici olarak tedarik edileceği anlamına gelir. Yönetim onayı olmadan Risk İşleme Planı uygulanamaz.

Karar verilirken iş etkileri ve öncelikleri dikkate alınır. Risk işleme için dört seçenek mevcuttur.

Kontrol (azaltma, hafifletme, tedavi - Treatment): Riskleri azaltmak için uygun kontrollerin seçilmesi ve uygulanmasıdır. Bu kontroller ISO 27001 Ek-A bölümündeki başlıklardan da seçilebilir. ISO 27002 kılavuzunda ayrıntılı olarak açıklanan kontrol önerileri de dikkate alınarak uygun kontroller seçilir. Seçilen kontrollerin maliyet-fayda karşılaştırmasına, uygulanabilirliğine, sürdürülebilirliğine ve yönetilebilirliğine bakılarak uygun olanları seçilir ve uygulanır.

Kabul (Accepted – tolerated): Kabul seçeneği içinde üç farklı değerlendirmeyi taşımaktadır:

- Kurumun politikalarını ve risk kabul kriterlerine uymak koşuluyla bazı riskler kabul edilebilir. Risk puanı kabul edilebilir seviyenin altında olanlar ve kabul edilebilir seviyeye yakın olanlar bu işleme tabi tutulurlar.
- Risk değeri "Kabul edilebilir Risk Seviyesi"nin üstünde olabilir. Ancak risk önleme maliyeti düşünülerek veya bütçe, altyapı, personel durumu uygun değilse Yönetim bu risk sonucunu kabul edebilir.
- Risk İşleme sonucu bile risk kabul edilebilir seviyenin altına inmiyorsa "Artık Risk Üstlenme Beyanı" ile riskin sonuçlarını üstlenerek kabul edebilir.

Kaçınma - Sonlandırma (Terminated): Risklerin çeşitli nedenlerle kontrol edilememesi durumunda uygulanır. Riskin kaynağı olan tehdidin gerçekleşme olasılığının ve iş etkisinin çok yüksek olduğu durumlarda riskten uzaklaşmak için her tür çaba, düzenleme, donanım, yazılım, ekipman, hizmet alımları gerçekleştirilir veya risk kaynağı uygulamalar devreden çıkarılır. İnternet saldırıları için internet bağlantısının kesilmesi gibi, deprem tehdidinden dolayı çalışma ortamını değiştirmek, taşımak gibi.

Aktarma (Transfered): Kurumun yönetiminde ve kontrolünde olmayan varlık ve fonksiyonlarla ilgili ve kurumun müdahale edemeyeceği konularla ilgili riskler başka kurumlara transfer edilir. Örneğin yangın, doğal afet, hırsızlık gibi tehditlerin azaltılması için yapılan kontrollerden sonra kalan artık risk itfaiye, sigorta şirketi, AKUT, emniyet güçleri vb. kurumlara aktarılır.

Seçilen uygun risk işleme kararları risklerin takibi için risk işleme planına kaydedilir. Risk işleme planında seçilen kontrol ile ilgili olarak (Ek A'ya göre) görevler, sorumluluklar, temrinler ve bütçeler belirtilir. Risk işleme planı sürekli güncellenerek uygulanan kontrollerin durumu kayıt altına alınır.

i) İzleme ve Gözden Geçirme

Risk analizi ve Risk işleme planı, 6 ayda bir bir kez veya majör yerleşim, altyapı, personel, teknik, yasal değişikliklerden sonra gözden geçirilir. Riskler kabul edilebilir seviyenin altına inmesi halinde rutin kontrollerle takip edilirler.

HAZIRLAYAN	ONAYLAYAN
BGYS YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR

	BİLGİ GÜVENLİĞİ RİSK YÖNETİMİ PROSEDÜRÜ	

HAZIRLAYAN	ONAYLAYAN
BGYS YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR