1. AMAÇ

Bu prosedürün amacı, iş sürekliliği açısından değerli olan iş bileşenlerine yönelik iç veya dış kaynaklı tehlikeleri ve bu tehlikelerin gerçekleşmesi durumunda meydana gelebilecek maddi veya manevi iş kayıplarını tespit etmek için kullanılacak yöntemler ile gerekli önlemlerin planlanması sürecini belirlemektir.

2. KAPSAM

Bu prosedür Bahçeşehir Üniversitesi ve Bilgi İşlem Daire Başkanlığı uhdesindeki tüm donanımı, yazılımı ve personellerini kapsar.

3. SORUMLULUKLAR

Bu prosedürün uygulanmasından BİDB sorumludur.

4. TANIMLAR

4.1. BİDB: Bilgi İşlem Daire Başkanlığı.

4.2. BAU: Bahçeşehir Üniversitesi.

4.3. Varlık: Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır. İnsan, bilgi, yazılım, donanım, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir.

4.4. Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: Şifreli e-posta gönderimi ile epostanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)

4.5. 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)

4.6. Erişilebilirlik/Kullanılabilirlik: Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifade ile, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Ör: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şasilerinde yedekli güç kaynağı kullanımı). Bu dokümanda “Erişilebilirlik” olarak kullanılacaktır.

4.7. Varlık Sahibi: Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi veya kişilerdir. Sahip kelimesi Türkçe de mülkiyet anlamını içinde barındırmaktadır. BGYS Varlık yönetimindeki sahip kavramı daha çok sorumluluk anlamında kullanılmaktadır. Varlık değerinin belirlenmesi, varlığa yönelik risk

tanımlamalarının yapılması varlık sahibinin görevleri arasındadır. (Ör: Kurum finansal bilgilerinin sahibi kurumun finans bölüm müdürüdür).

4.8. Tehdit: Herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir.
4.9. Tehdit Kaynağı: Varlıklara zarar verme potansiyeli olan olaylar ve durumlar.
4.10. Açıklık / Zafiyet: Sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır.
4.11. Olasılık: Bir olayın gün, hafta, ay, yıl gibi bir zaman dilimi içerisinde gerçekleşme durumunu ifade eder.
4.12. Etki: Tehlikenin oluşması durumunda birime vereceği zararı, hedef ve faaliyetler üzerindeki etkisini gösterir.
4.13. Risk Derecelendirme: Varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir.
4.14. Risk Değerlendirme: Tehlikelerden kaynaklanan riskin büyüklüğünü tahmin etmek ve mevcut kontrollerin yeterliliğini dikkate alarak riskin kabul edilebilir olup olmadığına karar vermek için kullanılan proses.
4.15. Risk Analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.
4.16. Risk İşleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması prosesi.

5. UYGULAMA

5.1. Birim Varlıklarının Belirlenmesi

İşin gerçekleştirilmesi için ve iş sürekliliği için gerekli olan tüm maddi ve manevi varlıklar birim varlıklarını oluştururlar. Bu varlıklar kullanım amaçları, işe etkileri, maddi ve manevi değerleri ile zayıflıklara karşı tehdit altında olabilirler. Kurum bünyesindeki varlıkların sınıflandırılarak belirlenmesi ve tanımlanması aşağıdaki tablodaki gibi yapılmıştır.

Varlık Sınıfı	**Açıklama**
Fiziksel Varlıklar	Birimde kullanılan fiziksel varlıklardır. **Alt Kategoriler:** a) Bilgisayar Ekipmanları (bilgisayar, sunucu, işlemci, dizüstü bilgisayarlar, modemler vb.); b) İletişim Ekipmanları (yönlendirici, telefon, faks vb.); c) Yedekleme Kayıt Ortamları (Storage, NAS vb.); d) Diğer Teknik Ekipmanlar (UPS kaynakları, havalandırma üniteleri vb.);

Yazılım Varlıkları	Projelerin gerçekleştirilmesinde kullanılan her türlü bilgisayar programı, işletim sistemi ve yardımcı yazılımlar **Alt Kategoriler:** e) Uygulama Yazılımları f) Sistem Yazılımları g) Geliştirme Araç ve Yazılımları h) Diğer
Bilgi Varlıkları	Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir. **Alt kategoriler:** i) Veri tabanları; j) Veri Dosyaları; k) Basılı Materyal (sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, destek uygulamaları, sözleşmeler; vb.) l) Arşivlenmiş Bilgi; m) Diğer (Yukarıdaki alt kategoriler dışında bulunan bilgi varlıklarıdır.)
Servisler (Hizmetler)	Bilgi İşleme ve Haberleşme servisleri (web servisi, ftp servisi)
İnsan Kaynağı	Faaliyetlerimizi gerçekleştirirken farklı pozisyonlarda görev yapan ve iş sonuçlarına doğrudan veya dolaylı etkisi olan tüm personelimiz

5.2. Bilgi Varlığı Güvenlik Sınıflandırılması

Bilgi varlığı güvenlik sınıflandırması aşağıdaki gibi kategorilendirilmiştir.

Sınıflandırma	Tanımlama
Çok Gizli	Bilgi varlıkları; güvenliği sağlanmış ve sadece yetkili kişilerin girebileceği odalarda bulunan kasa ya da kilitli dolaplarda saklanan bilgilerdir. Kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar yakılarak ya da birleştirilemeyecek derecede parçalanarak imha edilmelidir.
Gizli	Kurumun faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda güvenliği, saygınlığı ve çıkarları ciddi derecede zedeler. Gönderilen makamı ilgilendiren, sadece o makamın görebileceği bilgi türüdür. İş planları, fiyat teklifleri, sözleşmelerle ilgili bilgiler gizli kategorisine örnek olarak verilebilir. Kasa ya da kilitli ortamda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir.

Kuruma Özel	Kurum dahilin de üretilen; yönergeler, standartlar, prosedürler, politikalar ve bu bilgilerin bulunduğu ortamlar vb. gibi, Kurum dışına çıkarılması için üst yönetimden onay alınması gereken bilgi varlıklarıdır. Kurum içinde kullanımında, kopyalanmasında sakınca yoktur. Ancak yukarıda belirtilen dokümanlardan içeriği itibarı ile sadece kurumdaki yetki verilmiş kişilerin erişebileceği dokümanların gizlilik derecesinin kuruma özel olarak değil, uygun olan şekilde (çok gizli, gizli, gibi) verilmesi gerekir.
Hizmete Özel	Sadece belli bir grup tarafından örneğin proje ekibi, belli bir birim gibi görülebilecek olan bilgi varlıklarıdır. İçerdiği konular itibariyle, diğer gizlilik dereceli konular dışında olan ancak güvenlik işlemine ihtiyaç gösteren bilgi varlıkları hizmete özel olarak sınıflandırılır. Projeler özelinde üretilen proje planı, tasarım ve gerekli dokümanları, kaynak kodlar ve bu bilgilerin bulunduğu ortamlar vb. örnek olarak verilebilir. Gizli varlıklar gibi, yetkili kişi izni ile kopyalama, iletme ve imha işlemi yapılmalıdır.
Yayınlanabilir, Umumi (Kamuya açık)	Kullanılması güvenlik açısından önemli olmayan, kurumdaki veya kurum dışındaki her kişiye açık bilgilerdir. Örneğin duyurular vb.

5.3. Varlıkların Değerlendirilmesi

Varlıkların değerlendirilmesi aşağıdaki tablodaki şeklinde değerlendirilmiştir.

Güvenlik Hedefi	Düşük (1)	Orta (2)	Yüksek (3)	Çok Yüksek (4)
Gizlilik	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi çok az etkiler veya etkilemez. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Bütünlük	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi çok az etkiler veya etkilemez. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Erişilebilirlik	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi çok az etkiler veya etkilemez. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilginin kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

Ayrıca Varlık değeri belirlenirken Bilgi Güvenliği Yönetim Sisteminin Temeli olan Gizlilik, Bütünlük ve Erişilebilirlik açısından değerlendirme yapılır. Bu değerlendirme aşağıdaki yöntem ile belirlenir.

VARLIK DEĞERİ= GİZLİLİK x BÜTÜNLÜK x ERİŞİLEBİLİRLİK
Varlık Değeri≥ 50 ise Çok Gizli **50>Varlık Değeri≥ 25 ise Gizli** **25>Varlık Değeri≥ 10 ise Kuruma Özel** **10>Varlık Değeri ≥ 5 ise Hizmete Özel 5>Varlık Değeri ise Kamuya açık**

5.4. Risk Yönetimi

5.4.1. 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 (kullanıcıya 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.

Risk (R) = VARLIK DEĞERİ x OLASILIK x ETKİ

5.4.2. Risk Olasılık Değerinin Belirlenmesi.

Risklin gerçekleşme olasılığı, bu riskin kurumda gün, hafta, ay, yıl gibi bir zaman dilimi içerisinde gerçekleşme durumunu ifade eder. Riskin analizi yapılırken "Olasılık" sütunu aşağıdaki tablo dikkate alınarak doldurulur.

Riskin Olasılığı	**Derecesi**	**Riskin Gerçekleşme Olasılığı**
Çok Yüksek (Kesinlikle)	5	Risk durumu birçok kez gerçekleşti ve şu anda da gerçekleşiyor.
		Riskin meydana geleceği neredeyse kesindir.
Yüksek (Büyük Olasılıkla)	4	Risk durumu birçok kez gerçekleşti.
		Benzer durum kurum /birim/ bölüm içerisinde gerçekleşti
		Ortam gerçekleşmesi için son derece uygundur.
		Riskin meydana gelme ihtimali yüksektir.
Orta (Mümkün)	3	Risk ancak belirli durumlarda gerçekleşebilir.
		Benzer durum kurum / birim/bölüm süreçlerinde belirli durumlarda kısmen gerçekleşti.
		Ortam riskin gerçekleşmesi için uygun olabilir.
		Riskin meydana gelme ihtimali orta derecededir.
Düşük (Muhtemelen)	2	Risk durumu ancak çok özel koşullar altında söz konusu olabilir.
		Benzer durum kurum / birim/bölüm süreçlerinde ancak çok özel durumlarda gerçekleşebilir.
		Ortam gerçekleşmesi için uygun değildir.
		Riskin meydana gelme ihtimali düşüktür.
Çok Düşük (Nadir)	1	Risk çok istisnai durumlarda meydana gelebilir. Önlemeye yönelik kontrollerle hata yok edilmiştir.

5.4.3. Etki Faktörünün Belirlenmesi.

Riskin oluşması durumunda birime vereceği zararı, hedef ve faaliyetler üzerindeki etkisini gösterir. Aşağıdaki tabloya göre riskin etki değeri belirlenerek "Etki Faktörü" sütununa işlenir.

Etki	Derecesi	Riskin Etkisi
Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun ciddi zarara uğramasına (maddi, önemli servislerin durması vb) yol açabilecek önemdeki varlıklar.	5	Çok Yüksek
Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. Değiştirilmesi durumunda kurumun içerisinde telafi edilebilecek bilgiler. Çok sayıda lokasyon için ana hizmet kesintisine ya da personel/öğrenci memnuniyetsizliğine sebep olabilecek varlıklar.	4	Yüksek
Kurum/çalışanlar/paydaşlar ve yönetim üzerinde orta seviyede memnuniyetsizlik yaşatır. Tüm kurum tarafından bilinmesinde sakınca olmayan bilgilerdir. Değiştirilmesi durumunda ilgili grup içerisinde telafi edilebilecek bilgilerdir. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir.	3	Orta
Kurumun bazı önemli olmayan varlıkları etkilenebilir. Kurumun çıkarları, misyonu ve prestiji küçük çaplı zarar görebilir veya etkilenebilir. Değiştirilmesi durumunda kurumun süreçlerini etkilemeyecek bilgilerdir. Herkes tarafından bilinmesinde sakınca yoktur.	2	Düşük
Riskin gerçekleşmesi, finansal kayıplar, mevzuata aykırılık ve de itibar ve saygınlığın kaybedilmesine sebep olmaz. Kurum/çalışanlar/paydaşlar ve yönetim üzerinde çok düşük seviyede memnuniyetsizlik yaşatır. Değiştirilmesi durumunda kurumun süreçlerini etkilemeyecek bilgilerdir. Herkes tarafından bilinmesinde sakınca yoktur.	1	Çok Düşük

5.4.4. Risk Etki Büyüklüklerinin Sınıflandırılması ve Değerlendirilmesi.

Değerlendirme yapılırken L-tipi matris (5x5 Matris) yöntemi kullanılır. Risk değeri, olasılık, etki bileşkesinden hesaplanır.

L Tipi Matris Yöntemi: Her bir kriter için aşağıda verilen puan cetveli doğrultusunda puanlama yapılır:

OLASILIK	Zararın Gerçekleşme Olasılığı (Olasılık)		
	Skor	**Olasılık (İhtimal)**	**Açıklama**
	5	Hergün	Çok Yüksek
	4	Haftada Bir	Yüksek
	3	Ayda Bir	Orta
	2	Üç İla Altı Ayda Bir	Düşük
	2	Çok Düşük	Hemen Hemen Hiç

ETKİ	Şiddet Skor	Şiddet Puanlama Kriterleri	Açıklama
	5	Düzeltici önlemlerin alınması şarttır. Hemen çalışma yapılmalı.	Çok Yüksek Risk
	4	Düzeltici önlemlerin alınması gerekmektedir. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır. Hemen Çalışma Yapılmalı	Yüksek Risk
	3	Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır. Mümkün Olduğunca Çabuk Müdahale edilmeli	Orta Risk
	2	Acil Tedbir Gerektirmeyebilir, Dikkatli Olunmalı ,önlem alınıp alınmayacağı sistem sahibi /sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.	Düşük Risk
	1	Önlemeye yönelik kontrollerle hata yok edilmiştir.	Etkisiz Risk (KabulEdilebilir)

Risk = Olasılık x Etki (Şiddet)

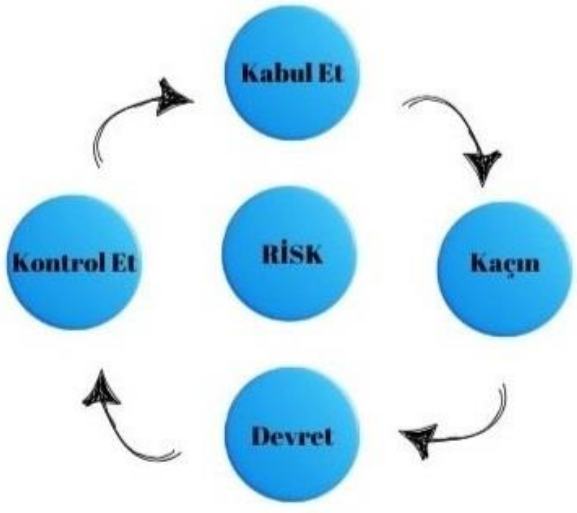
Olasılık ve Şiddet (Etki) Değerlendirmesi						
RİSK		ZARAR VERME ETKİ DERECESİ				
		ÇOK HAFİF	HAFİF	ORTA DERECE	CİDDİ	ÇOK CİDDİ
OLASILIK	ETKİSİZ RİSK 1	DÜŞÜK 1	DÜŞÜK 2	DÜŞÜK 3	DÜŞÜK 4	DÜŞÜK 5
	DÜŞÜK RİSK 2	DÜŞÜK 2	DÜŞÜK 4	DÜŞÜK 6	ORTA 8	ORTA 10
	ORTA DERECE 3	DÜŞÜK 3	DÜŞÜK 6	ORTA 9	ORTA 12	YÜKSEK 15
	YÜKSEK 4	DÜŞÜK 4	ORTA 8	ORTA 12	YÜKSEK 16	YÜKSEK 20
	ÇOK YÜKSEK 5	DÜŞÜK 5	ORTA 10	YÜKSEK 15	YÜKSEK 20	YÜKSEK 25

Bulunan risk derecesi çok yüksek, yüksek, orta, düşük ve etkisiz seviyelerde Risk Değerlendirme Tablosu üzerinde ilgili aralıkta puanlanır. Etkisiz Risk seviyesinden yukarı çıkması durumunda önleyici tedbirler alınarak yeniden risk değerlendirmesi yapılır ve Etkisiz Risk seviyesine düşürülür. Etkisiz Risk seviyesine çekilemeyen riskler artık risk olarak değerlendirilir ve artık risk onayıyla kurum yetkilisi tarafından onaylanır.

5.4.5. 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 şu şekilde sıralayabiliriz;

- *Riskin Kabulü:* Riskin var olduğunu kabul ederek BT sistemlerini kullanmaya devam etmektir.
- *Riskten Kaçınma:* Riski yaratan sebebi ortadan kaldırmak, İşi gerçekleştirmenin başka yollarını aramak, Var olan hizmeti sonlandırmak, bazı faaliyetleri durdurmak olarak tanımlanabilir. (örneğin bir yazılımın risk yaratan kısmının yüklenmemesi ve kullanılmaması gibi)
- *Riskin Azaltılması:* Açıklığın gerçekleşmesi halinde oluşacak etkinin uygulanan kontroller ile azaltılması. Karşılaşılabilecek riskler tanımlandıktan sonra bu risklerin etkisini veya gerçekleşme olasılıklarını azaltmak için ek önlemler alarak, riske yanıt verme planı oluşturma çalışmasıdır.
- *Riskin Transferi:* Riskin gerçekleşmesi durumunda oluşabilecek zararı karşılayacak çözümler bularak (örneğin sigorta yaptırmak), Riski bir başka kuruma veya bireye devretme. Bu uygulamada aslında risk yok edilmiş olmayacaktır, sadece riskin sorumluluğunun başkası tarafından yüklenilmesi sağlanacaktır. Risk, riskin transfer edildiği birimde analiz edilmelidir.



Kabul Edilebilir Risk/ Etkisiz Risk seviyesi yönetim tarafından 1-25 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.

5.4.6. Risk Sahiplerinin Belirlenmesi.

Her bir risk için, risk sahibi (riskten sorumlu olan kişi veya kurumsal birim) belirlenmelidir. Bu kişi varlık sahibiyle aynı kişi olmayabilir.

5.4.7. Fırsatların Belirlenmesi.

Risk analizi ile birlikte süreç ya da varlık bazında fırsatların belirlenmesi için çalışma yapılır. Fırsatları belirlemek için, proses / varlık bazında yapılan risk analizi sonucunda fırsat olarak görülen noktalar dikkate alınarak çalışma yapılır.

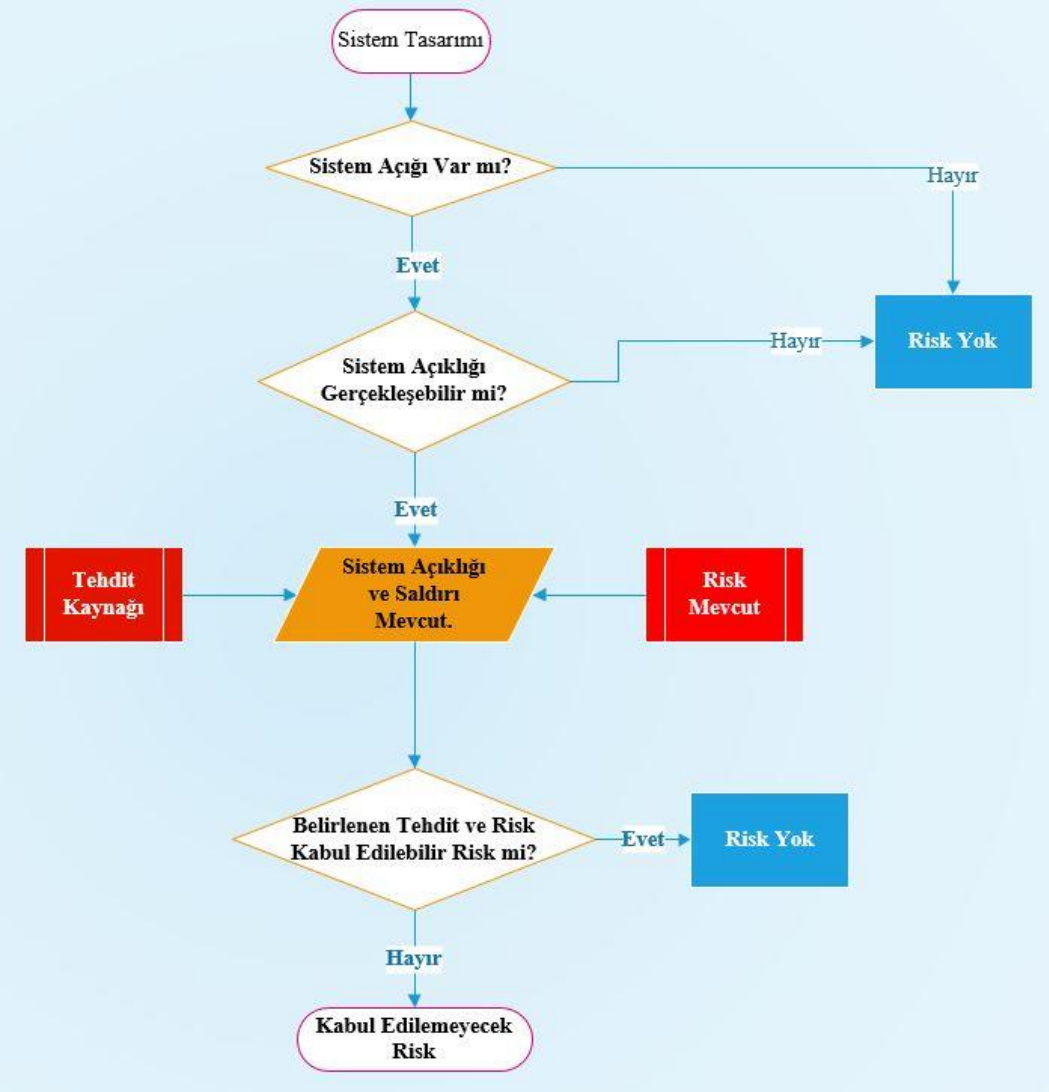
5.4.8. Risk ve Fırsatları Ele Alma Faaliyetlerinin Değerlendirilerek Revizyonu.

Risk süreçleri ilgili süreç sorumluları tarafından;

- Verilen hizmette bir değişiklik olduğunda,
- İç Tetkik veya belgelendirme denetimlerinde majör uygunsuzluk olması halinde,
- Yasal mevzuat değişikliklerinde
- Yetkili kurumlar tarafından ceza verildiğinde
- Tedarikçi denetimlerinde bulunan bulgular olduğunda
- Fırsata çevrilen riskler ile ilgili alınan aksiyonlar devreye alındığında
- Herhangi bir değişiklik söz konusu olmasa bile yılda bir kez
- İlgili tarafların bağlam veya gereksinimlerinde değişiklik olduğunda,

Risk analizi kontrol edilir ve gerek görüldüğü takdirde revize edilir.

5.4.9. Risk Analizi İş Akış Diyagramı.



Yukarıdaki akış diyagramında bulunan riskler için karar adımları ile ilgili uygulanan bazı yaklaşımlar şunlardır;

- Eğer açıklık mevcutsa açıklığın uygulanma olasılığını azaltacak kontroller uygulanır.
- Eğer açıklık gerçekleşebiliyorsa kademeli güvenlik anlayışı, güvenli mimariler ve yönetimsel kontroller kullanılarak risk azaltılır.
- Saldırının maliyeti saldırı sonucu elde edilecek kazançtan fazlaysa saldırganın maliyetlerini arttıracak ve motivasyonunu düşürecek önlemler alınır.
- Tahmini kayıp çok büyük olduğunda doğru tasarım prensipleri, güvenli mimariler, teknik ve teknik olmayan kontroller kullanarak saldırının yaratacağı kayıp azaltılır.

5.4.10. Artık Risk.

Uygulanan kontroller var olan riski tamamen ortadan kaldırmadığı durumlarda risk işleme sonrası kalan riske artık risk adı verilir. Uygulanan kontroller sonrası artık risk belirlenir. Eğer bulunan risk seviyesi kabul edilebilir risk seviyesinin üzerinde ise risk analizi ve risk işleme tekrar yapılır, eğer bulunan artık risk seviyesi kabul edilebilir riskin altında ise artık risk dokümante edilmelidir ve varlığı yönetim tarafından onaylanıp kabul edilir.