## EK-2 ISO 27001 Belgelendirme Başvuruları İçin

| | | | | | |
|---|---|---|---|---|---|
| Kuruluş Adı: | | | | | |
| Adres(ler):<br>**(Kalıcı Lokasyon ve Şubeler)** | | | | | |
| Telefon: | | Faks: | | E-Posta: | |
| İlgili Kişi/ YT: | | Firma Yetkilisi: | | | |

| | |
|---|---|
| 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 | | | | | |
| Yazılım-Yazılım Destek | | | | | |
| Donanımcı | | | | | |
| Kurumsal bilgi sistemi yöneticisi | | | | | |
| Veri tabanı yöneticisi | | | | | |
| Satış Departmanı | | | | | |
| Kalite Kontrol | | | | | |
| Diğer- Organizasyon | | | | | |

| | | | |
|---|---|---|---|
| Toplam IT departmanı çalışan sayısı: | | Toplam IT dışı çalışan sayısı: | |

*Birden fazla görevi bulunan personel bir kere sayılacaktır.

**BGYS Efektif Personeli, sisteme aktif olarak katkıda bulunanlar kişilerdir.

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,<br>Sadece az hassas veya gizli bilgiler, az uygunluk gerekliliği | ☐ Yüksek miktarda ürün ve hizmet ile birlikte standart ama tekrarlanmayan prosesler olması,<br><br>Yüksek uygunluk gereklilikleri veya bazı hassas/gizli bilgiler | ☐ Belgelendirilecek kapsam içinde karmaşık prosesler, yüksek sayıda ürün ve hizmetler, birçok iş ünitesi olması.<br>(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,<br>Yasal gerekliliğin olmadığı düşük riskli işler | ☐ Kritik iş sektörlerinde müşterisi olan organizasyonlar,<br>Yüksek yasal gereklilikler | ☐ Kritik iş sektöründe çalışan organizasyonlar,<br>Yüksek riskli işler ve sınırlı yasal gereklilikler |
| | Açıklama: | | |
| c) BGYS'nin önceden kanıtlanmış performansı | ☐ Yakın zamanda sertifikalandırıldı veya<br>-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<br>-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<br>-BGYS yeni ve tam olarak kurulmamıştır (örneğin, yönetim sistemine özgü kontrol mekanizmalarının eksikliği, olgunlaşmamış sürekli iyileştirme süreçleri, geçici süreç yürütme) |
| | Açıklama:<br>Uygulanabilirik Bildirgesi Tarihi:<br>İç tetkik Tarihi:<br>YGG Tarihi: | | |

| | | | |
|---|---|---|---|
| d) BGYS'nin çeşitli bileşenlerinin uygulanmasında kullanılan teknolojinin kapsamı ve çeşitliliği (örneğin, farklı IT platformlarının sayısı, ayrılmış ağların sayısı)<br><br>Bilişim varlıklarının sayısı (sunucu, network, dış arayüzler bilgi sistemleri vb.)<br><br>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.)<br><br>* IT Varlığı < 500 veya<br>* Donanım < 300 veya<br>* Yazılım < 50 veya<br>* İletişim Ağları < 10 | ☐ Standartlaştırılmış ancak değişik IT platformları, sunucular, işletim sistemleri, veri tabanları, ağ çalışmaları<br><br>*500 ≤ IT Varlığı < 5000 veya<br>*300 ≤ Donanım < 1000 veya<br>* 50 ≤ Yazılım < 5000 veya<br>* 10 ≤ İletişim Ağları <50 | ☐ IT'nin yüksek çeşitliliği veya karmaşıklığı (örneğin, birçok farklı ağ kesimi, sunucu veya veri tabanı türü, kilit uygulama sayısı)<br><br>* IT Varlığı ≥ 5000 veya<br>* Donanım ≥ 1000 veya<br>* Yazılım ≥ 200 veya<br>* İletişim Ağları ≥ 50 |
| | Açıklayınız<br>IT platformu sayısı:<br>Server sayısı:<br>İşletim sistemi sayısı:<br>Uzaktan erişimli ağ sayısı: | | |
| e) BGYS kapsamında kullanılan dış kaynak kullanımı ve üçüncü taraf düzenlemelerinin kapsamı | ☐ Dış kaynak kullanımı olmaması ve tedarikçilere az bağımlılık<br>veya<br>İyi tanımlanmış, yönetilmiş ve izlenen dış kaynaklardan yararlanma<br>veya<br>Dış kaynak kullanan kuruluş BGYS'e sahip<br>veya<br>İlgili bağımsız teminat raporları mevcut olması | ☐ Yönetilebilen birkaç dış kaynaktan yararlanma | ☐ Tedarikçilere veya dış kaynaklardan yararlanmaya önemli iş aktivitelerinde yüksek bağımlılık<br>veya<br>Bilinmeyen miktar veya kapsamda dış kaynaktan yararlanma<br>veya<br>Birkaç yönetilmemiş dış kaynaktan yararlanma |
| | Açıklama: | | |
| f) Bilgi sistemi gelişiminin kapsamı | ☐ Kurum içi yazılım üretme yok<br><br>Standartlandırılmış yazılım platformlarının kullanımı | ☐ Karmaşık kurulum/parametrizasyon ile standartlandırılmış yazılım platformlarının kullanımı<br>Yüksek derecede özelleştirilmiş yazılım<br>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<br>- Birkaç DR sahası veya<br>- 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 fiziksel kontrollerin olmaması | ☐ 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 - Yukarıdaki faktörlerde önemli değişiklikler |
| | 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/Yönetimi Hizmetleri | Veri Yönetimi |
|---|---|---|---|
| ☐ Güvenlik sistemleri (firewall, proxy, IPS, IDS gibi)<br>☐ Kriptografi (SSL, VPN gibi)<br>☐ Teknik açıklık analizi (kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri)<br>☐ Kapalı devre izleme (CCTV vb.)<br>☐ Log yönetimi<br>☐ İçerik filtreleme<br>☐ PCI/DSS | ☐ Yerel ağlar<br>☐ Geniş alan ağları<br>☐ Aktif ağ cihazları (Router, switch, hub, axesss point vb.)<br>☐ İletişim teknolojileri (mobil ağ, karasal ağ vb.)<br>☐ Kablosuz ağ teknolojileri<br>☐ Santral / sanal santral<br>☐ Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi)<br>☐ İşletim merkezleri | ☐ Uygulama geliştirme (asp.net, java, php, python vb.)<br>☐ Mobil uygulamalar<br>☐ Web tabanlı uygulamalar<br>☐ Paket programlar<br>☐ Müşteri ilişkileri yönetimi (CRM)<br>☐ Kurumsal Kaynak Planlama (ERP)<br>☐ Özelleştirilmiş yazılım temini<br>☐ Fikri mülkiyet<br>☐ Tasarım ve modelleme uygulamaları (örn; 3ds Max ve Flash MX gibi) | ☐ Veri tabanları sistemleri DBA (mssql, mysql)<br>☐ Veri yönetimi teknikleri (büyük veri, veri madenciliği, iş zekâsı)<br>☐ Doküman Yönetim Sistemi<br>☐ Bulut teknolojisi<br>☐ Yedekleme sistemleri (NAS, RAID, load balancer vb.) |

| Üretim Yazılım Uygulama | Sistem Uygulamaları | E-Hizmet | Diğer |
|---|---|---|---|
| ☐ Endüstriyel kontrol sistemleri<br>☐ Elektronik devre tasarımları<br>☐ Tasarım uygulamaları (CAD-CAM) (örn; autocad vb.) | ☐ Sanallaştırma (VMware, Hyper-V, KVM vb.)<br>☐ Sunucular<br>☐ Masaüstü yönetimi<br>☐ IT hizmet yönetimi | ☐ E-ticaret (online ödeme sistemleri)<br>☐ E-fatura<br>☐ E-arşiv<br>☐ E-defter<br>☐ E-imza<br>☐ Elektronik mesajlaşma (e-posta, kurumsal anlık mesajlaşma) | |

| Yetkili İmzası | Tarih |
|---|---|
| | |