1. AMAÇ

Bu prosedürün amacı, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı kapsamındaki bilgi güvenliği risklerinin belirlenmesi ve işlenmesi yöntem oluşturmaktır.

2. KAPSAM

Bu prosedür, Bursa Uludağ Üniversitesi bünyesindeki Bilgi İşlem Daire Başkanlığı için belirtilen risk değerlendirme ve işleme kontrollerini kapsar.

3. TANIMLAR VE KISALTMALAR

Varlık Sahibi: Varlığın üzerinde taşıdığı bilgiyi, erişim ve kullanım yöntemlerini, varlığın üzerindeki riski en iyi bilen kişidir. Sürecin sahibidir.
Bilgi Varlıkları: Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir.
Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir).
Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Ör: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması, dijital imza)
Erişilebilirlik (Kullanılabilirlik): Bir varlığın yetkili varlıklarca talep edildiğinde erişilebilir ve kullanılabilir olma özelliği.
Tehdit: Varlıklar ya da varlıklardan oluşan sistem üzerinde gerçekleşen istenmeyen, zarar verici ya da yok edici olaylardır.
Zayıflık: Bir varlığın ya da varlık grubunun bir ya da daha fazla tehdit tarafından zarar görme zafiyetidir. Zayıflık yönetilemez ise tehdit gerçekleşir ve zararlara sebep olur.
Olasılık: Varlıklar üzerindeki tehditlerin gerçekleşme sıklığıdır.
Şiddet: Bir tehdit meydana geldiğinde ilgili yere bıraktığı etki.
Risk: Bir tehdidin olasılığı ile şiddetinin bileşkesi şeklinde ele alınır. Bir varlığın zarara, kayba uğrama tehlikesidir.
Risk Sahibi: Bir riski yönetmek için sorumluluk ve yetki sahibi kişi veya birim.
Risk Değerlendirmesi: Risk analizi ve risk derecelendirmesini kapsayan tüm proses.
Risk İşleme: Riski azaltmak için alınması gereken önlem ve faaliyetleri uygulama prosesi.
Riskin Kabulü: Bir riski kurumun kabul etme kararıdır.

4. SORUMLULUK

Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı çalışanlarıdır.

5. UYGULAMA

5.1 Risk Yönetimi

Varlıklar, Kişisel veriler ve süreçler üzerinde bulunan riskler BGYS ekibi, ilgili bölüm temsilcisi ve varlık sorumluları ile birlikte Risk İşleme Planı üzerinde kayıt altına alınır ve işlenir. Risk Yönetimi sürecinde; Riskin Belirlenmesi, Risk Analizi, Risk Değerlendirme ve Risk İyileştirme adımları uygulanacaktır. Departman bazında açıklıklar ve tehditler belirlenecektir.

Risk değerlendirme risk senaryoları ile başlatılır. Risk senaryosu, bir tehdidin (iç/dış), kurumsal sürecin, varlığın mevcut zafiyetlerini/özniteliklerini, ortaya çıkma olasılığına/sıklığına göre istismar etmesi sonucu, süreç veya varlık üzerinde ortaya çıkabilecek gizlilik, bütünlük, erişilebilirlik kayıplarının ifadesi olarak yazılır.

5.2 Riskin Belirlenmesi

a- Bilgi varlıkları ve süreçler ile ilgili risklerin belirlenmesi için aşağıdaki girdiler kullanılır:

- İç/dış hususların gereksinimleri ile ilgili riskler
- Personelin deneyimleri
- Yaşanan ihlal olayları ve bu olaylardan çıkarılan dersler
- Geçmiş yıllarda yapılmış risk değerlendirme çalışmaları
- Düzeltici ve iyileştirici faaliyetler
- Sektörde, Türkiye'de ve dünyada ortaya çıkmış bilgi güvenliği olayları
- Sızma, teknik açıklık ve servis durdurma test sonuçları
- Güncel teknolojik ilerlemeler ve oluşabilecek zafiyetler
- İç ve dış denetim raporları
- Düzenleyici ve denetleyici kurumlar tarafından iletilmiş talimatlar

b- Ortaya konan iç/dış hususlar ile ilişkili bilgi güvenliği riskleri, ilgili birim/iş süreci yetkilileri ile birlikte belirlenir. Bu kapsamda aşağıdaki hususlar dikkate alınır:

- İlgili konu ve iş süreci ile ilgili bilgi güvenliği riskleri
- Risklerin etkileyebileceği varlıklar ve süreçler

c- Çalışmaların çıktıları Bilgi Güvenliği Yönetim Temsilcisi tarafından değerlendirilir. Değerlendirmeler sonucunda, bu çalışmada belirlenen riskler, Risk İşleme Planına eklenir.

d- Risk senaryo tanımı genel olarak; varlık/süreç adı, zafiyet/açıklık ifadesi, tehdit ifadesi, riskin muhtemel sonuçları parametrelerini içerir.

Örnek Risk Tanımı
Varlık: Sunucular
Zafiyet: Jeneratörün olmaması
Tehdit: Elektrik kesintisi
Muhtemel Sonuç: Hizmetin kesintiye uğraması/durması
Risk Tanımı: Jeneratör altyapısının olmaması sebebiyle sunucuların elektrik kesintisinden dolayı hizmet verememesi.
Mevcut Kontroller: Sistemi 20 dakika kesintisiz çalıştırabilecek UPS sistemi bulunmaktadır.
Etki: Çok Yüksek
Olasılık: Yüksek

5.3 Mevcut Kontrollerin Belirlenmesi

a. Riskler, risk sahipleri ile görüşmeler yapılarak uygulanan kontroller ile tanımlanır ve varlıklarla eşleştirilir.
b. Eşleştirmeler yapılırken paralel olarak, mevcut dokümanlar incelenerek ve varlık sahipleriyle görüşmeler yapılarak uygulanan mevcut kontroller belirlenir ve değerlendirilir.
c. Mevcut kontroller, ilgili ISO 27001 kontrol maddeleri, risk değerlendirmesine girdi olarak alınan çeşitli havacılık ve güvenlik çerçevelerinin beklentileri veya üreticilerin tarafından önerilen en iyi uygulama önerileri ile eşleştirilir.

5.4 Risklerin Derecelendirilmesi

Risk derecelendirilirken, varlık ve süreçlerin gizlilik, bütünlük erişilebilirlik değerleri, risklerin etkileri ve risklerin oluşma olasılıkları göz önünde bulundurulur.

5.4.1 Varlık Değerinin Belirlenmesi

Envanterde tanımlanan varlıkların değerinin belirlenmesi için Gizlilik, Bütünlük ve Erişilebilirlik değerlerinin belirlenmesi gerekmektedir. Varlık değerini belirlerken var "Varlık Yönetimi Prosedürü" nden faydalanılır. Varlık değeri hesaplanırken Gizlilik, Bütünlük ve Erişilebilirlik değerlerinin toplamı esas alınır.

Varlık Değeri = Gizlilik + Bütünlük + Erişilebilirlik

Envantere eklenen tüm varlıklar varlık grupları altında sınıflandırılır. Risk değerlendirme sürecinde varlık grupları da değerlendirilebilir. İlgili varlık grubunun varlık değeri, içinde bulunan en yüksek değerli varlığın puanı olacak şekilde belirlenir.

5.4.2 Varlıkların ve Varlık Gruplarının Etki Açısından Değerlendirilmesi

Her bir risk değerlendirme çalışmasında tanımlanan riskin gerçekleşmesi durumunda olası etkilerinin hesaplanması gerekmektedir. Varlık/Varlık grubu açısından risk değerlendirme yapılırken "Etkilenen Kişi Sayısı, Toplumsal Sonuçlar, Kurumsal Sonuçlar, Sektörel Etkisi ve Bağımlı Varlıklar" dâhil olacak şekilde tüm etki alanları referans alınarak yapılır senaryolandırılır ve değerlendirme sorusuna göre puanlanır.

Etkilenen Kişi Sayısı (ES)
Değerlendirme: Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı DDO Ek-C.1 – Varlık Grubu Kritiklik Derecelendirme Anketi rehberinde yer alan varlık grubu için anket sorularından B bendinde belirtilen Varlık Grubunun Etki Açısından Değerlendirilmesi Etkilenen Kişi Sayısı (4) tablosu kullanılmaktadır.

Toplumsal Sonuçlar (TS)
Değerlendirme: Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı DDO Ek-C.1 – Varlık Grubu Kritiklik Derecelendirme Anketi rehberinde yer alan varlık grubu için anket sorularından B bendinde belirtilen Varlık Grubunun Etki Açısından Değerlendirilmesi Toplumsal Sonuçlar (5) tablosu kullanılmaktadır.

Kurumsal Sonuçlar (KS)
Değerlendirme: Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı DDO Ek-C.1 – Varlık Grubu Kritiklik Derecelendirme Anketi rehberinde yer alan varlık grubu için anket sorularından B bendinde belirtilen Varlık Grubunun Etki Açısından Değerlendirilmesi Kurumsal Sonuçlar (6) tablosu kullanılmaktadır.

Sektörel Etki (SE)
Değerlendirme: Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı DDO Ek-C.1 – Varlık Grubu Kritiklik Derecelendirme Anketi rehberinde yer alan varlık grubu için anket sorularından B bendinde belirtilen Varlık Grubunun Etki Açısından Değerlendirilmesi Sektörel Etki (7) tablosu kullanılmaktadır.

Bağımlı Varlıklar (BV)
Değerlendirme: Varlık grubunuzda yer alan varlıklar üzerinde gizlilik, bütünlük ve erişilebilirlik boyutlarının tamamını etkileyecek, olası en kötü senaryoya sahip bir bilgi güvenliği ihlal olayı meydana geldiğinde doğrudan etkilenebilecek kişi sayısı DDO Ek-C.1 – Varlık Grubu Kritiklik Derecelendirme Anketi rehberinde yer alan varlık grubu için anket sorularından B bendinde belirtilen Varlık Grubunun Etki Açısından Değerlendirilmesi Bağımlı Varlıklar (8) tablosu kullanılmaktadır.

Etki değeri aralığı aşağıdaki formülle belirlenir.

ETKİ DEĞERİ FORMÜLÜ = ES + TS + KS + SE + BV

Etki değeri hesaplanırken aşağıdaki tabloda bulunan puanlama sistemi kullanılır;

Boyut	Soru No.	Şıkların Puanları				
		a	b	c	d	e
Etki Alanı Açısından						
Etkilenen Kişi Sayısı	4	1 puan	2 puan	3 puan	4 puan	5 puan
Toplumsal Sonuçlar	5	1 puan	2 puan	3 puan	5 puan	6 puan
Kurumsal Sonuçlar	6	1 puan	2 puan	3 puan		
Sektörel Etki	7	1 puan	2 puan	3 puan	5 puan	
Bağımlı Varlıklar	8	1 puan	2 puan	3 puan	5 puan	6 puan

Tablo : Etki Değerlendirme Tablosu

5.4.3 Riskin Olasılığının Değerlendirilmesi

a. Kurum'da, risk değerlendirme çalışmaları kapsamında risklerin ortaya çıkma olasılıkları risk sahiplerinden gelen bilgilere göre Bilgi Güvenliği Yönetim Temsilcisi tarafından aşağıdaki tabloya göre belirlenir.

OLASILIK SINIFI	OLASILIK DEĞERİ	AÇIKLAMA
Neredeyse Kesin	**5**	Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerlerinden bağımsız olarak riskin 7 gün içerisinde bir veya birkaç kez oluşması ya da oluşabilir olması durumu olasılık değerini neredeyse kesin sınıfına çekecektir.
Büyük İhtimal	**4**	Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerlerinden bağımsız olarak riskin 1 ay içerisinde bir veya birkaç kez oluşması ya da oluşabilir olması durumu olasılık değerini büyük ihtimal sınıfına çekecektir.
Mümkün	**3**	Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerlerinden bağımsız olarak riskin 3 ay içerisinde bir veya birkaç kez oluşması ya da oluşabilir olması durumu olasılık değerini mümkün sınıfına çekecektir.
Muhtemel	**2**	Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerlerinden bağımsız olarak riskin 12 ay içerisinde bir veya birkaç kez oluşması ya da oluşabilir olması durumu olasılık değerini muhtemel sınıfına çekecektir.
Düşük	**1**	Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerlerinden bağımsız olarak riskin ortaya çıkma ihtimalinin neredeyse olmadığı durumlar düşük olarak değerlendirilir. Kolayca tespit edilebilir ve akabinde hemen önlem alınabilir, yalnızca ilgili olduğu iş sürecine bağlı olan, bilginin gizlilik, bütünlük ve erişilebilirlik açısından cazibesi olmayan bilgi varlıklarına atanan risklerin olasılığı düşük olarak değerlendirilir.

Tablo : Olasılık Sınıfı

5.5 Risk Seviyelerinin Hesaplanması

a. Gizlilik, bütünlük, erişilebilirlik, olasılık ve etki değerleri belirlenen risk senaryolarının risk değeri aşağıdaki formüle göre hesaplanır.

Risk Değeri = Varlık Değeri + Etki Değeri * Olasılık

b. Hesaplanan risk değerleri düşükten yükseğe doğru sıralanır. Risklerin öncelikleri, kritiklik seviyeleri dikkate alınarak aşağıdaki tabloya göre belirlenir.

RİSK DEĞER ARALIĞI	RİSK SINIFI	AÇIKLAMA
0 - 19	Düşük	Kabul edilebilir.
20 - 99	Yüksek	Risk işleme gerektirir.
100 - 200	Çok Yüksek	Kabul & transfer edilemez.

Tablo: Risk Seviyeleri

0 - 19 arasındaki riskler "kabul edilebilir risk seviyesi" olarak kabul edilmiştir. Kabul edilebilir risk seviyesinin değiştirilmesinden Üst Yönetimin bilgisi dâhilinde Bilgi Güvenliği Yönetim Temsilcisi sorumludur. Risk değerlendirme sonucunda "Orta", "Yüksek" ve "Çok Yüksek" aralığındaki risklerin kabul edilebilir seviyeye çekilmesi gerekecektir.

Risk puanı 20 - 99 arasındaki riskler sadece Üst Yönetim onayı ile kabul ve transfer edilebilir risklerdir. Yüksek aralığında yer alan risklere ilişkin önleyici ve/veya telafi edici kontrol konulması gerekir. Bu aralıkta yer alan risklere ilişkin önleyici kontrollerin risk değerlendirme işlemi yılda bir olacak şekilde risk sorumlusu birim ve Bilgi Güvenliği Yönetim Temsilcisi tarafından gözden geçirilmesi gerekir.

Risk puanı 100 - 200 arasındaki riskler kabul edilemez ve transfer edilemez risklerdir ve riski önleyici aksiyon çalışmalarının yapılması gereklidir. Bu aralıkta yer alan riskler için oluşturulan önleyici kontrollerin risk değerlendirme yılı içerisinde ayda bir risk sorumlusu birim ve Bilgi Güvenliği Yönetim Temsilcisi tarafından gözden geçirilmesi gerekir. Gözden geçirilen risk ve mevcut kontrollerin çözüm süreci Risk işleme planı üzerinden takip edilir.

c. Risk değerlendirme çalışmalarında elde edilen istatistiksel bilgiler Yönetim Gözden Geçirme toplantılarında üst yönetime sunulur. Risk puanı yüksek çıkan ve risk işlemeye konu olan riskler istatistiksel bilgilere ek olarak üst yönetime raporlanır. İşlenecek veya kabul edilecek riskler aşağıdaki kriterlere uygun olarak raporlanır:

d.

- Risk sınıfı yüksek olanlar riskler, risk işleme çalışmalarını başlatmak üzere seçilir.
- Risk sınıfı çok yüksek olan riskler, öncelikli olarak risk işlemeye konu olur.
- Üst yönetim, risk sınıfı yüksek ve çok yüksek olan riskler dışındaki riskleri de uygun gördüğü doğrultuda risk işlemeye konu edebilir.
- Risk sınıfı düşük, orta, kabul edilebilir olan riskler üst yönetimin onayı ile kabul edilir.
- İşlenmek üzere seçilmiş riskler bir sonraki değerlendirmede hala kabul edilebilir risk seviyesine gelmemiş ise ve buna karşılık alınacak herhangi bir iyileştirme önlemi yoksa bu riskler risk sahibinin değerlendirmesine bağlı olarak üst yönetim tarafından artık risk olarak üstlenilir.

5.6 Risk İşleme

a. Risklerin, firma varlıklarına/süreçlerine/verilerine olan potansiyel etkilerini azaltmak, aktarmak, kabul etmek ya da ortadan kaldırmak için yapılan çalışmalar risk işleme olarak tanımlanır.
b. Bilgi Güvenliği Yönetim Temsilcisi ve Üst Yönetim, belirlenen risklerden işlenecek olanlarla ilgili karar alır.
c. İşlenecek riskler için Bilgi Güvenliği tarafından risk değerlendirme ve işleme planı hazırlanır.
d. Risklerin işlenmesi için 6.2.2 maddesindeki yöntemlerden firma için en uygun olanı seçilir.

5.6.1 Risk İşleme için Kontrollerin Belirlenmesi

a. Listelenen risklerin her biri için bir veya birden fazla düzeltici veya önleyici kontrol belirlenebilir.
b. Bilgi Güvenliği Yönetim Temsilcisi, risk sahipleri ile bir araya gelerek kontrol listeleri, teknik araştırmalar ve önceki tecrübelerden çıkan sonuçları da değerlendirerek riske ilişkin kontrolleri belirler.
c. Kontroller sadece teknik açıdan değil yönetimsel ve operasyonel açılardan da değerlendirilir.

5.6.2 Risk İşleme İçin Kontrollerin Değerlendirilmesi ve Seçimi

Log kayıt ortamlarına erişim yalnızca yetkili personelce sağlanır ve erişim yetkileri periyodik olarak gözden geçirilir.

5.6.3 Yönetici ve Operatör Kayıtları

a. Üst yönetim ve Bilgi Güvenliği Yönetim Temsilcisi, kontrol alternatiflerini ve analiz sonuçlarını değerlendirir.
b. Üst yönetim, kontrol alternatiflerinden en uygun olanlarının, aşağıda belirtilen risk işleme yöntemlerine göre uygulanmasına karar verir.
   - KABUL: Riskin var olduğunun kabul edilip riske maruz kalan sürecin işletilmesi ve ilgili bilgi varlığının kullanılmasına devam edilmesidir. Risk değeri "Kabul Edilebilir Risk Seviyesi" nin üstünde ise aksiyon alınması gerekir. Ancak bütçe, altyapı, personel durumu uygun değilse üst yönetim bu risk sonucunu daha sonra tekrar ele almak üzere kabul edebilir. Alınan aksiyonlar sonucu risk "Kabul Edilebilir Risk Seviyesi" ne inmiyorsa üst yönetim tarafından "Artık Risk" olarak kabul edilebilir.
   - AZALTMA: Riskin oluşturacağı etkinin ve riskin ortaya çıkma olasılığının, çeşitli kontroller uygulanarak azaltılmasıdır (Örneğin Anti virüs yazılımı kullanılarak virüs bulaşma riskinin azaltılması).
   - TRANSFER: Riskin gerçekleşmesi durumunda oluşabilecek zararı karşılayacak çözümler bularak risklerin diğer süreç sahiplerine veya üçüncü taraflara aktarılmasıdır (Örneğin Çağrı Merkezinin işletilmesi işinin dışarıdan sağlanması ile risklerinin dış kaynağa transferi, sigortalama, siber saldırılar sonrası ortaya çıkacak zarar ve kayıpların azaltılması için siber sigorta yapılması, vb.).
   - KAÇINMA: Riski yaratan sebebi ortadan kaldırmaktır (örneğin bir yazılımın risk yaratan kısmının yüklenmemesi ve kullanılmaması gibi).
c. Üst yönetim, karar verme aşamasında kontrol alternatiflerinin fayda/maliyet değerlendirmesini göz önünde bulundurur.
d. Üst yönetim, verilen kararlar doğrultusunda Risk Değerlendirme ve İşleme Planının hazırlanması için Bilgi Güvenliği Yönetim Temsilcisini görevlendirir. Çalışma sonunda çıkan sonuçların teknik açıdan yapılabilirliği ve yaklaşık maliyet analizi yapılır.

5.6.3 Risk İşleme Planının Hazırlanması

a. Risk işleme için kaynak aktarımı yapılırken öncelik yüksek puanlı risklere verilir ve bu riskin etkilerine karşı önlemler daha önce alınır.
b. İşlenmek üzere seçilen riskler, ISO 27001 standardının EK-A'sındaki kontroller ile karşılaştırılır ve gerekli tüm kontrollerin dikkate alındığından emin olunur.
c. BGYS ekibi, her bir riskin işlenmesi için seçilen her bir kontrolü inceleyerek, bu kontrolün nasıl kurgulanacağını ve işletileceğini belirler.
d. Kontrolün hayata geçirilmesi için mevcut kaynaklar kullanılacak ise, bu amaç için gerçekleştirilecek faaliyetleri ve bu faaliyetler ile ilgili sorumluları tanımlar ve planlamasını yapar.
e. Eğer kontrolün hayata geçirilmesi için yeni hizmet/ürün alımı gerekiyor ise, faaliyetten sorumlu olacak personeller ile BGYS ekibi bu konu ile ilgili teknik araştırma ve piyasa araştırması yapar.
f. Risk işleme planlarında, kontrolün hayata geçirilmesi ile ilgili tüm faaliyet adımları, bu faaliyetleri gerçekleştirecek sorumlu kişiler ve faaliyetlerin ne zaman ne kadar sürede gerçekleştirileceği açık olarak tanımlanır.
g. Risk işleme planlama süreci; Risk İşleme Planı üzerinden ilgili riskler üzerine aksiyon oluşturularak sağlanabilir. Aksiyonlar oluşturulurken; risk stratejisi, gerektiği durumda kanıt dosyaların eklenmesi, sorumlu ve sahiplerinin atanması, sağlayacağı fırsat ve ilgili faaliyetin gerçekleşmesi durumunda olacak olan güncel olasılık ve etki değerleri tanımlanır.

5.6.4 Fırsatların Değerlendirilmesi

a. Düzeltici faaliyetler, risk ve fırsatlar bazında ele alınarak Bilgi Güvenliği Yönetim Sistemi'nin sürekli iyileştirilmesine katkıda bulunur.
b. Kurum bünyesinde gerçekleştirilen risk çalışmaları kapsamında, riskler gözden geçirilirken aynı zamanda buna bağlı olarak iyileştirme gereksinimleri de ortaya koyulur. Gereksinimlerin karşılanması halinde ortaya çıkabilecek fırsatlar değerlendirilir.

c. Fırsatlar; teknolojik gelişmelere dayalı fırsatlar, iş fırsatları, yasal ve düzenleyici şartların getirdiği fırsatlar, politik ve sosyal gelişmelerin getirdiği fırsatlar olabilir.
d. Fırsatlar, risk işleme çalışmalarına bağlı olarak ele alınır. Risk işleme çalışmaları sonucunda ortaya çıkabilecek fırsatlar değerlendirilir.

5.6.5 Risk İşleme Planının Gözden Geçirilmesi ve Onaylanması

a. Oluşturulan Risk Değerlendirme ve İşleme Planı risk sahipleri tarafından sürekli güncel tutulması beklenir.

b. Risk sahipleri risklerle ilgili kaynaklar, önlemler ve aksiyonların zamanlamasını değerlendirir ve varsa gerekli değişiklikleri uygular.

c. Son haline Risk Değerlendirme ve İşleme Planı, Bilgi Güvenliği Yönetim Temsilcisi onayı ile üst yönetime sunulur. Üst yönetim, Risk Değerlendirme ve İşleme Planı inceler ve değerlendirir. Yapılmasını istediği değişiklikler tamamlandıktan sonra planı onaylar.

5.6.6 Risk İşleme Planının Hayata Geçirilmesi ve Takibi

a. Planın onaylanmasından sonra faaliyetlerin hayata geçirilmesi için risk sahiplerine görev ataması üst yönetim tarafından yapılır.

b. Planda yer alan faaliyetlerin zamanında ve istendiği şekilde yerine getirilip getirilmediği BGYS ekibi tarafından takip edilir ve Bilgi Güvenliği Yönetim Temsilcisine raporlanır.

c. Aksayan faaliyetler ile ilgili iyileştirici faaliyetler gerçekleştirilir.

5.6.7 Artık Risk Yaklaşımı

a. Risk işleme planına göre hayata geçirilen kontroller sonrası, risk seviyesi yüksek olan ilgili varlıklar için yeniden bir risk değerlendirmesi yapılır. Bu risk değerlendirmesinin amacı, kontrollerden sonra hedeflenen kabul edilebilir risk seviyesine ulaşılıp ulaşılmadığının tespitidir.

b. Risk değerlendirme sonucunda çıkan risk puanı ile risk işleme planında hedeflenen kabul edilebilir risk puanı karşılaştırılır ve işleme faaliyetlerinin etkinliği değerlendirilir.

c. Kabul edilebilir risk seviyesine ulaşılamadıysa, Bilgi Güvenliği Yönetim Temsilcisi tarafından, gerek risk işleme planındaki alternatif faaliyetlerin gerekse yeni faaliyetlerin uygulanması ile ilgili karar alınır.

d. Bu faaliyetler sonrasında risk üzerindeki değerlendirme yeniden yapılır.

e. Alternatif faaliyetlerin uygulanması için mevcut altyapı geçersiz olabilir, firma bütçesi yeterli olmayabilir veya uzun süreli bir projeye gereksinim duyuluyor olabilir. Bu durumda risk sahibinin değerlendirmesi ile artık riskler ya üst yönetim tarafından ya da risk sahibi tarafından üstlenilir. Bu durum Risk Değerlendirme ve İşleme Planında tanımlanır.

5.6.8 Artık Riskleri Kabul Edilebilir Seviyeye İndirgeme

Uygulanan kontroller ve gerçekleşen faaliyetler (risk işleme) sonrasında ilgili varlık üzerinde **kalan risk** artık risk olarak ifade edilir.

5.6.9 Risklerin Periyodik Olarak Değerlendirilmesi ve İşlenmesi

a. Her yıl en az bir kez olmak üzere periyodik olarak risk değerlendirme çalışması yapılır. Bunun haricinde, büyük değişikliklerde, sadece değişiklik yapılan ve değişikliğin doğrudan etkilediği varlıkları/süreçleri içerecek şekilde risk değerlendirme çalışması yeniden yapılır.

b. Rutin yapılan değerlendirmelerde kapsam, en geniş haliyle bilgi güvenliği kapsamına giren tüm riskler olarak ele alınır.

c. Bilgi güvenliği Yönetim Sistemi kapsamındaki varlıklarda güncelleme veya değişiklik olması nedeniyle düzenlenen risk değerlendirmeler için kapsam, sadece bu değişikliklerin etkilediği varlıklarla/yapılarla sınırlı olabilir.

d. Risk değerlendirmeleri sonrası tekrardan risk işleme çalışmaları gerçekleştirilir.

e. Risk işleme çalışmalarının gerçekleştirilmesinden sonra işlenen riskler ile ilgili artık risk değerlendirmeleri tekrar yapılır.

5.7 Risk Sistematiğinin Gözden Geçirilmesi

Risk sistematiği Yönetimin Gözden Geçirmesi toplantılarında gözden geçirilir. Bu kapsamda aşağıda yer alan hususlar sorgulanır:

- Risk değerlendirme metodunun şirket yapısına uygunluğu
- Tanımlı risklerin güncelliği
- Kabul edilebilir risk seviyesi
- Devreye alınan kontrollerin uygulanıp uygulanmadığı
- Risklerin yönetim tarafından onaylanıp onaylanmadığı

5.7.1 Risklerin Hedef-Performans Takibi

Risk iyileştirmesi için alınan aksiyonlar sonucunda yeni risk puanı hedefi ve bu hedefin sağlanma performansı takip edilir. 12 aylık periyotlar sonucunda bu performans raporları yönetime sunulur.

6. İLGİLİ DOKÜMANLAR

TS ISO / IEC 27001 Bilgi Güvenliği Yönetim Sistemi
TS ISO / IEC 27002 Bilgi Teknolojisi-Güvenlik Teknikleri Bilgi Güvenliği Yönetimi için Uygulama Kuralları
TS ISO / IEC 27005 Bilgi Güvenliği Yönetim Sistemi Risk Yönetim Standardı
TS ISO / IEC 31000 Risk Yönetimi – Prensipler ve Kılavuzlar
6698 Sayılı Kişisel Verilerin Korunması Kanunu
Kişisel Verilerin Korunması Kurumu Veri Güvenliği Rehberi