1. AMAÇ

Bu prosedürün amacı, Entegre Yönetim Sistemi uygulamaları kapsamında iş sürekliliği açısından varlık değeri olan iş bileşenlerine iç veya dış kaynaklı olarak gelebilecek tehlikeler ve bu tehlikelerin vuku bulması durumunda ortaya çıkabilecek maddi veya manevi iş kayıplarını tespit edecek yöntemler ve gerekli önlemlerin planlanması için izlenecek yolu belirlemektir.

2. KAPSAM

Bu prosedür, Entegre Yönetim Sistemi uygulamaları neticesinde kurumun tüm donanımı, yazılımı ve personellerini kapsar.

3. SORUMLULUK

Bu prosedürün yürütülmesinden Yönetim Temsilcisi, uygulanmasından Süleyman Demirel Üniversitesi Rektörlüğü idari birimleri tüm çalışanları doğrudan sorumludur.

4. TANIMLAR

4.1. Entegre Yönetim Sistemi: ISO 27001 BGYS, ISO 9001 KYS, ISO 20000-1 HYS ve ISO 22301 İSYS ve ISO 27701 KVYS standartlarını kapsar.

4.2. 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.

4.3. 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)

4.4. 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)

4.5. 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.

4.6. 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)

4.7. Tehdit: Herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir.

4.8. Tehdit Kaynağı: Varlıklara zarar verme potansiyeli olan olaylar ve durumlar

4.9. Açıklık / Zaafiyet : Sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır.

4.10. Olasılık: Bir olayın gün, hafta, ay, yıl gibi bir zaman dilimi içerisinde gerçekleşme durumunu ifade eder.

4.11. Etki: Tehlikenin oluşması durumunda birime vereceği zararı, hedef ve faaliyetler üzerindeki etkisini gösterir.

4.12. Risk Derecelendirme: Varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir.

4.13. Risk Değerlendirme: Tehlikelerden kaynaklanan riskin büyüklüğünü tahmin etmek ve mevcut kontrollerin yeterliliğini dikkate alarak riskin kabul edilebilir olup olmadığına karar vermek için kullanılan proses.

4.14. Risk analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.

4.15. Risk işleme: 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 bünyesinde varlıklarımız şu şekilde sınıflandırılır ve tanımlanır.

VARLIK SINIFI	AÇIKLAMA

Fiziksel Varlıklar:	Birimde kullanılan fiziksel varlıklardır. **Alt kategoriler:** a) Bilgisayar ekipmanları (bilgisayar, sunucu, işlemci, diz üstü bilgisayarlar, modemler vb.); b) İletişim ekipmanları (yönlendirici, telefon, faks vb.); c) manyetik kayıt ortamları (teyp, kartuş, disket, disk, cd vb.); d) Diğer teknik ekipmanlar (güç kaynakları, adaptör, 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) Veritabanları; j) Veri dosyaları; k) Basılı materyal (sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, sözleşmeler; vb.) l) Arşivlenmiş bilgi; m) Diğer (Yukarıdaki alt kategoriler dışında bulunan bilgi varlıklarıdır.)
Servisler (Hizmetler)	Bilgi işleme 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. Varlıkların Değerlendirilmesi

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

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

5.3. Bilgi Varlığı Güvenlik Sınıflandırması

Bilgi varlığı aşağıdaki kategorilerde sınıflandırılabilir:

Varlık Değeri	Sınıflandırma Seviyesi	Bilgi Sınıflandırma Karşılığı	Tanımlama
50 – 64	**Çok Yüksek**	**Çok Gizli**	Sadece üst yönetim ve belirli yetkililer erişebilir. İfşası kurumun bekasını tehlikeye atar. 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.
25 – 49	**Yüksek**	**Gizli**	Kurumun faaliyetini devam ettirebilmesi için kritik olan ve yetkisiz kişilerin eline geçmesi durumunda güvenliği, saygınlığı ve çıkarları ciddi derecede zedeler. Sadece ilgili birim ve süreç sahipleri erişebilir. İfşası yasal yaptırım veya yüksek zarar doğurur. Kasa ya da kilitli ortamda saklanmalı; kopyalama, iletme, imha için yetkili kişinin onayı alınmalıdır. Bu varlıklar, yakılarak ya da birleştirilmeyecek derecede parçalanarak imha edilmelidir
10 - 24	**Orta**	**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.

5 - 9	**Orta**	**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.
0 - 4	**Düşük**	**Yayınlanabilir, umumi (Kamuya açık)**	Kullanılması güvenlik açısından önemli olmayan, kurumdaki veya kurum dışındaki her kişiye açık bilgilerdir. Örneğin duyurular vb.

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

5.4.1.1. Riskin 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.

Risk Olasılık Derecesi	Olasılık Tanımı	Gerçekleşme Sıklığı	Detaylı Açıklama
1	Çok Düşük	Yılda bir den daha az	Kurumda geçmişte hiç yaşanmamış veya yalnızca teorik olarak mümkün olan olaylardır. Güçlü ve etkin kontroller

Risk Olasılık Derecesi	Olasılık Tanımı	Gerçekleşme Sıklığı	Detaylı Açıklama
			mevcuttur. Olayın gerçekleşmesi olağan dışı koşullara bağlıdır.
2	Düşük	Yılda bir	Nadiren gerçekleşir. Geçmişte istisnai olarak yaşanmış olabilir. Mevcut kontroller genel olarak etkilidir ancak kontrol zafiyeti oluşması durumunda risk ortaya çıkabilir.
3	Orta	Altı ayda bir	Benzer olaylar kurum içinde veya sektörde yaşanmıştır. Kontroller mevcuttur ancak insan hatası, süreç eksiklikleri veya çevresel faktörler nedeniyle riskin gerçekleşmesi mümkündür.
4	Yüksek	Üç ayda bir	Olayların daha önce tekrar ettiği veya sık yaşandığı görülmüştür. Kontroller yetersizdir ya da tutarlı şekilde uygulanmamaktadır. Riskin gerçekleşmesi beklenen bir durumdur.
5	Çok Yüksek	Ayda bir veya daha sık	Olaylar düzenli olarak yaşanmaktadır veya yaşanması kaçınılmazdır. Kontroller yoktur veya etkisizdir. Acil iyileştirme aksiyonları gereklidir.

5.4.1.2. 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.

Risk Etki Derecesi	Riskin Etkisi	Etki Tanımı
1	Çok Düşük	İhmal edilebilir düzeyde etki vardır. Kurumsal faaliyetler, hizmetler ve itibar üzerinde anlamlı bir etkisi yoktur. Riskin gerçekleşmesi, finansal kayıplar, mevzuata aykırılık ve de itibar ve saygınlığın kaybedilmesine sebep olmaz.
2	Düşük	Küçük çaplı operasyonel aksaklıklar oluşur. Kısa sürede telafi edilebilir, hizmet sürekliliği etkilenmez.
3	Orta	Süreçlerde aksama veya gecikme yaşanır. Hizmetler devam eder ancak düzeltici faaliyet gerektirir. İtibar etkisi sınırlıdır.

Risk Etki Derecesi	Riskin Etkisi	Etki Tanımı
4	Yüksek	Temel hizmetlerde önemli kesinti yaşanır. Mali kayıp oluşur. Bilgi güvenliği ihlali veya paydaş memnuniyetsizliği meydana gelir.
5	Çok Yüksek	Kurum faaliyetleri ciddi şekilde durur. Yasal yaptırım, ağır mali kayıp veya ciddi kişisel veri ihlali meydana gelir. Kurumsal itibar ağır zarar görür.

5.4.1.3. Risk Etki Büyüklüklerinin Sınıflandırılması Ve Değerlendirilmesi

- **Varlık Değeri = Gizlilik (1–4) × Bütünlük (1–4) × Erişilebilirlik (1–4)**
- **Risk Büyüklüğü (R) = Varlık Değeri × Olasılık (1–5) × Etki (1–5)**

Hesaplanan risk büyüklüğü **1–1600** aralığındadır ve aşağıdaki kriterlere göre sınıflandırılır.

Risk Değeri Aralığı	Risk Seviyesi	Tanım	Yönetim / Aksiyon	Renk
1 – 192	**Etkisiz Risk (Kabul Edilebilir)**	Riskin etkisi ihmal edilebilir düzeydedir veya mevcut önleyici kontroller ile risk ortadan kaldırılmıştır.	Mevcut kontroller yeterlidir. Risk izlenir, ilave aksiyon gerektirmez.	Açık Yeşil
193 – 384	**Düşük Risk**	Kurumsal hedefler üzerinde sınırlı etkiye sahiptir.	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından değerlendirilir. İlave önlem alınmayacaksa risk kabul edilir.	Sarı
385 – 768	**Orta Risk**	Kurumsal faaliyetleri olumsuz etkileyebilir.	Alınacak önlemler ve uygulama yöntemi için makul süre içinde aksiyon planı hazırlanır ve uygulanmaya başlanır.	Turuncu
769 – 1024	**Yüksek Risk**	Kurum için önemli düzeyde tehdit oluşturur.	Düzeltici önlemler alınmalıdır. Sistem çalışmaya devam edebilir; ancak önlemler ivedilikle belirlenmeli ve uygulanmalıdır.	Kırmızı

Risk Değeri Aralığı	Risk Seviyesi	Tanım	Yönetim / Aksiyon	Renk
1025 – 1600	**Çok Yüksek Risk**	Kurum açısından kabul edilemez düzeyde risktir.	Düzeltici önlemlerin alınması zorunludur. Gerekli görüldüğünde faaliyet durdurulur. Derhal aksiyon alınır.	Koyu Kırmızı

Risk büyüklüğü aralıkları, varlık değerinin maksimum değeri (64) ile olasılık ve etki kombinasyonları dikkate alınarak, kuruluşun risk iştahına uygun şekilde belirlenmiştir.

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.

5.4.2. 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 şunlardır:

- 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- 192 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.

5.4.3. Risk Sahiplerinin Belirlenmesi

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

5.4.4. Fırsatların Belirlenmesi

Risk analizi ile birlikte proses yada 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.

5.4.5. Risk ve Fırsatları Ele Alma Faaliyetlerinin Değerlendirmesi ve Revizyonu

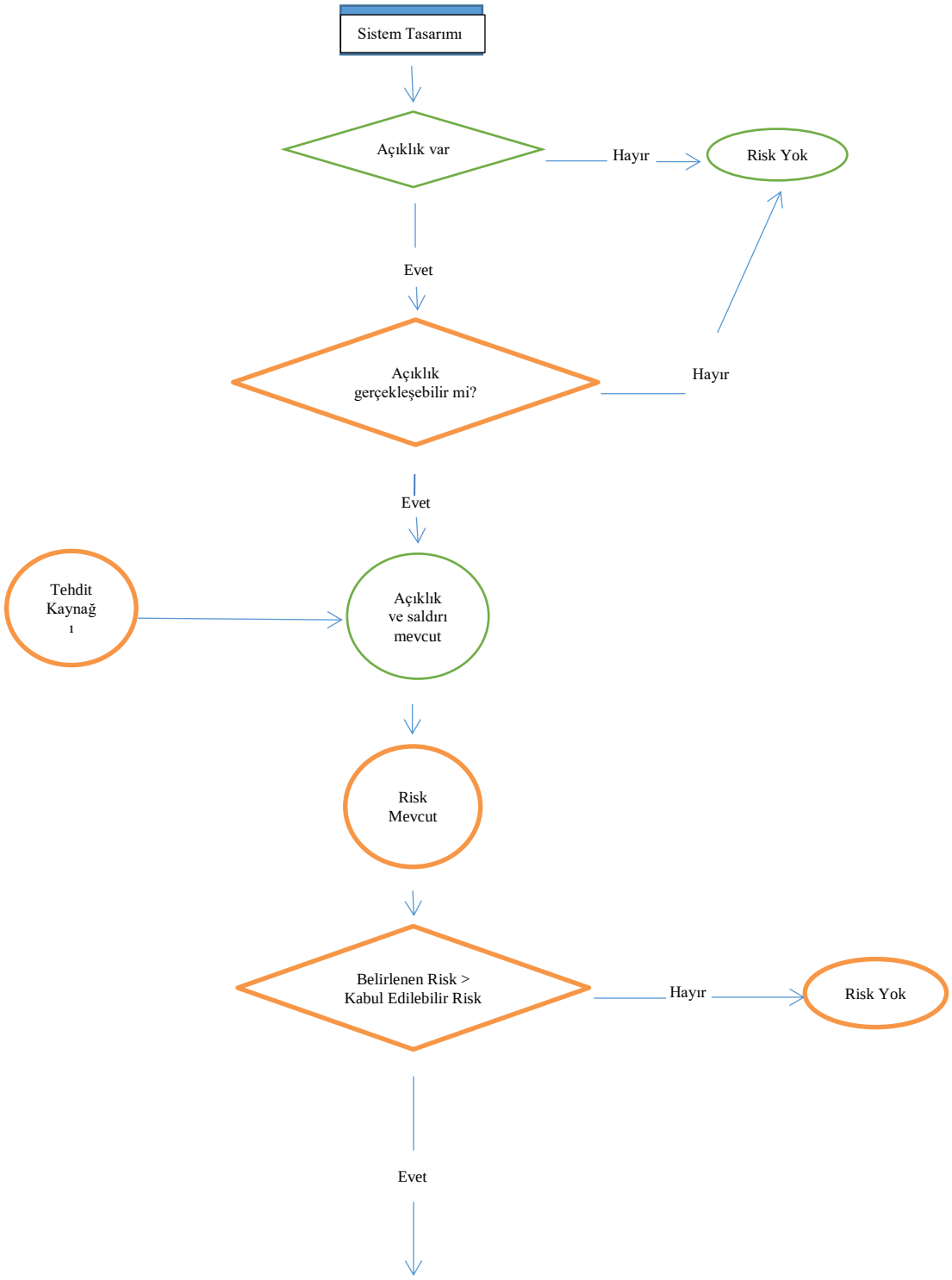
Riskler BGYS Komitesi ve süreç sahipleri tarafından;

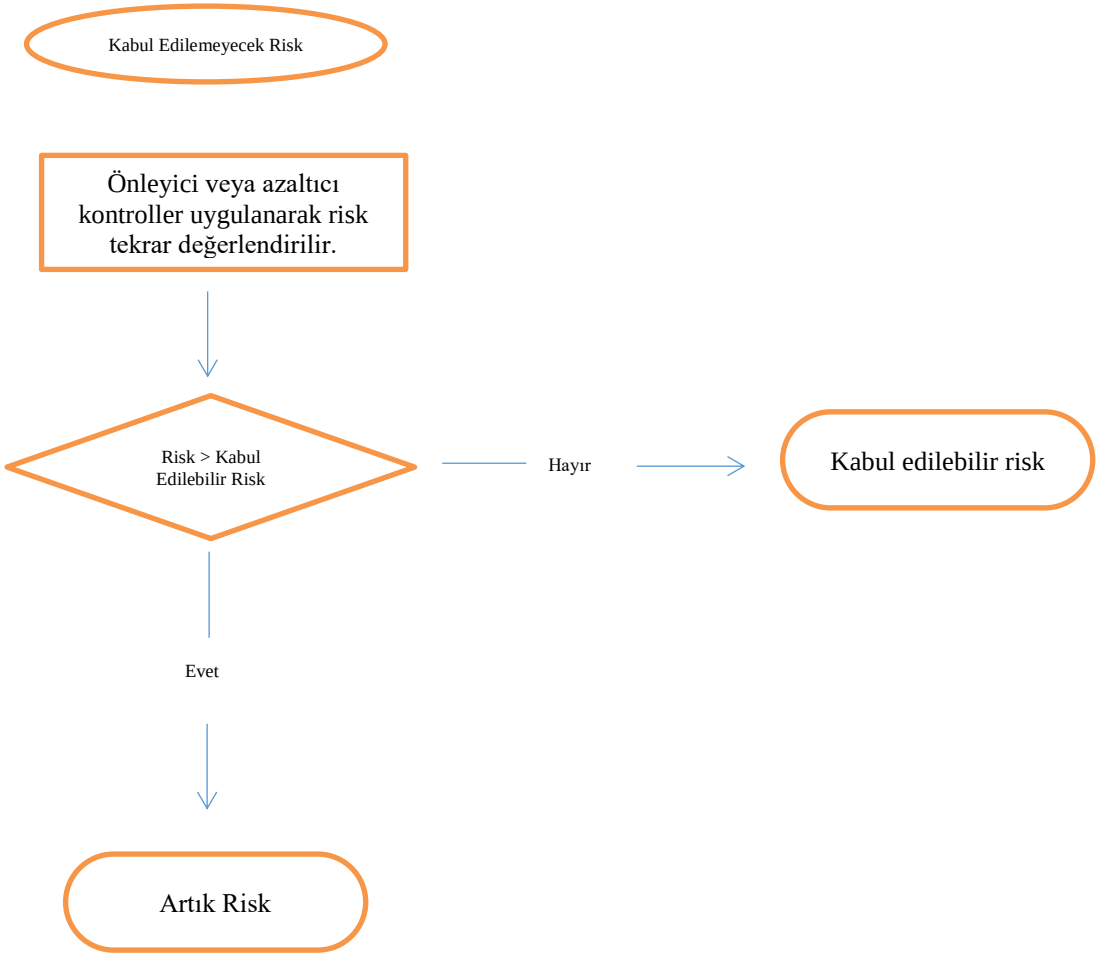
- Verilen hizmette bir değişiklik olduğunda
- İç Tetkik veya belgelendirme denetimlerinde major uygunsuzluk olması halinde
- Yasal mevzuat değişikliklerinde
- Yetkili kurumlar tarafından ceza verildiğinde
- Tedarikçi denetimlerinde bulunan bulgular olduğunda

- 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 gözden geçirilir ve gerektiğinde revize edilir.

Risk Analizi İş Akışı





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.

5.4.6. Artık RİSK

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.

6. İLGİLİ DOKÜMANLAR

- FR-009 Artık Risk Formu
- PL-005 Risk ve Fırsatları Değerlendirme Planı
- LST-024 Risk İzleme Tablosu
- LST-028 Tehdit Listesi
- LST-029 Zayıflık Listesi
- DD-001Varlık Envanteri
- İA-034 Risk Analizi İş Akışı

7. REVİZYON TAKİP TABLOSU

REVİZYON NO	TARİH	AÇIKLAMA
000	22.01.2020	İlk yayın.
001	09.09.2022	Prosedür içeriği değiştirilmiş ve entegre yönetim sistemlerine geçildiğinden Tek bir Risk değerlendirme ölçümü belirlenmiş ve uygulanmaktadır.
002	22.01.2024	Kontrol kısmı güncellenmiştir.
003	22.12.2024	Tanımlar kısmında EYS: Entegre Yönetim Sistemi (BGYS, KYS, HYS, İSYS, KVYS) olarak güncellenmiştir.
004	24.12.2025	Risk olasılık tanımlamaları güncellendi.