Birim Adı: BİLGİ İŞLEM DAİRE BAŞKANLIĞI

Sıra No	Hassas Görevler	Riskler	Risk Düzeyi (Yüksek-Orta-Düşük)	Gerekli Kontroller/Tedbirler
1	**Bilişim Altyapı Hizmetlerinin Sağlanması** 1-Şebeke Elektriği 2-UPS 3-İklimlendirme Sistemi 4-Ortam İzleme Sistemi 5-Yangın Söndürme Sistemi	1-Aktif cihazlarda kalıcı hasar oluşma riski. 2-Hizmetlerde erişilebilirliğin sekteye uğraması riski. 3-Veri kayıplarının oluşması riski. 4-Sistem odasına enerji sağlayan hatlarda olası enerji kesintisi veya fazlalığı riski. 5-Aktif cihazların üretimine ya da desteğine son verilmiş olması riski.	Yüksek	1-Aktif cihazların düzenli olarak takip edilip izlenmesi, bakım ve onarımlarının yapılması, gerekli ortamın sağlanması. 2-Sistem odasının enerji alt yapısının etkin ve sağlıklı bir şekilde çalışmasının sağlanması amacıyla Yapı İşleri ve Teknik Daire Başkanlığı ile iş birliği içerisinde olunması. 3- Mevcut personele cihazları manuel olarak aktif/pasif hale getirebilecek yetkinliğin kazandırılması için gerekli olan eğitimlerin verilmesi. 4-Olası veri kayıplarının önüne geçmek amacıyla başka bir lokasyonda bilişim altyapı yedekliğinin sağlanması. 5-Mevcut cihazlarla ilgili bilgi ve eğitim verilmesi dahil her türlü tedbirin alınması. 6-İş sağlığı ve güvenlik tedbirlerinin değişen şartlara göre uygun hale getirilmesi.
2	**Kurum İnternet Erişiminin Sağlanması** 1-Kurumun internete erişiminin uygun olan en güvenli ve hızlı şekilde sağlanması	1-İnternet hizmeti kesintisi riski. 2-Sunulan hizmetlerin erişilebilirliğinin sekteye uğraması riski. 3-Kurumsal imajın zarar görme riski.	Yüksek	1-Kesintisiz internet hizmeti için ağ güvenliği ve yapılandırmalarının sağlanması. 2-Yedekli yapının oluşturulması. 3-Kurumun internet hizmeti ile ilgili bir izleme sisteminin kurulması.

3	**Kablolu Ağ Hizmetinin Sağlanması** 1-Ağ altyapısının yönetilmesi 2-Yeni lokasyon ve ayarlamaların planlanması ve yönetilmesi 3-Kesintisiz hizmet sağlanması 4-Ağ güvenlik önlemlerinin alınması	1- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 2- Hizmetlerin erişilebilirliğin sekteye uğraması riski.	Düşük	1- Ağın izlenebilir olmasının sağlanması. 2- Olası arızlara karşı yedek konfigürasyonlar ve yedek cihazların hazır bulundurulması. 3- Mümkün olduğu ölçüde fiziksel olarak yedekli bir yapının kurulması. 4- Cihazlara erişim yöntemleri/yetkileri incelenmeli ve yetkisiz erişimlere karşı önlemlerin alınması. 5- Profillere/lokasyonlara/cihazlara göre farklı sanal ağların oluşturulması ve birbirleri arasında erişimlerin kontrollü şekilde sağlanması. 6-Yeterli güvenlik tedbirlerinin alınması ve yapılacak testler ile periyodik olarak kontrol edilmesi. 7-Ağ aktif cihazları ve kablo yenileme prosedürünün hazırlanması ve uygulamaya konulması.
4	**Kablosuz Ağ Hizmetinin Sağlanması** 1- Farklı profildeki kullanıcılara çözümler sunulması. 2- Güvenlik ve kullanılabilirlik ölçülerine göre en efektif çözümlerin sunulması.	1- Kurumda kablosuz internet hizmetlerinin verilememesi riski. 2- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Düşük	1- Ağın izlenebilir olmasının sağlanması. 2- Olası arızlara karşı yedek konfigürasyonlar ve yedek cihazların hazır bulundurulması. 3- Mümkün olduğu ölçüde fiziksel olarak yedekli bir yapının kurulması. 4- Cihazlara erişim yöntemleri/yetkileri incelenmeli ve yetkisiz erişimlere karşı önlemlerin alınması. 5- Profillere/lokasyonlara/cihazlara göre farklı sanal ağların oluşturulması ve birbirleri arasında erişimlerin kontrollü şekilde sağlanması. 6-Yeterli güvenlik tedbirlerinin alınması ve yapılacak testler ile periyodik olarak kontrol edilmesi.

				7- Farklı gruplar için farklı yayınlar oluşturulması ve farklı kimlik doğrulama yöntemleriyle erişimlerin sağlanması. 8- Kimlik doğrulaması olmayan hiçbir yayın sunulmaması. 9- Ağ Aktif cihazları ve kablo yenileme prosedürünün hazırlanması ve uygulamaya konulması.
5	**Sunucu Kaynaklarının Yönetilmesi** 1- Sunucularının yapılandırılması. 2- Sunucuların sağlıklı işlemesinin sağlanması. 3- Sanallaştırma altyapısı.	1- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 2- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Yüksek	1- Sunucu ve üzerinde kurulu olan uygulamalardaki driver, firmware, versiyon, lisans vb. güncellemelerin düzenli aralıklarda yapılması. 2- Sunucuların yedekli bir yapıda konumlandırılmasının sağlanması. 3- Sunucuların izlenebilir olmasının sağlanması. 4- Sanallaştırma altyapısı, storage, sunucular ile çevresel birimler ve sistemlerinin bakımının düzenli olarak yapılmasının sağlanması. 5- Kaynaklara erişimlerin kontrol edilmesi ve güvenlik tedbirlerinin alınması. 6- Fiziki ve sanal ortamlar için alarm üretilmesi ve en hızlı şekilde aksiyon alınabilmesi için süreçlerin belirlenmesi. 7- Sunucu ve lisansların yenileme prosedürünün hazırlanması ve uygulamaya konulması.
6	**Veri Depolama Kaynaklarının Yönetilmesi** 1- Donanımların yüksek erişilebilirlikte çalışmasının sağlanması. 2- Sanallaştırma ve yedekleme yazılımlarının yönetilmesi.	1- Hizmetlerin erişilebilirliğinin sekteye uğraması riski. 2- Kurumda barındırılan dijital verilerin zarar görmesi riski.	Yüksek	1- Cihaz yedekliğinin sağlanması. 2- Cihazlardaki olası arızalara karşı donanım yedekliğinin (disk, controller vb.) sağlanması.

	3- Sistemlerin sorunsuz ve güvenli şeklide çalışmasının sağlanması.	3-Depolama alanlarının zamanla yetersiz kalması riski. 4-Kurum genelinde veri kaybı yaşanması riski.		3- Cihazların güncelliklerinin kontrol edilmesi ve kontrollü şekilde güncellenmelerinin yapılmasının sağlanması. 4- Cihaz, lisans ve depolama alanı kapasitesi yenileme prosedürünün hazırlanması ve uygulamaya konulması.
7	**Yedekleme Süreçlerinin Yönetilmesi** 1-Sanal ortam yedekleri. 2-Fiziksel ortam yedekleri.	1- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 2- Kurum genelinde veri kaybı yaşanması riski.	Düşük	1- Yedekleme yazılımlarının güncelliğinin sağlanması. 2- Yedek alınan cihazlarının güvenilir ve kesintisiz erişiminin sağlanması. 3- Kritiklik seviyelerine göre yedekleme planlarının oluşturulması. 4- Yedekten geri dönüş testleri ile yedeklerin doğruluklarının test edilmesi. 5-Farklı lokasyonlarda ve formatlarda yedeklerinin tutulmasına yönelik önlemlerin alınması.
8	**Felaketten Kurtarma Süreçlerinin Yönetilmesi** 1- Fayda maliyet analizleri yapılarak afet durumu için planlamaların yapılması.	1- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 2- Kurum genelinde veri kaybı yaşanması riski.	Düşük	1- Sistem odasındaki cihazların güncelliğinin ve kesintisizliğinin sağlanması. 2- FKM senaryolarının oluşturulması.
9	**E-Posta Hizmetinin Sağlanması** 1- Personel ve öğrenci kurumsal e-posta hesaplarının tanımlanması. 2- Kullanıcı sorunlarının çözülmesi.	1- Kişilerin verilerinin kaybolması riski. 2- Spam, virüs gibi zararlı yazılımların bulaşması sonucu sistemde ciddi sorunlara sebebiyet verme riski.	Orta	1- Kurumsal e-posta kullanım politikasında sıkılaştırmaya gidilmesi. 2- Farkındalık bilgilendirmelerin kurum genelinde yapılması. 3-Kara listelerin güncel takibi ve listeden çıkma prosedürlerinin işlenmesi.

		3- Kurumsal e-posta domainimizin uluslararası kara listelere düşmesi riski.		
10	**Siber Güvenlik Tedbirlerin Sağlanması** 1- Sistem ve network güvenliğinin düzenlenmesi. 2- Kullanıcı erişiminin denetlenmesi ve yetkilendirilmesi. 3- Yeni teknolojileri takip etmek ve uygulanabilirliği olan ürün/sistemler için satın alma aşamasına geçmek.	1-Siber saldırılara maruz kalma riski. 2- Üniversite faaliyetlerinin aksamasına sebebiyet verme riski. 3- Bilişim kaynaklarının yetkisiz kişilerce kullanılması, suç unsurunda kişinin tespit edilememesi riski. 4- Kurumsal imajın zarar görme riski. 5-Kurum genelinde veri kaybı yaşanması riski.	Yüksek	1- Ağ ve sistem güvenlik önlemlerinin alınması. 2- Güvenlik cihazlarının kuruma özel ayarlarının yapılması ve takiplerinin sağlanması. 3- Mümkün olduğu ölçüde sürekli denetimlerle zafiyet ve tehditlerin tespit edilmesi ve giderilmesi. 4- Yeterli seviyede yetkilendirmeler ile kişilerin sadece ilgili oldukları alanlara erişimlerinin sağlanması. 5-Görev ayrılığı ilkesinin uygulanması 6- SOME ekibinin yetkinliklerinin artırılması.
11	**Bilişim Altyapılarında Son Kullanıcı Güvenliğinin Sağlanması** 1- Antivirüs programının sağlanması. 2- Son kullanıcı aktivitelerinin sınırlanması.	1- Kişisel veri kayıplarının yaşanması riski. 2- Zararlı yazılımların kurum ağına yayılabilmesi riski. 3- Kurumsal veri kayıplarının yaşanması riski.	Yüksek	1- Lisanslı program kullanılması ve düzenli aralıklarla güncellenmesi. 2- Yazılımın otomatik olarak tarama modunda çalıştırılması. 3- Otomatik olarak tüm cihazlara kurulması ve kullanıcı tarafından kaldırılmasının iptal edilmesi. 4-Kurumsal antivirüs yazılımının kullandırılması.
12	**Bilgisayar Bakım ve Onarım Hizmetinin Sağlanması**	1- Lisanssız program kullanma sonucunda kurumun yaptırımlara maruz kalması riski.	Düşük	1- Bilgisayar envanteri çıkartacak ortamların oluşturulması ve kurum bilgisayarlarının yazılım ve donanım takibinin yapılması.

	1- Birimlerin kullandığı bilgisayarlara, Üniversitemizin lisanslı programlarını kurmak. 2- Birimlerden gelen bilgisayarların bakım ve onarımını yapmak. 3- Telefonda destek vermek. 4- Birimlere istendiğinde yerinde servis hizmeti vermek. 5- Ekonomik ömrünü tamamlamış olan veya tamamlamadığı halde teknik ve fiziki nedenlerle alınış amaçları doğrultusunda kullanılması imkânı kalmayan ya da tamiri mümkün veya ekonomik olmayan arızalar nedeniyle kullanılmasında yarar görülmeyecek bilgisayar ve bilişim malzemelerinin tespit edip, hurdaya ayrılması için görüş bildirmek. 6- Üniversitemize alınacak bilgisayar ve bilgisayar parçalarına teknik şartname hazırlamak	2- Arızaların zamanında giderilememesi durumunda iş akışının sekteye uğraması riski. 3-Kamu zararına sebebiyet verme riski. 4- Kurumda tamiri mümkün olan bilgisayarların hurdaya ayırılması riski. 5- Kuruma teknik özellikleri uygun olmayan bilgisayar alınması riski.		2- Müdahale edilebilecek arızalara en hızlı şekilde iç kaynak ile müdahale edilmesi. 3- Müdahale edilemeyecek arızalarla ilgili dış kaynaklı hizmet yönlendirmesi yapılması ve alınacak aksiyonla ilgili görüş bildirilmesi. 4- Depo takibinin yapılarak ihtiyaç halinde parça temininde sorun yaşanmamasının sağlanması.
13	**IP Telefon/Telefon Hizmetinin Sağlanması** 1- Telefon ağı yapısal kablolama mantığına uygun bir biçimde üniversitemizin tüm birimlerinin telefon ve santral altyapısının planlanması. 2- Tüm birimlerin kurum içi ve kurum dışı sesli iletişim problemlerinin çözümüne destek verilmesi.	1- İletişim altyapısının sekteye uğraması veya durması riski.	Düşük	1- IP telefon hizmeti için gerekli alımların yapılması ve lisans takibinin yapılması. 2- Sistemlerin güncel tutulmasının ve yetkilerinin kontrol edilmesinin sağlanması. 3- Olası arızalarda hızlı bir şekilde iletişime geçilmesi ve sürecin takibinin yapılması. 4- Son kullanıcılara olası sorunlarda en hızlı şekilde destek verilmesi.

	3- Dâhili telefon numaralarının dağıtımı ve yönetilmesi. 4- Kurum için IP yönetiminin yapılması.			
14	**Ortak Klasör Hizmetinin Sağlanması** 1- Birimler için klasörlerin hazırlanması. 2- Erişim yetkilerinin hazırlanması ve kontrol edilmesi. 3- Yedek alınarak olası hatalara karşı veri kaybının önüne geçilmesi.	1- Personelin ortak işleri yürütememe riski. 2- Birimlerin iş süreçlerinin sekteye uğraması riski.	Düşük	1- Ortak Klasör paylaşımı için gerekli sunucuların hazırlanması. 2- Ortak Klasör paylaşımı için gerekli network ayarlarının yapılması. 3- Ortak Klasör paylaşımı için gerekli yetkilendirmelerin yapılması.
15	**İz Kayıtlarının (Loglama) Yönetilmesi** 1- Sistemlerin iz kayıtlarını toplamak, izlemek, yedeklemek. 2- İz kayıtlarından kritiklik derecelerine göre alarmlar üretmek.	1- Herhangi bir suç unsurunda kişinin belirlenememesi riski.	Düşük	1- Merkezi log sunucusunun kurulması ve lokal log kayıtlarının düzenlenmesi. 2- Log verilerinin 5651 sayılı Kanunla belirlenen kurallara göre tutulmasının sağlanması. 3- Kritik sistemlerin loglarının merkezi log sunucusuna aktarılması.
16	**Yazılım Geliştirme Hizmetinin Sağlanması** 1- Kurumun yazılım ihtiyaçlarını karşılamak ve mevcut yazılımların geliştirilmesi için mevcut bütçe, personel ve zamanın en verimli şekilde kullanılması.	1- İhtiyacın düzgün tespit edilememesi nedeniyle iş ihtiyaçlarının karşılanamaması riski. 2-Kamu zararına sebebiyet verme riski. 3-Yazılımın geliştirildiği teknolojinin güncelliğini yitirmesi riski. 4-Tek kişiye bağımlı olarak yazılım geliştirilmesi riski.	Orta	1-Kurumun yazılım ihtiyaçlarının en doğru şekilde tespit edilmesi. 2-Birimlerden gelen yazılım ihtiyaçlarının doğru analiz edilmesi. 3-Mevcut kaynaklar ile yapılabileceklerin tespiti ve mevcut kaynaklar ile ihtiyacın giderilmesi. 4-Mevcut kaynaklar ile ihtiyaç giderilemiyor ise piyasa araştırmasının yapılarak en verimli ürünün seçilmesi. 5-Takım çalışmasına imkan verecek versiyonlama gibi sistemlerin devreye alınması. 6-Projelerin dokümantasyonlarının detaylı ve güncel halde tutulması.

		5-Güvenli yazılım geliştirme tekniklerinin uygulanmaması riski.		7-Güvenli kod geliştirme teknikleri konusunda personel yetkinliklerinin artırılması. 8-İki faktör doğrulama gibi ekstra güvenlik tedbirlerinin mevcut yazılımlara entegrasyonu ile ilgili gerekli temin işleminin yapılması.
17	**Dış Kaynaklı Yazılım Temini ve Koordinasyonun Sağlanması** 1- İç kaynak ile karşılanamayan ihtiyaçların giderilmesi için dış kaynaklı yazılımların tercih edilmesi.	1- Hizmetlerin erişilebilirliğinin sekteye uğraması riski. 2- Dış kaynak paydaşın el değiştirmesi ve/veya faaliyetine son vermesi halinde alınan yazılım sağlama/bakım/destek hizmetinin sürdürülemez duruma gelmesi riski. 3- Birimlerin iş süreçlerinin sekteye uğraması riski. 4-Kişisel verilerin hukuka aykırı olarak işlenmesi ve erişilmesi riski.	Orta	1- Yazılımların ihtiyaçları karşılayıp karşılamadığının teknik olarak denetlenmesi. 2- Yazılımlarda var olan zafiyet ve eksikliklerin giderilmesi ve gerekli geliştirmelerin yapılması için firmalarla koordineli şekilde çalışılması. 4- Satın alma, yenileme ve yükseltme vb. süreçlerin takip edilmesi ve gerçekleştirilmesi. 5- 6698 sayılı ve 5651 sayılı Kanunlar ve ikincil mevzuatlar kapsamında gizliliği ve mahremiyeti sağlamak üzere ilgili taraflarla sözleşmelerin tesis edilmesi. 6-Dış kaynak temin yazılımlarda açık kaynak koda dönüşüm ve/veya alınan yazılımın hizmet sağlayıcının el değiştirmesi halinde aynen devamı, faaliyete son vermesi halinde kaynak kodlarının kuruma tesliminin sözleşme ile sağlanabilmesi.
18	**Web Servis Hizmetlerinin Yönetimi** 1- Sistemler arası entegrasyonun sağlanması. 2- İnsan hatasını en aza indirmek için otomatik süreçler tasarlanması.	1- Bilişim sistemlerinin entegre çalışmalarının sağlanamaması riski. 2- Hizmetlerin erişilebilirliğinin sekteye uğraması riski. 3-Kontrolsüz ve yetkisiz erişimlerin oluşması riski.	Düşük	1- Web servis entegrasyonlarının kontrollerinin yapılması. 2- Entegre edilecek sistemler için senaryonun oluşturulması ve uygulamasının testlerinin yapılması veya ilgili birimlere yaptırılması. 3- İlgili birimlerin bilgilendirmelerinin sağlanması.

				4- Daha entegre ve otonom sistemler için ihtiyaç duyulan servislerin ve entegrasyonların tespit edilip, gerçekleştirilmesinin sağlanması. 5-Servis hizmetlerinin merkezi bir yapıyla kontrolü ve loglanması.
19	**Web Sitesi Yönetimi** 1- Web sayfaların oluşturulması ve İYS yetkililerinin atanması. 2- Eğitimlerin verilmesi.	1- Gerekli bilgileri dış dünyayla paylaşılamaması riski. 2- Kurumsal imajın zarar görme riski. 3-Şifrelerin 3.şahısların eline geçmesi riski.	Orta	1- Gelen taleplere göre yetkilendirmelerin yapılması ve ilgili kişilere İYS eğitimlerinin verilmesi. 2- Web sitesinin 7/24 sürekliliğinin sağlanması. 3- İçerik girişlerinin güncel ve doğru olması. 4- Alınması gereken güvenlik önlemlerinin sunucu ve uygulama katmanında alınması. 5-Yönetim paneline girişlerine iki faktör doğrulama gibi ekstra güvenlik mekanizmalarının entegre edilmesi.
20	**Elektronik Belge Yönetim Sistemine Teknik Destek Sağlanması** 1- Karşılaşılan problemlere teknik destek sağlanması ve firma ile koordinasyonun sağlanması.	1-İhtiyacın düzgün tespit edilememesi nedeniyle iş ihtiyaçlarının karşılanamaması riski. 2-EBYS ile ilgili aksaklıklar yaşanması riski. 3- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Orta	1- Bilgi İşlem Daire Başkanlığı tarafından çözülebilecek teknik problemlerle ilgili hızlı ve pratik çözümlerin üretilmesi ve sunulması. 2- Gerektiği durumda firma ile hızlı şekilde iletişime geçerek problemin çözümlenmesinin sağlanması.
21	**Bilişim Alanında Teknik Şartname Desteğinin Sağlanması**	1- Alınacak mal ve hizmet işinin nitelik ve nicelik bakımından eksik ya da yetersiz yapılması riski.	Düşük	1- Yasal mevzuatlar çerçevesinde süreçlerin yürütülmesi. 2- Resmi yazışma kurallarına uygun ve hızlı bir şekilde yazıların oluşturulması. 3- Kurumun ihtiyaçlarının eksiksiz ve yanlış anlaşılmaya meydan vermeden belirlenmesi.

				4- Kurumun ihtiyaçlarına göre tüm piyasa araştırılarak en uygun teknolojiye göre şartların belirlenmesi.
22	**Başkanlığımız Yazı İşlerinin Yürütülmesi**	1- Hizmetlerin erişilebilirliğinin sekteye uğraması riski.	Düşük	1- Yasal mevzuatlar çerçevesinde süreçlerin yürütülmesi. 2- Resmi yazışma kurallarına uygun ve hızlı bir şekilde yazıların oluşturulması. 3-Evrakların dosyalanmasında Standart Dosya Planına uyulması.
23	**Başkanlığımız Taşınır Kayıt ve Kontrol İşlemlerinin Yürütülmesi**	1- Düzenli yapılmayan ve kontrol edilmeyen taşınır işlemlerinin, sistem ve depo kayıtlarında tutarsızlığa sebep olması riski. 2- Zimmet kayıtlarının düzgün şekilde yapılmaması nedeniyle malzemenin takip edilmesinin zorlaşması ve malzeme kayıplarının oluşması riski.	Düşük	1- Taşınır yıl sonu işlemlerinin zamanında yapılması. 2- Tüketim Malzemesi Çıkış Raporunun 3 aylık periyotlarla düzenlenmesi, Strateji Geliştirme Daire Başkanlığına teslim edilmesi. 3- Malzeme giriş-çıkış işlemlerinde gerekli evrakların süresi içinde düzenlenerek Strateji Geliştirme Daire Başkanlığına teslim edilmesi. 4- Kişi zimmet kayıtlarının zamanında yapılması ve ıslak imza alınarak dosyada muhafaza edilmesi.
24	**Birim Faaliyet Raporunun Hazırlanması**	1- Şeffaflık ve hesap verme sorumluluğunun yerine getirilememesi riski.	Düşük	1-Faaliyet raporunun performans programı baz alınarak hazırlanmasının sağlanması, bu konuda ilgili kişilere gerekli bilgilendirmelerin yapılması. 2-İlgili mevzuatında belirtilen tarihler dikkate alınarak çalışma takviminin belirlenmesi.
25	**Birim İç Kontrol Süreçlerinin Yürütülmesi**	1- Üniversitemizin amaç ve hedeflerine ulaşmasını engelleyecek muhtemel risklerin gözden kaçırılması.	Düşük	1-İç kontrolün sadece bir mali kontrol değil bir yönetim şekli olduğunun birime benimsetilmesine ve eylem planlarının bu temelde gerçekleştirilmesine özen gösterilmesi.

				2-Bilgi paylaşım toplantılarının yapılması. 3-Birim bazında faaliyetlerin takip edilerek geri bildirim yapılması.
26	**Satın Alma Süreçlerinin Yürütülmesi**	1- Zamanında alınmayan yazılım, lisans ve hizmetlerin, üniversite işleyişinde yavaşlamaya ve aksamaya neden olması riski. 2- Depoda ki malzemenin tükenmesi ve zamanında temin edilememesi sonucu Üniversitenin işlerinin yavaşlaması veya aksaması riski.	Orta	1- Satın alınan yazılım ve lisanslardan Bilgi İşlem Daire Başkanlığı sorumluluğunda olanlarının garanti sürelerinin takip edilerek ihtiyaç durumunda yenilemelerinin yapılması, sorumluluğunda olmayanlar için ilgili birimden gelen taleplere göre işlemlerin hızlı şekilde yerine getirilmesi. 2- Bilgi İşlem Daire Başkanlığı deposundaki mal ve malzemelerin takibi yapılarak olası ihtiyaçlara karşı hazırlıklı olunması ve gerektiği durumlarda yeni alımların yapılması. 3- Kurum bilişim ihtiyaçları tespit edilerek alımların yapılması ya da alım için gerekli taleplerin oluşturulması.
27	**Birim Bütçe Planlamasının Yapılması**	1- Üniversite bünyesinde ihtiyaç duyulan bilişim kaynaklarının karşılanamaması riski. 2-Kamu zararına sebebiyet verme riski.	Yüksek	1- Üniversite içinde kullanılan bilişim kaynaklarının bakım ve güncelleme ihtiyaçlarının belirlenmesi. 2- Üniversite için temin edilmesi gereken bilişim sistemlerinin belirlenmesi ve ön çalışmaların yapılması. 3- Kurum hedef ve amaçları doğrultusunda tüm ihtiyaçların belirlenerek yıllık bütçe planlamasının yapılması.