|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Müşteri Kuruluş Adı  (Varsa Bağlı Olduğu Kuruluş) | æfirmaadiæ | | | | | | | | |
| Adres | æfirmaadresiæ | | | | | | | | |
| Telefon | æfirmatelefonæ | | Faks | æfirmafaksæ | | E-mail | | æfirmaepostaæ | |
| Müşteri Yetkilisi Adı/Soyadı |  | | | | | | | | |
| Yönetim Temsilcisi Adı/Soyadı | æyonetimtemsilcisiadiæ | | | | | | | | |
| Toplam Çalışan Sayısı | æbgyscalisansayisiæ | Vardiya sayısı/Vardiyada toplam çalışan sayısı | | |  | | Taşeron çalışan sayısı | | ætaseroncalisansayisiæ |
| BGYS Kapsamı Dahilinde Çalışan Sayısı | æbgyscalisansayisiæ | | | | | | | | |
| Belgelendirme kapsamındaki faaliyet alanları, departmanlar & prosesler | *Örn: FKM var mı?* | | | | | | | | |
| Dış kaynaklı prosesler (Bakım, yazılım desteği, IT faaliyetleri vb.) |  | | | | | | | | |
| Saha Sayısı | *FKM adresi farklıysa yazınız* | | | | | | | | |
| Varsa Saha Bilgileri | Adres | | | | | Faaliyet Alanları, Departmanlar&Prosesler | | | Çalışan  Sayısı |
|  | | | | |  | | |  |
|  | | | | |  | | |  |
|  | | | | |  | | |  |
| Mevcut belgeler | ISO 9001  ISO 14001  Diğer…………… | | | | | | | | |
| İncelenmesini istemediğiniz gizlilik içeren dokümanınız mevcut mu? |  | | | | | | | | |
| Uymakla yükümlü olduğunuz yasal mevzuat ve standardlar |  | | | | | | | | |
| SoA Revizyon No/Tarihi | æsoarevnodateæ | | | | | | | | |
| ISO/IEC 27001:2022 Ek-A kontrol listesinden hariç tutulan kontrol varsa bilgi veriniz. |  | | | | | | | | |

Sektör ve Teknolojik Alan Bilgisi; (Lütfen hangi sektörde faaliyet gösterdiğinizi belirtiniz)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sektör  Grubu | Sektör | Risk Grubu | Teknik Alan | Teknik  Alan Kodu | İlgili Alanı  İşaretleyiniz |
| A | Üretim | Karmaşıklık faktörleri  her kuruluş için ayrı ayrı belirlenir | Üretim | A.01 |  |
| B | Hizmet | Hizmet | B.01 |  |
| C | Bilişim  Teknolojileri | Yüksek | Yazılım ve programlama hizmetleri danışmanlık ve servisi | C.01 |  |
| D | Özel | Yüksek | Kamu Yönetimi | D.01 |  |
| Eğitim | D.02 |  |
| Finans | D.03 |  |
| Sağlık | D.04 |  |
| Havacılık | D.05 |  |
| Telekomünikasyon | D.06 |  |
| Enerji | D.07 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Teknolojik  Alan Kodu | Teknik Grup | Kodu | İlgili Alanı  İşaretleyiniz |
| T | Bulut teknolojisi ve sanallaştırma  (Yedekleme ve replikasyon kontrolleri, malware tehlikeleri, vb.) | T.01 |  |
| Ağ ve sistem güvenliği  (Domain Controller tasarımı, yetkilendirme, çift yönlü doğrulamalar, sunucu rol bazlı güvenliği, VPN, son kullanıcı anomalileri vb.) Data Center Alt Yapı  (Kablo güvenliği, yapılandırma, sunucu odası gereksinimleri vb.) VOIP Sistemler  (IP üzerinden ses iletimi. Örnek; santraller, IP telefonlar vb.) | T.02 |  |
| Yazılım ve veri tabanı geliştirme güvenliği  (Yazılım yetki yapısı, kaynak kodları, geliştirme ve test ortamları, vb.) Web servis sistemleri, E-ticaret sistemleri, mobil teknolojiler | T.03 |  |
| Siber güvenlik, zafiyet analizi  (Penetrasyon testleri) Kriptografik Kontroller  (Disk şifreleme, e-imza, vb.) | T.04 |  |
| Endüstriyel kontrol sistemleri  (SCADA alt yapısı, HES, doğalgaz santralleri, elektrik-gaz dağıtım şirketleri vb.) Üretim teknolojileri (Cad/Cam, ERP, otomasyon yazılımları, reçete vb.) | T.05 |  |

|  | Çabaya olan etkisi | | |
| --- | --- | --- | --- |
| Azaltılmış | Normal | Artırılmış |
| Bilgi güvenliği gereklilikleri [gizlilik, bütünlük ve erişilebilirlik] | Sadece az hassas veya gizli bilgiler, düşük erişilebilirlik gereklilikleri | Daha yüksek erişilebilirlik gereklilikleri olan veya bazı hassas/gizli bilgiler | Hassas veya gizli bilgilerin miktarının fazlalığı  (ör: sağlık, kişiyi tanımlamak için kullanılan bilgiler, sigorta, bankacılık) veya yüksek erişilebilirlik gereklilikleri |
| Kritik varlık sayısı | 1-3 önemli varlık | Bazı kritik varlıklar | Birçok önemli varlık |
| Proseslerin ve hizmetlerin sayısı | 1 basit proses | 2-3 basit proses | 3’ten fazla karmaşık proses |
| BGYS kapsamında uygulanan iş türü/türleri | Düzenleyici gereklilikleri olmayan düşük riskli iş türü/türleri | Yüksek düzenleyici gereklilikleri | Kısıtlı düzenleyici gerekliliklere sahip yüksek riskli iş kolları |
| Daha önceden ispat edilmiş BGYS performansı | Yeni belgelendirilmiş  Belgelendirilmemiş, ama, BGYS dokümante edilmiş; iç denetimler, yönetim gözden geçirmeleri ve etkili sürekli iyileştirme sistemi dahil birçok denetim ve iyileştirme döngülerinde tam olarak uygulanmış | Gözetim denetimi yapılmış  Belgelendirilmemiş ama kısmen uygulanmakta olan BGYS: Bazı yönetim sistemi araçları mevcut ve uygulanmakta; bazı sürekli iyileştirme prosesleri yürürlükte ancak kısmen dokümante edilmiş | Belgelendirilmemiş ve yakın geçmişte denetimi yapılmamış  BGYS yeni ve tam olarak kurulmamış (ör: yönetim sistemine özgü kontrol mekanizmalarının eksikliği, olgunlaşmamış sürekli iyileştirme prosesleri, özel proses uygulaması) |
| BT platform sayısı | Basit 1-3 | Standardlaştırılmış 3’ten çok çeşitli | Karmaşık veya 3’ten çok çeşitli |
| Sunucu sayısı | Basit 1-3 | Standardlaştırılmış 3’ten çok çeşitli | Karmaşık veya 3’ten çok çeşitli |
| İşletim sistemi sayısı | Basit 1-3 | Standardlaştırılmış 3’ten çok çeşitli | Karmaşık veya 3’ten çok çeşitli |
| Veri tabanı sayısı | Basit 1-3 | Standardlaştırılmış 3’ten çok çeşitli | Karmaşık veya 3’ten çok çeşitli |
| Bölünmüş ağ sayısı | Basit 1-3 | Standardlaştırılmış 3’ten çok çeşitli | Karmaşık veya 3’ten çok çeşitli |
| BGYS kapsamında kullanılan dış kaynak kullanımı kapsamı ve üçüncü taraf düzenlemeleri | Hiçbir dış kaynak kullanımı olmaması veya 1 yönetilen dış kaynak kullanımı | 1-3 kısmen yönetilen dış kaynak düzenlemeleri | 3’ten çok önemli dış kaynak kullanımı veya bilinmeyen miktar veya kapsamda dış kaynak kullanımı veya 1’den çok yönetilmeyen dış kaynak kullanımı |
| Bilgi sistemleri geliştirmenin kapsamı | Kuruluş içi sistem geliştirme yok  Standardlaştırılmış yazılım platformlarının kullanımı | Karmaşık yapılandırma/ parametreli standardlaştırılmış yazılım kullanımı  Kişiselleştirilmiş yazılım  Bazı geliştirme faaliyetleri (kuruluş içi veya dış kaynaklı | Önemli iş hedefleri için devam eden proje ile birlikte kapsamlı iç yazılım geliştirme faaliyetleri |
| Bölge sayısı ve Felaket Kurtarma (DR) bölgeleri sayısı | Düşük erişilebilirlik gereklilikleri ve alternatif bir Felaket Kurtarma bölgesinin olmaması veya 1 tane olması | Orta veya yüksek erişilebilirlik gereklilikleri ve alternatif bir Felaket Kurtarma bölgesinin olmaması veya 1 tane olması | Yüksek erişilebilirlik gereklilikleri (ör. 7/24 hizmet)  1’den çok alternatif Felaket Kurtarma bölgeleri olması  1’den çok Veri Merkezi olması |
| Gözetim veya yeniden belgelendirme denetimi: ISO/IEC 17021-1, 8.5.3’e uygun olarak BGYS ile ilişkili değişim | Son yapılan yeniden belgelendirme denetiminden sonra değişiklik yok | BGYS kapsamındaki veya (SoA)’daki küçük değişiklikler ör. bazı politikalar, dokümanlar vb. | BGYS kapsamındaki veya (SoA)’daki önemli değişiklikler, ör. yeni prosesler, yeni iş birimleri, alanlar, risk değerlendirme yönetimi metodu, politikalar, dokümantasyon, risk işleme |

|  |  |  |  |
| --- | --- | --- | --- |
| Müşteri Yetkili İmzası | æyonetimtemsilcisiadiæ | Tarih |  |

Bu bölüm, Aliment tarafından doldurulacaktır.

|  |  |  |  |
| --- | --- | --- | --- |
| Denetim Zamanı Hesabı/Azaltma ve Arttırma Gerekçeleri | | | |
| İş karmaşıklığı |  | BT Karmaşıklığı |  |
| Arttırma/Azaltma Puanı |  | Azaltma/Arttırma Yüzdesi | ætotoran270011æ |
| *Denetim Zamanı* | æmerkez27sureæ | *Azaltma/Arttırma Sonrası Denetim Zamanı* | æsonuctoplamgunæ |
| *-varsa- Entegrasyon İndirimi Yüzdesi* | æentegreazaltmaoraniæ | *-varsa- Denetim hazırlık ve Raporlama İndirimi* |  |
| *Azaltma ve Arttırma Gerekçeleri ve Varsa Notlar* | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Teknik Alan |  | Teknolojik Alan |  |
| Denetim için önerilen Denetçi/Teknik Uzman | ædenetimeonerilendenetciæ | | |
| Karar için önerilen Denetçi/Teknik Uzman | æuye1adiæ | | |

\*Gözden geçirende ilgili teknik alan/teknolojik alan bilgisi bulunmaması durumunda, ilgili ilgili teknik alan/teknolojik alan için atanmış bir denetçi veya teknik uzman tarafından da gözden geçirilerek imzalanmalıdır.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Gözden Geçiren | | | Gözden Geçiren | | |
| Ad Soyad –  Teknik Alan/Teknolojik Alan | Tarih | İmza | Ad Soyad –  Teknik Alan/Teknolojik Alan | Tarih | İmza |
|  |  |  |  |  |  |