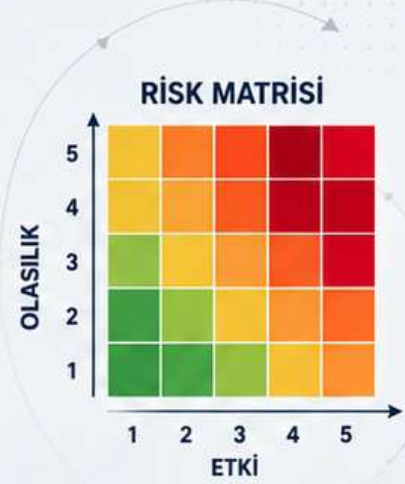




T.C.
KASTAMONU ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

BİRİM RİSK KONTROL EYLEM PLANI

2026 YILI



- GÜVENLİ
- SÜRDÜRÜLEBİLİR
- ERİŞİLEBİLİR
- DİJİTAL ÜNİVERSİTE



PLANLA • DEĞERLENDİR • ÖNLEM AL • İZLE • GELİŞTİR

bidb.kastamonu.edu.tr



KASTAMONU ÜNİVERSİTESİ
Bilgi İşlem Daire Başkanlığı
GÜVENLİ | ERİŞİLEBİLİR | SÜRDÜRÜLEBİLİR | YENİLİKÇİ

2026
Birim Risk Eylem Planı
Yıllık Görev ve Süreç Takvimi
Eylül – Ekim – Kasım – Aralık



No	Başlık	Faaliyet / Görev	Eylül	Ekim	Kasım	Aralık
	İdari ve Süreç Yönetimi	1 İş yükü ve görev dağılımını 6 ayda bir, genel görev tanımlarını yılda en az bir kez gözden geçirmek.				Genel İş Yükü / Görev Tanımları Gözden Geçirme Toplantısı
		2 Mevzuat değişikliklerinde birim içi değerlendirme toplantıları düzenlemek.		● Birim İçi Mevzuat Değişikliği Bilgilendirme Toplantısı		
		3 İç kontrol sistemi için izleme/denetim planı oluşturmak ve eksiklikleri takip etmek.	● Planlama Toplantısı	● Takip Toplantısı	● Takip Toplantısı	● Değerlendirme Toplantısı
		4 Kişisel veri işleme süreçlerini inceleyerek gereksiz erişim yetkilerini kaldırmak ve veri ihlali müdahale prosedürlerini güncelleyip test etmek.		● KVKK Prosedürlerini İnceleme Toplantısı		
	Bilgi Güvenliği ve Personel Farkındalığı	5 Yazılımları OWASP Top 10 standartlarına göre kontrol etmek; periyodik zafiyet taramaları ve penetrasyon testleri gerçekleştirmek.	● Zafiyet Taraması / Sızma Testi	● Zafiyetlerin Önlenmesini Belirleme Toplantısı		
		6 Personele yönelik ortalama (phishing) simülasyonları yapmak, şüpheli işlem bildirim mekanizmaları kurmak ve sosyal mühendislik ile KVKK eğitimleri düzenlemek.			● Siber Güvenlik Farkındalık Eğitimi	
		7 Çok faktörlü kimlik doğrulamayı (MFA) yaygınlaştırmak ve hesapları güvenlik açısından düzenli izlemek.			● Siber Güvenlik Farkındalık Eğitimi	
	Altyapı, Sistem Odası ve İş Sürekliliği	8 DDoS koruma ve trafik filtreleme mekanizmalarını güçlendirmek; load balancing kurmak ve stres testleri yapmak.				DDoS Koruma ve Trafik Filtreleme Süreçlerini Değerlendirme Toplantısı
		9 ÜBYS ve kritik sunucular için iş sürekliliği/felaket kurtarma planları hazırlamak; yedekleri farklı ortamda tutmak ve geri dönüş testleri yapmak.		● Felaket Kurtarma Planları Hazırlama Toplantısı		
		10 Sunucu disklerinin sağlık/performans durumlarını izlemek, kapasite planlaması yapmak ve disk yedekliliğini artırmak.			● Sunucu Sağlık / Performans Durumlarını İzleme Toplantısı	
		11 Sistem odası klima ve UPS yedekliliğini artırmak; sıcaklık, nem, enerji ve yangın için alarm mekanizmalarını güçlendirip test etmek.				● Sistem Odası İnceleme
	Kamera Sistemleri ve Entegrasyonlar	12 Kamera sistemlerinin periyodik bakımlarını yapmak, arızalar için merkezi bildirim mekanizması kurmak ve kritik noktalardaki kameralara alternatif enerji sağlamak.		● Bakım Planları Hazırlama Toplantısı		
		13 Kritik entegrasyonlar için sürekli izleme/otomatik alarm mekanizmaları kurmak ve hata kayıtlarını düzenli analiz etmek.			● Entegrasyon Süreçlerini İzleme Toplantısı	
		14 Dış sistemlerde yaşanabilecek kesintilere karşı alternatif işlem ve veri aktarım yöntemleri belirleyerek periyodik testler yapmak.		● Periyodik Test		



Planlama Toplantısı / Çalışma



Toplantı / Çalışma



Eğitim / İzleme



Değerlendirme / Test



4 Ay
(Eylül – Aralık)



14
Toplam Faaliyet

Ek-2: Birim Risk Belirleme ve Eylem Planı Formu																																			
BİRİM																																			
Bilgi İşlem Daire Başkanlığı																																			
ADİ:																																			
Dönem:					2026 Yılı																														
Risklerin Belirlenmesi					İdare Risk Eylem Planına Teklif					Risklerin Değerlendirilmesi										Riske Yönelik Alınacak Kararların Belirlenmesi				İlave Risk Yönetim Faaliyetlerin Takip Edilmesi			Risklerin İzlenmesi								
S. No.	Risk Kodu	Tespit Edilen Riskler	Risk Türü	Risk Güncellik Durumu	İdare Risk Eylem Planına Teklif Edilecek Mİ?	Stratejik Amaç No.	Stratejik Amaç Tanımı	Stratejik Hedef No.	Stratejik Hedef Tanımı	Etki	Olasılık	Doğal Risk Puanı	Doğal Risk Seviyesi	Mevcut Risk Yönetimi Faaliyetleri	Mevcut Risk Yönetimi Faaliyetlerinin Yeterlilik Katmanları	Mevcut Risk Yönetimi Faaliyetleri Riskin Etkisini Mİ Gölgeletiyor Mİ Değiştiriyor?	Artık Risk Puanı	Artık Risk Seviyesi (Sonuç)	Riske Yönelik Alınacak Karar	İlave Risk Yönetim Faaliyeti	Faaliyet Sorumluları	Faaliyet Başlangıç Tarihi	Faaliyet Tamamlanma Tarihi	Faaliyet Durumu	Açıklama / Reviz	Reviz Faaliyet Tarihi	Doğal Risk Seviyesi Değişti mi?	Mevcut Risk Yönetimi Faaliyetleri Değişti mi?	Artık Risk Seviyesi Değişti mi?	Değişim Nedenleri	Yeni Doğal Risk Seviyesi	Yeni Artık Seviyesi	Değişim Risk Seviyelerine İlişkin Reviz Faaliyet Tamamlanması Gerekli mi?		
1	BİDB-RSK-01	Görev, yetki ve sorumlulukların güncel olmasını nedeniyle görev karmaşası, işlemler gecikmesi veya hesap verilebilirlik zayıflığı olmasını riski.	Operasyonel	Güncel						5	3	15	Yüksek	Görev tanımları yeni görev, görev dağılımı personelle yapılarak belirlenmektedir, görev dağılımı çizelgeleri güncel tutulmakta ve görev dağılımı birim amiri tarafından takip edilmektedir.	Kısmen Yeterli	0,4	Olasılık	6	Orta	Riski Azaltmak	Görev tanımları, yeni görev, görev dağılımı veya mevzuatın icrası halinde gerçekleştirilen güncelleme personelle yapılarak belirlenmektedir, görev dağılımı ve iş yükü ayrı ayrı belirlenir, görev tanımlarının güncel güncelliği ise yılda en az bir kez belirlenmektedir.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
2	BİDB-RSK-02	Kritik görevlerin sınırlı sayıda personel tarafından yapılması nedeniyle izin, rapor, görev değişikliği veya personel ayrılığı durumunda işlemler aksaması riski.	Operasyonel	Güncel						5	2	10	Orta	Kritik görevler için vakti personel belirlenmiş olup personelin izin,rapor, görev değişikliği veya ayrılığı durumunda işlemler vakti personelle yürütülmeye sağlanmaktadır.	Kısmen Yeterli	0,4	Etki ve Olasılık	4	Düşük	Riski Kabul Etmemek					Seçiniz			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
3	BİDB-RSK-03	Birimlerin kendi görev, yetki ve sorumluluk alanına giren iş ve işlemleri yerine getirmeye yetkinliklerini yeterince sağlamaması nedeniyle, Bilgi İşlem Daire Başkanlığının teknik destek, altyapı sağlama, rehberlik ve koordinasyon görevinin yerine getirilmesinde birim sorumluluğu olarak algılanması ve süreçlerde görev/sorumluluk karmaşası olmasını riski.	Operasyonel	Güncel						4	3	12	Yüksek	İç kontrol, risk yönetimi, stratejik planlama, performans programı, faaliyet raporları vb. süreçlerde birimlerin görev ve sorumlulukları, beşeriyat, duyurular, rehber dokümanlar, formlar, yazılımlar ve diğer araçlarla ilgili birimlere bildirilmektedir.	Kısmen Yeterli	0,4	Etki ve Olasılık	5	Düşük	Riski Kabul Etmemek					Seçiniz			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
4	BİDB-RSK-04	Mevzuat değişikliklerinin zamanında takip edilememesi veya uygulanması yeterince yapılmasında nedeniyle iş ve işlemlerin hata, eksik veya gecikmeli yürütülmesi; uygulamaların birliğin bütünlüğüne ve mevzuata aykırılık olmasını riski.	Operasyonel	Güncel						5	3	15	Yüksek	1-Mevzuat değişiklikleri Resmi Gazete, ilgili kamu kurumlarının duyuruları, iş yolları ve kurumsal bilgilerden kanunlar aracılığıyla takip edilmektedir; görev alanına giren değişiklikler ilgili birimlere, personelle duyurulmakta ve iş süreçlerine yansıtılmaktadır. 2-İlgili personelle mevzuat değişiklikleri ile Resmi Gazete'nin durumu olarak takip edilmesi hususunda bilgilendirme yapılmakta ve görev alanına giren düzenlemelerin zamanında izlenmesi konusunda gerekli uyarılarla bilgilendirilmektedir.	Kısmen Yeterli	0,4	Etki ve Olasılık	6	Orta	Riski Azaltmak	Bilgi İşlem Daire Başkanlığı görev alanına giren mevzuatlarla ilgili değişikliklerde birim içi değerlendirme toplantıları yapılmaktadır.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
5	BİDB-RSK-05	Yazılımlarda güvenli kodlama standartlarına (OWASP Top 10) uyum sağlanmaması ve API'ler üzerinden veri sunumlarının meydana gelmesi nedeniyle bilgi güvenliği ihlallerinin, yetkisiz erişimlerin ve veri kayıplarının olmasını riski.	Operasyonel	Güncel						4	3	12	Yüksek	DevSecOps süreçlerine geçilmesi. Canlıya alın öncesi otomatik kaynak kod analizi (SAST/DAST) yapılması.	Kısmen Yeterli	0,4	Etki ve Olasılık	5	Düşük	Riski Azaltmak	Yazılımlarda OWASP Top 10 güvenli standartlarına uyum sağlanmasını düzenli olarak kontrol edilmesi, güvenli yazılımların testine yönelik periyodik yazılım testleri ve penetrasyon testlerinin gerçekleştirilmesi, API güvenli kodlama standartlarına uyum sağlanması, güvenli yazılımların geliştirilmesi, API güvenli kodlama standartlarına uyum sağlanması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
6	BİDB-RSK-06	İç kontrol sisteminin ve süreçlerinin düzenli olarak izlenmesi ve denetlenmesi nedeniyle kontrol faaliyetlerinin etkinliğini düşürülmesi, mevcut risklerin zamanında tespiti edilememesi ve gerekli iyileştirmelerin gerçekleştirilememesi riski.	Operasyonel	Güncel						3	3	9	Orta	İç kontrol süreçlerinin ilgili birimler tarafından takip edilmesi, risk ve kontrol faaliyetlerinin belirli dönemlerde gözden geçirilmesi, gerçekleştirilen faaliyetlerin kayıtlı olarak alınması ve gerekli güncellemelerin düzenli ve yetersizliği faaliyetlerin planlanması.	Kısmen Yeterli	0,4	Olasılık	4	Düşük	Riski Azaltmak	İç kontrol sisteminin etkinliğini değerlendirilmesine yönelik periyodik izleme ve denetim planının oluşturulması, belirlenen kontrol faaliyetlerinin gerçekleştirilmesini düzenli olarak takip edilmesi, tespit edilen eksiklikler için sorumlu personel ve birimlerin belirlenmesi, sonuçların raporlanması ve gerekli düzeltici faaliyetlerin takip edilerek sonuçlandırılması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
7	BİDB-RSK-07	Son kullanıcıların olumsuz (phishing), sosyal mühendislik ve benzeri yöntemlerle gerçekleştirilen sahte e-posta ve mesajlara karşı yeterli farkındalığa sahip olmaması nedeniyle kurumsal bilgi ve verilerin ele geçirilmesi, yetkisiz erişim sağlanması ve bilgi güvenliği ihlallerinin meydana gelmesi riski.	Operasyonel	Güncel						4	4	16	Yüksek	Kurumsal e-posta hesaplarında spam ve olumsuz (phishing) içerikli mesajların filtrelenmesine yönelik güvenlik kontrollerinin uygulanması, kullanıcı hesaplarının güvenli kullanılması ve erişim kontrollerinin yapılması, personelle bilgi güvenliği ve güvenli e-posta kullanımı konusunda bilgilendirme yapılması, şüpheli e-posta ve mesajların Bilgi İşlem Daire Başkanlığına bildirilmesini sağlanması ve kullanıcı hesaplarının güvenli kullanımı için uyarılar yapılması.	Kısmen Yeterli	0,4	Etki ve Olasılık	6	Orta	Riski Azaltmak	Personelin olumsuz ve sosyal mühendislik saldırılarına karşı farkındalığının artırılması amacıyla düzenli bilgilendirme ve eğitimlerin gerçekleştirilmesi, periyodik olarak kullanıcıların eğitimleri yapılması, şüpheli e-posta ve mesajların bildirilmesine yönelik mekanizmaların oluşturulması, çok faktörlü kimlik doğrulama (MFA) kullanımıyla doğrulanması ve tespit edilen kullanıcı hesaplarının güvenli kullanımı için uyarılar yapılması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
8	BİDB-RSK-08	Kayıt, tercih, sunar ve benzeri yazılım sistemlerinde web servislerine yönelik sızma, trafik ve DDoS saldırıları nedeniyle sistem kaynaklarının yetersiz kalması, hizmetlerin sağlanmaması veya tamamen erişilemez hale gelmesi, buna bağlı olarak kullanıcıların işlemlerinin aksaması, hizmet sürekliliğinin olumsuz etkilenmesi ve iş ve işlemlerin zamanında gerçekleştirilememesi riski.	Operasyonel	Güncel						5	3	15	Yüksek	Web servisleri ve sistem kaynaklarının performansı ve erişilebilirlik açısından izlenmesi, sunucu ve ağ altyapısının düzenli olarak kontrol edilmesi, yoğun işlem dönemlerinde sistem kaynaklarının takip edilmesi, güvenlik duvarı ve ağ güvenlik cihazları üzerinden trafik kontrollerinin yapılması ve meydana gelen erişim ve performans sorunlarına yönelik teknik müdahalelerin gerçekleştirilmesi.	Kısmen Yeterli	0,4	Etki ve Olasılık	6	Orta	Riski Azaltmak	oğun trafik ve DDoS saldırılarına karşı web servisleri için DDoS koruma ve trafik filtreleme mekanizmalarının güçlendirilmesi, kritik servislerde sızma, denetim ve izlenilmesini altyapısının uygulanması, yoğun dönemlerde öncelikli yük ve stres testlerinin gerçekleştirilmesi, kritik sistemler için kapasite planlaması yapılması, acil durumlarda gerekli zamanlı izlenerek erişim tespiti edilmesi ve hizmet sürekliliğini sağlayacak alternatif erişim ve kurulum senaryolarının oluşturulması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
9	BİDB-RSK-09	ÜBYS sisteminin sunucu donanım veya yazılım sorunları, elektrik kesintileri, ağ altyapısı problemleri ve diğer saldırılar nedeniyle devre dışı kalması veya hizmet verememesi sonucunda akademik ve idari iş ve işlemlerin aksaması, veri erişiminin kesintisi olgusuna ve hizmet sürekliliğinin olumsuz etkilenmesi riski.	Operasyonel	Güncel						4	3	12	Yüksek	ÜBYS sunucu ve sistem altyapısının düzenli olarak izlenmesi ve bakımının yapılması, sunucu ve ağ cihazlarının çalışma durumlarının takip edilmesi, yedekleme faaliyetlerinin gerçekleştirilmesi, elektrik kesintilerine karşı kesintisiz güç kaynağı ve jeneratör altyapısının kullanılması, güvenlik duvarı ve güvenlik sistemleri ile diğer tehditlerin izlenmesi ve meydana gelen sistem kesintilerine yönelik teknik müdahalelerin gerçekleştirilmesi.	Kısmen Yeterli	0,4	Etki ve Olasılık	5	Düşük	Riski Azaltmak	ÜBYS için iş sürekliliği ve felaket kurtarma planlarının geliştirilmesi, kritik sunucu ve sistemlerin yedekli ve yüksek erişilebilirlik sağlayacak şekilde yapılandırılması, yedeklerin fakat bir ortamda düzenli olarak tutulması ve geri dönüş testlerinin gerçekleştirilmesi, diğer saldırılara karşı güvenlik kontrollerinin ve izleme mekanizmalarının geliştirilmesi, enerji ve ağ altyapısında oluşabilecek kesintilere karşı alternatif altyapıların oluşturulması ve periyodik olarak sistem kurtarma tatbikatlarının yapılması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
10	BİDB-RSK-10	Mevcut sunucu sistemlerinde kullanılan disklerin elektrik kesintileri, donanım arızaları veya kullanım hatalarından kaynaklı olarak arızalanması sonucunda veri kaybı, sistemlerin hizmet dışı kalması, bilgi ve belgelerin erişiminin kesintisi olgusuna ve iş sürekliliğinin olumsuz etkilenmesi riski.	Operasyonel	Güncel						5	4	20	Çok Yüksek	Sunucu disklerinin ve depolama sistemlerinin düzenli olarak izlenmesi, donanım arızalarının takip edilmesi, kritik verilerin düzenli olarak yedeklenmesi, elektrik kesintilerine karşı kesintisiz güç kaynağı ve jeneratör sistemlerinin kullanılması ve arızaların disklerin gerekli durumlarda değiştirilerek sistemlerin çalışır durumda tutulması.	Kısmen Yeterli	0,4	Etki ve Olasılık	8	Orta	Riski Azaltmak	Sunucu disklerinin sağlık ve performans durumlarının düzenli olarak izlenmesi, kullanımı ömrünün tamamlanma diskleri için planlı yenileme ve kapasite planlaması yapılması, kritik sistemlerde disk yedekliliğinin artırılması, yedekleme ve geri yükleme süreçlerinin periyodik olarak test edilmesi ve elektrik kesintilerine karşı enerji altyapısının güçlendirilmesi.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
11	BİDB-RSK-11	Güvenlik kameralarının elektrik kesintileri, donanım arızaları veya bağlantı problemleri nedeniyle çalışmaması ve görüntü kaydı yapamaması sonucunda güvenlik olaylarının izlenememesi, olaylara ilişkin görüntü kayıtlarının oluşturulmaması ve kurulum fiziksel güvenliğin olumsuz etkilenmesi riski.	Operasyonel	Güncel							4	3	12	Yüksek	Güvenlik kameralarının ve kayıt sistemlerinin düzenli olarak kontrol edilmesi, kamera görüntülerinin ve kayıt durumlarının takip edilmesi, meydana gelen kamera arızalarına teknik müdahalelerin yapılması, elektrik kesintilerine karşı kesintisiz güç kaynağı ve jeneratör sistemlerinin kullanılması ve arızalı kamera ve ekipmanların gerekli durumlarda onarılması veya değiştirilmesi.	Kısmen Yeterli	0,4	Etki ve Olasılık	5	Düşük	Riski Azaltmak	Kamera sistemlerinin periyodik bakım ve kontrollerinin planlı şekilde gerçekleştirilmesi, kamera ve kayıt cihazlarının arıza durumlarının mekânleri olarak izlenmesi ve bildirim mekanizmalarının oluşturulması, kritik kamera noktalarında yedekleme ve alternatif enerji kaynaklarının sağlanması, kayıtların düzenli olarak kontrol edilmesi ve sistemin kesintisiz çalışmasını yönelik kapasite ve yenileme planlarının oluşturulması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz
12	BİDB-RSK-12	Sistem odasında bulunan klima, UPS ve benzeri altyapı ekipmanlarının arızalanması veya yangın gibi fiziksel risklerin meydana gelmesi nedeniyle sunucu, ağ ve depolama donanımlarının zarar görmesi, sistemlerin hizmet dışı kalması, veri kaybı ve bilgi işlemlerinde kesinti yaşanması riski.	Operasyonel	Güncel						4	3	12	Yüksek	Sistem odasının sıcaklık, nem ve enerji durumunun takip edilmesi, klima ve UPS sistemlerinin düzenli olarak kontrol ve bakımının yapılması, yangın algılama ve söndürme sistemlerinin belirlenmesi, sistem odasına yerleştirilen erişimin sınırlandırılması ve kritik donanımların düzenli olarak kontrol edilmesi.	Kısmen Yeterli	0,4	Etki ve Olasılık	5	Düşük	Riski Azaltmak	Sistem odası altyapısına yönelik periyodik bakım ve test planlarının oluşturulması, klima ve UPS sistemlerinde yedekliliğinin artırılması, sıcaklık, nem, enerji ve yangın durumlarının anlık izlenmesine yönelik alarm ve bildirim mekanizmalarının güçlendirilmesi, yangın söndürme sistemlerinin periyodik olarak test edilmesi ve olağan donanım kayıplarına karşı iş sürekliliği ve felaket kurtarma planlarının güncellenmesi.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz	
13	BİDB-RSK-13	YÖKSİS, ÖSYM, e-Devlet ve banka gibi dış sistemlerle gerçekleştirilen entegrasyonların teknik arızalar, bağlantı sorunları veya karşı sistemlerdeki yangın kesintileri nedeniyle çalışmaması sonucunda veri altyapısının gerçekleştirilememesi, iş ve işlemlerin aksaması, veri bütünlüğünün bozulması ve hizmetlerin zamanında sunulmaması riski.	Operasyonel	Güncel							4	3	12	Yüksek	Kritik entegrasyonların çalışma durumlarının ve veri altyapılarının takip edilmesi, entegrasyon servislerinin hata ve erişim durumlarının izlenmesi, oluşan bağlantı ve veri akışları sorunlarına yönelik teknik kontrollerin gerçekleştirilmesi, ilgili kurumlara iletişim sağlanarak kesintilerin takip edilmesi ve gerekli durumlarda işlemlerin alternatif yöntemlerle yürütülmesi.	Kısmen Yeterli	0,4	Etki ve Olasılık	5	Düşük	Riski Azaltmak	Kritik entegrasyonlar için sürekli izleme ve otomatik alarm mekanizmalarının oluşturulması, entegrasyon servislerinin hata kayıtlarının düzenli olarak analiz edilmesi, dış sistemlerde yaşanabilecek kesintilere karşı alternatif işlem ve veri akışları yöntemlerinin belirlenmesi, entegrasyonların periyodik olarak test edilmesi ve hizmet sürekliliğini sağlayacak yedekleme ve felaket kurtarma senaryolarının oluşturulması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz
14	BİDB-RSK-14	Kişisel verilerin yetkisiz kişilerle paylaşılması, hukuka aykırı şekilde izlenmesi veya gerekli güvenlik tedbirlerinin alınmaması nedeniyle kişisel veri ihlallerinin meydana gelmesi, KVKK kapsamında idari yaptırım ve idari para cezası uygulanması, kurumun itibarının ve güvenliğinin olumsuz etkilenmesi riski.	Operasyonel	Güncel							4	4	16	Yüksek	Kişisel verilerin erişiminde yetki ve görev tanımları doğrultusunda sınırlandırılması, kullanıcı erişimlerinin kontrol edilmesi, kişisel verilerin güvenliğin sağlanmasına yönelik teknik ve idari tedbirlerin uygulanması, veri izleme ve paylaşım süreçlerinin ilgili mevzuat kapsamında yürütülmesi, bilgi güvenliği ve KVKK konusunda personelle yönelik bilgilendirme ve farkındalık faaliyetlerinin gerçekleştirilmesi.	Kısmen Yeterli	0,4	Etki ve Olasılık	6	Orta	Riski Azaltmak	Kişisel veri izleme ve paylaşım süreçlerinin periyodik olarak gözden geçirilmesi, erişim yetkilerinin düzenli olarak kontrol edilerek gereksiz yetkilerin kaldırılması, kişisel veri ihlallerinin tespiti ve bildirilmesine yönelik prosedürlerin güncel tutulması, veri ihlali durumlarında yapılacak müdahale ve bildirim süreçlerinin düzenli olarak test edilmesi ve personelle yönelik KVKK farkındalık eğitimlerinin periyodik olarak yapılması.	BİDB	1.01.2026	31.12.2026	İlave Risk Yönetimi Faaliyeti Planlandı			Seçiniz	Seçiniz	Seçiniz				Seçiniz