EK-2 ISO 27001 Belgelendirme Başvuruları İçin

Kuruluş Adı:					
Adres(ler): **(Kalıcı Lokasyon ve Şubeler)**					
Telefon:		Faks:		E-Posta:	
İlgili Kişi/ YT:			Firma Yetkilisi:		
Veri Sorumlusu/ Ünvanı:			Veri İşleyen/ Ünvanı:		

Kullanılan Yazılım Uygulamaları:	
Kullanılan Bulut Sistemleri:	
Kullanılan Sunucu Hizmet Sağlayıcı:	
İnternet üzerinden satış durumu:	☐ Evet ☐ Hayır
E-posta/elektronik dokümanlarda dijital imza teknolojisi kullanımı:	☐ Evet ☐ Hayır
Smart Kart Teknolojisi kullanımı:	☐ Evet ☐ Hayır
3D Secure teknolojisi kullanımı:	☐ Evet ☐ Hayır
Ağ kullanım durumu:	☐ Wi-fi ☐ Mobil ağ ☐ Kablolu ağ
Elektronik kayıtların tutulması, internet trafiği kayıtlarının zaman kilitli tutulma durumu (log, depolama, back up vs):	☐ Evet ☐ Hayır
Uygulanabilirlik Bildirgesi (SOA) Tarih/Rev. No:	
BGYS Risk Analiz Tarihi/Rev. No:	

ISO 27001 BELGELENDIRME İÇIN ORGANIZASYON DETAYLARI:

1.Organizasyonel Yapı ve Personel Sayısı Detayları (Ref: ISO 27006:2024):

Adres veya saha ismi / Organizasyon	Üretim/ Saha Personel Sayısı				
	Merkez	Saha-1	Saha-2	Saha-3	Saha-4
Yönetici					
Muhasebe					
Finans Hizmetleri					
Güvenlik Hizmetleri					
Fiziksel Güvenlik Hizmetleri					
Bilgi Güvenliği Hizmetleri					
Bilgi Teknolojisi					
Yazılımcı					
Donanımcı					
Kurumsal bilgi sistemi yöneticisi					
Veri tabanı yöneticisi					
Satış Departmanı					
Kalite Kontrol					
Diğer- Organizasyon					

Toplam IT departmanı çalışan sayısı:		Toplam IT dışı çalışan sayısı:	

2. Denetim Süresinin Hesaplanmasına Yönelik Faktörler (Ref: ISO 27006:2024 EK-D):

Tablo D.1 - Denetim süresinin hesaplanmasına yönelik faktörlerin sınıflandırılması

(Lütfen uygun seçeneği işaretleyiniz Not: bir madde için üç faktörden (düşük, orta, yüksek) aynı anda seçim yapılamaz, tek faktörden seçim yapılmalıdır.)

Faktörler (ISO 27006: 2024 Madde D.2'ye bağlı olarak)	**Faktörlerin Etkisi**		
	Düşük Faktör	**Normal Faktör**	**Yüksek Faktör**
a) BGYS'nin karmaşıklığı			
1-Bilgi güvenliği gereksinimleri [gizlilik, bütünlük ve kullanılabilirlik, (CIA)]	☐ Standart prosesler standart ve tekrarlanan görevler; birden fazla insanın bir organizasyonun kontrolü altında aynı görevleri yapması; az ürün veya servis olması, Sadece az hassas veya gizli bilgiler, az uygunluk gerekliliği	☐ Yüksek miktarda ürün ve hizmet ile birlikte standart ama tekrarlanmayan prosesler olması, Yüksek uygunluk gereklilikleri veya bazı hassas/gizli bilgiler	☐ Belgelendirilecek kapsam içinde karmaşık prosesler, yüksek sayıda ürün ve hizmetler, birçok iş ünitesi olması. (BGYS'nin yüksek derecede karmaşık veya nispeten yüksek miktarda özgün aktiviteleri kapsadığı durumlar.)
	Örneklerle Açıklayınız:		
2- Kritik varlık sayısı	☐ Az sayıda kritik varlıklara sahip olunması (CIA açısından)	☐ Bazı kritik varlıklara sahip olunması	☐ Çok kritik varlıklara sahip olunması
	Açıklama (Örn: müşteri ticari bilgileri, kişisel bilgiler, sağlık bilgileri vb.):		
3-Proses ve hizmet sayısı	☐ Birkaç arayüz ve iş ünitesine sahip sadece bir önemli prosese sahip olunması	☐ Birkaç arayüz ve iş birimlerine sahip 2-3 prosese sahip olunması	☐ Birçok arayüz ve iş birimlerine sahip 2'den fazla proseslere sahip olunması
	Açıklama:		
b) BGYS kapsamında gerçekleştirilen iş türü/türleri	☐ Kritik olmayan iş sektörlerinde çalışan organizasyonlar, Yasal gerekliliğin olmadığı düşük riskli işler	☐ Kritik iş sektörlerinde müşterisi olan organizasyonlar, Yüksek yasal gereklilikler	☐ Kritik iş sektöründe çalışan organizasyonlar, Yüksek riskli işler ve sınırlı yasal gereklilikler
	Açıklama:		
c) BGYS'nin önceden kanıtlanmış performansı	☐ Yakın zamanda sertifikalandırıldı veya -Sertifikalı değil ancak belgelendirilmiş iç denetimler, yönetim incelemeleri ve etkili sürekli iyileştirme sistemi dahil olmak üzere birkaç denetim ve iyileştirme döngüsü boyunca BGYS tam olarak uygulanmıştır	☐ Son gözetim denetimi yapıldı veya -Sertifikalı değil ancak BGYS kısmen uygulanıyor: Bazı yönetim sistemi araçları mevcut ve uygulanıyor; bazı sürekli iyileştirme süreçleri mevcut ancak kısmen belgelendirilmiş	☐ Sertifika yok ve yakın zamanda denetim yapılmamış veya -BGYS yeni ve tam olarak kurulmamıştır (örneğin, yönetim sistemine özgü kontrol mekanizmalarının eksikliği, olgunlaşmamış sürekli iyileştirme süreçleri, geçici süreç yürütme)
	Açıklama: Uygulanabilirlik Bildirgesi Tarihi: İç tetkik Tarihi: YGG Tarihi:		

d) BGYS'nin çeşitli bileşenlerinin uygulanmasında kullanılan teknolojinin kapsamı ve çeşitliliği (örneğin, farklı IT platformlarının sayısı, ayrılmış ağların sayısı) Bilişim varlıklarının sayısı (sunucu, network, dış arayüzler bilgi sistemleri vb.) Çalışma alanlarının toplam sayısı (dizüstü bilgisayarlar, masaüstü bilgisayarlar, akıllı telefonlar v.b.)	☐ Düşük çeşitliliğe sahip yüksek oranda standartlaştırılmış ortam (az sayıda IT platformu, seriler, işletim sistemleri, veri tabanları, ağ çalışmaları, vb.) * IT Varlığı < 500 veya * Donanım < 300 veya * Yazılım < 50 veya * İletişim Ağları < 10	☐ Standartlaştırılmış ancak değişik IT platformları, sunucular, işletim sistemleri, veri tabanları, ağ çalışmaları *500 ≤ IT Varlığı < 5000 veya *300 ≤ Donanım < 1000 veya * 50 ≤ Yazılım < 5000 veya * 10 ≤ İletişim Ağları <50	☐ IT'nin yüksek çeşitliliği veya karmaşıklığı (örneğin, birçok farklı ağ kesimi, sunucu veya veri tabanı türü, kilit uygulama sayısı) * IT Varlığı ≥ 5000 veya * Donanım ≥ 1000 veya * Yazılım ≥ 200 veya * İletişim Ağları ≥ 50
	Açıklayınız IT platformu sayısı: Server sayısı: İşletim sistemi sayısı: Uzaktan erişimli ağ sayısı:		
e) BGYS kapsamında kullanılan dış kaynak kullanımı ve üçüncü taraf düzenlemelerinin kapsamı	☐ Dış kaynak kullanımı olmaması ve tedarikçilere az bağımlılık veya İyi tanımlanmış, yönetilmiş ve izlenen dış kaynaklardan yararlanma veya Dış kaynak kullanan kuruluş BGYS'e sahip veya İlgili bağımsız teminat raporları mevcut olması	☐ Yönetilebilen birkaç dış kaynaktan yararlanma	☐ Tedarikçilere veya dış kaynaklardan yararlanmaya önemli iş aktivitelerinde yüksek bağımlılık veya Bilinmeyen miktar veya kapsamda dış kaynaktan yararlanma veya Birkaç yönetilmemiş dış kaynaktan yararlanma
	Açıklama:		
f) Bilgi sistemi gelişiminin kapsamı	☐ Kurum içi yazılım üretme yok Standartlandırılmış yazılım platformlarının kullanımı	☐ Karmaşık kurulum/parametrizasyon ile standartlandırılmış yazılım platformlarının kullanımı Yüksek derecede özelleştirilmiş yazılım Bazı geliştirme aktiviteleri (kurum içi veya dışarıdan sağlanan hizmetler)	☐ Önemli iş amaçları için birkaç devam eden projeyle birlikte kapsamlı iç yazılım geliştirme aktiviteleri
	Açıklama:		
g) Afet Kurtarma (DR) sahalarının sayısı ve saha sayısı	☐ Düşük kullanılabilirlik gereksinimleri ve alternatif DR sahası olmaması veya tek olması	☐ Orta veya Yüksek kullanılabilirlik gereksinimleri ve alternatif DR sitesi yok veya bir tane	☐ Yüksek kullanılabilirlik gereksinimleri, örneğin 7/24 hizmetler veya - Birkaç DR sahası veya - Birkaç veri merkezi
	Açıklama:		
h) Kontrollerin sayısı ve karmaşıklığı	☐ Bazı ortak kontrol alanlarının dahil edilmediği normalden daha az sayıda kontrol, örn. sistem geliştirme kontrollerinin veya	☐ Tipik kontrol sayısı ve karmaşıklığı	☐ Normalden daha fazla sayıda ayrıntılı ve karmaşık kontrol, örn. ağ protokolleri veya kriptografi ile ilgili birçok kontrol

	Açıklama:		
i) Gözetim veya yeniden belgelendirme denetimi için: ISO/IEC 17021-1, 8.5.3 e uygun olarak BGYS ile ilgili değişiklik miktarı ve kapsamı	☐ Son yeniden belgelendirme denetiminden bu yana değişiklik yok	☐ BGYS'nin kapsamı veya SoA'sında küçük değişiklikler, örneğin bazı politikalar, belgeler vb. veya -Yukarıdaki faktörlerde küçük değişiklikler	☐ BGYS'nin kapsamı veya SoA'sında büyük değişiklikler, örneğin yeni süreçler, yeni iş birimleri, alanlar, risk değerlendirme yönetimi metodolojisi, politikalar, dokümantasyon, risk işleme veya
	Açıklama:		

3.Diğer Bilgiler

BGYS kapsamında gizlilik oluşturan ve OBJEKTİF ile paylaşılamayacak gizli ve hassas bilgi (maaş bilgisi, personel özel bilgileri, ar-ge, tasarım, finansal bilgiler vb.) içeren kayıtlar var mı?	☐ Var ☐ Yok	Var, ise lütfen açıklayınız:
BGYS kapsamında yer alan ama denetimde kanıt/kayıt gösteremeyeceğiniz, bakmamızı istemeyeceğiniz özel bölümleriniz, uygulamalarınız, tesisleriniz vb. var mı? *	☐ Var ☐ Yok	Var, ise lütfen açıklayınız:
Belgelendirme kapsamı dışı proseslerinizi/faaliyetleriniz var mı?	☐ Var ☐ Yok	Var, ise lütfen bu proseslerinizin/faaliyetlerinizin neler olduğunu açıklayınız:
(Yukarıdaki soruya "Yok" işaretlediyseniz bu soruyu cevaplamayınız.) Kapsam dışı prosesler ve bu proseslerle ilgili bağlantı noktaları/lokasyonlar risk analizine konu edildi mi?	☐ Evet ☐ Hayır	Hayır, ise lütfen nedenlerini açıklayınız:

* *Gizli ya da hassas kayıtları incelemeden BGYS'nin uygun bir şekilde denetiminin yapılmasının mümkün olmadığı durumlarda uygun erişim düzenlemeleri sağlanana kadar belgelendirme denetimi gerçekleştirilemez.*

Aşağıda listelenmiş olan teknolojik alanlardan firmanızda kullanılanları ve alt yapı gerekliliklerinden ve uygulamalardan kendi bünyenizde gerçekleştirdiklerinizi işaretleyiniz.

Güvenlik Uygulamaları	Ağ ve Donanım	Yazılım ve Uygulama Temini	Yazılım ve Veri Uygulama Yönetimi
☐ Güvenlik sistemleri (firewall, proxy, IPS, IDS gibi) ☐ Kriptografi (SSL, VPN gibi) ☐ Teknik açıklık analizi (kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri) ☐ Kapalı devre izleme (CCTV vb.) ☐ Log yönetimi	☐ Yerel ağlar ☐ Geniş alan ağları ☐ Aktif ağ cihazları (Router, switch, hub, axesss point vb.) ☐ İletişim teknolojileri (mobil ağ, karasal ağ vb.) ☐ Kablosuz ağ teknolojileri ☐ Santral / sanal santral	☐ Uygulama geliştirme (asp.net, java, php, python vb.) ☐ Mobil uygulamalar ☐ Web tabanlı uygulamalar ☐ Paket programlar ☐ Müşteri ilişkileri yönetimi (CRM) ☐ Özelleştirilmiş yazılım temini	☐ Tasarım ve modelleme uygulamaları (CAD-CAM) (örn; autocad, 3D max gibi ☐ Elektronik mesajlaşma (e-posta, kurumsal anlık mesajlaşma) ☐ Fikri mülkiyet
Veri Yönetimi	**Üretim Yazılım Uygulama**	**Sistem Uygulamaları**	**E-Hizmet**
☐ Veri tabanları sistemleri DBA (mssql, mysql) ☐ Veri yönetimi teknikleri (büyük veri, veri madenciliği, iş zekâsı) ☐ Doküman Yönetim Sistemi ☐ Müşteri ilişkileri yönetimi (CRM) ☐ Kurumsal Kaynak Planlama (ERP)	☐ Endüstriyel kontrol sistemleri ☐ Elektronik devre tasarımları	☐ Bulut teknolojisi ☐ Yedekleme sistemleri (NAS, RAID, load balancer vb.) ☐ Sanallaştırma ☐ Sunucular ☐ Masaüstü yönetimi ☐ Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi) ☐ İşletim merkezleri ☐ İçerik filtreleme	☐ E-ticaret (online ödeme sistemleri) ☐ E-fatura ☐ E-arşiv ☐ E-defter ☐ IT hizmet yönetimi ☐ E-imza ☐ PCI/DSS
Diğer:			

Yetkili İmzası	Tarih