1. Amaç

Bu doküman, Kütüphane ve Dokümantasyon Daire Başkanlığı bilgi varlıklarının risklerinin yönetilmesi için gerekli olan yöntemlerin belirlenmesi amacıyla hazırlanmıştır.

2. Kapsam

SDÜ1PR02 Kütüphane ve Dokümantasyon Daire Başkanlığı Risk Yönetimi Prosedürü, SDÜ6GE01 BGYS kapsamı dokümanında belirtilen tüm iş süreçlerine ilişkin risk ve fırsatların yönetimini kapsar.

3. Tanımlar

Kurum: Kütüphane ve Dokümantasyon Daire Başkanlığı

BİDB: Bilgi İşlem Daire Başkanlığı

BGYS: Bilgi Güvenliği Yönetim Sistemi

4. Uygulama

4.1 Risk ve Fırsatların Değerlendirilmesi

Risk, bir tehdit kaynağının mevcut bir açığı kullanma olasılığı ile bu durumun yaratacağı olumsuz etkinin fonksiyonudur.

Kurum, bilgi varlıklarına ilişkin risklerin yaratabileceği olumsuz etkileri kontrol altında tutabilmek amacıyla risk yönetimi faaliyetleri yürütür. Bu faaliyetler diğer taraftan, Kurum'a değişik alanlarda fırsatlar yaratma potansiyeline de sahiptir. Kurum Üst Yönetim'i, risklerin yönetimine ilişkin alınacak kararlarda fırsatları da göz önünde bulundurur.

Bilgi güvenliği risk değerlendirme çalışmaları yılda en az 1 kez ya da aşağıdaki durumların oluşması halinde en kısa sürede tekrarlanır:

- Altyapı, teknoloji, uygulama ya da mevzuat değişikliklerinde
- Büyük çaplı bilgi ihlal olayları sonrasında
- İş süreçlerindeki değişikliklerde

Risk değerlendirmenin temel adımları aşağıdaki şekildedir:

- Bilgi varlıklarının ve değerlerinin belirlenmesi
- Zafiyet ve tehditlerin belirlenmesi
- Olasılıkların belirlenmesi
- Riskin ortaya çıkması durumundaki iş etkilerinin, gizlilik, bütünlük ve erişilebilirlik açılarından değerlendirilmesi

4.1.1 Zafiyet ve Tehdit

Zafiyet, bilgi varlıklarının doğasında, tasarımında, işletilmesinde, uygulanmasında, kullanılmasında ya da kontrollerinde bulunan ve bilgi güvenliği ihlal olayına neden olabilecek zayıflık, hata ya da kusurlardır. Tehdit ise, herhangi bir tehdit kaynağının kasıtlı olarak ya da kazayla bir zafiyeti kullanarak bilgi varlıklarına zarar verme potansiyelidir.

4.1.2 Olasılık

Tehdidin ortaya çıkma olasılığı aşağıdaki tabloya göre belirlenir.

OLASILIK	PUAN	AÇIKLAMA
Çok Sık	5	Olağandır, her an gerçekleşmesi mümkündür.
Sık	4	Gerçekleşmesi beklenmektedir. Yılda birçok kez yaşanabilir.
Nadir	3	Gerçekleşmesine fazla ihtimal verilmemektedir. Yılda birkaç kez yaşanabilir.
Çok Nadir	2	Gerçekleşmesine çok fazla ihtimal verilmemektedir. Birkaç yılda bir yaşanması beklenebilir.
Hemen Hiç	1	Olağan dışıdır, gerçekleşmesi çok güç ya da olanaksızdır. Yıllar boyu yaşanmayabilir ya da daha önce yaşanmamıştır.

4.1.3 İş Etkisi

Risk ortaya çıktığında bu durumun Erişilebilirliğe, Gizliliğe ve Bütünlüğe etkisi ayrı ayrı değerlendirilir. Değerlendirme aşağıdaki etki tablosuna göre gerçekleştirilir.

ETKİ	PUAN	AÇIKLAMA
Kritik	5	Riskin bilgi varlıkları üzerinde etkisi kritiktir. Çok önemli derecede bilgi kaybı, tolere edilemeyecek şekilde uzun süreyle hizmet kesintisi ya da fazla sayıda varlığın bütünlüğünün bozulması yaşanır. Kurumun imajı zedelenir.
Yüksek	4	Riskin bilgi varlıkları üzerinde etkisi yüksektir. Önemli derecede bilgi kaybı, uzun süreyle hizmet kesintisi ya da önemli sayıda varlığın bütünlüğünün bozulması yaşanır. Kurumun imajı zedelenebilir.
Orta	3	Riskin bilgi varlıkları üzerinde etkisi orta derecededir. Kısıtlı miktarda ve önemde bilgi kaybı, makul sürede hizmet kesintisi ya da varlığın bütünlüğünün bozulması yaşanır. Kurumun imajı zedelenmez.
Düşük	2	Riskin bilgi varlıkları üzerinde etkisi düşüktür. Az miktarda ve bilgi kaybı, az süreyle hizmet kesintisi ya da varlığın bütünlüğünün bozulması yaşanır. Kurumun imajı zedelenmez.
Çok Düşük	1	Riskin bilgi varlıkları ve hizmetler üzerindeki etkisi ihmal edilebilir.

4.1.4 Risk Hesaplama Yöntemi

Risk, varlık değeri, olasılık ve etkinin fonksiyonudur ve aşağıdaki formül ile hesaplanır.

Risk = [Toplam (Varlık Değeri)] x [Olasılık] x [Maksimum (İş Etkisi)]

4.1.5 Risk Değerlendirme Sonuçlarının Onaylatılması

Risk değerlendirme sonuçları, risk sahiplerine sunularak onaylatılır ve kayıtlar en az 5 yıl süreyle saklanır.

4.2 Risklerin İşlenmesi

4.2.1 Önceliklendirilme

Risk değerlendirme çalışmaları kapsamında 3-225 puanla değerlendirilen riskler, aşağıdaki tabloya göre öncelik kazanır.

RİSK DEĞERİ	RİSK ÖNCELİĞİ	EYLEM
150-225	Kritik Risk	Risk değerinin, en geç 3 ay içerisinde kabul edilebilir risk değerine düşürülmesi hedeflenerek, eylemler planlanır
50-149	Önemli Risk	Risk değerinin, en geç 6 ay içerisinde kabul edilebilir risk değerine düşürülmesi hedeflenerek, eylemler planlanır
3-49	Kabul Edilebilir Risk	Herhangi bir eylem planlanmak zorunda değildir

4.2.2 Eylemlerin Belirlenmesi

Risk işleme amacıyla aşağıdaki dört temel eylem türü kullanılır.

- Azaltma / Kontrol
  - Fiziksel/Çevresel
  - Teknik
  - Yönetsel
- Kaçınma
- Aktarma
- Kabul Etme

Risk işlemede, kontroller aracılığıyla riskin azaltılarak kabul edilebilir risk seviyesine düşürülmesi hedeflenir.

Kontroller belirlenirken fayda/maliyet değerlendirmesi yapılır. Herhangi bir riskin bertaraf edilmesi için gerekli maliyetin, riskin ortaya çıkması durumundaki maliyetten küçük olmasına dikkat edilir.

Kontroller aracılığıyla düşürülemeyen riskler için, diğer risk işleme eylemleri olan riskten kaçınma, riski aktarma ya da riski kabul etme değerlendirilebilir.

4.2.3 Risk İşleme Eylemlerinin Onaylatılması

Risk işleme eylemleri ile eylemler sonrasında kalması beklenen artık riskler, plan haline getirilir ve risk sahiplerine sunularak onaylatılır. Risk işleme kayıtları en az 5 yıl süreyle saklanır.

4.2.4 Risk İşleme Eylemlerinin Uygulanması

Risk sahiplerine onaylatılan eylemler, BGYS Komisyonu tarafından belirlenen kişi ya da ekiplerce, önceliklerine uygun şekilde planlama yapılarak uygulanır. Eylemlerin izlenmesi ve risk sahibine raporlanması, BGYS Komisyon Başkanı'nın sorumluluğundadır.

4.2.5 Risk Planı

SDÜ1PR02 BGYS Risk Yönetimi Prosedürü kapsamında yürütülen risk değerlendirme ve risk işleme faaliyetlerine ilişkin kayıtlar, SDÜ5PN02 BGYS Risk Planı aracılığıyla kayıt altına alınır ve söz konusu kayıtlar en az 5 yıl süreyle saklanır.