IT BAŞVURU BİLGİ FORMU

FİRMA ÜNVANI	
İşletmenin başvuru standardı *(ISO/IEC 20000-1, ISO 22301, ISO/IEC 27001, ISO/IEC 27701, ISO 42001)* kapsamında yer alan faaliyetleri hakkında standart bazında ayrı ayrı belirtiniz?	
CyberCert A.Ş.'yi nereden tanıyorsunuz?	
Belgelendirme Kapsamı Nedir?	
Daha büyük bir işletme ile ilişkiniz varsa bilgi veriniz.	
Belgelendirme kapsamında kamusal bilgiler yer alıyor mu? (Örneğin toplumsal, vatandaşlık, e-devlet bilgileri vb)	
Belgelendirme kapsamında kişisel veriler yer alıyor mu? (telefon no, e-posta, vatandaşlık, e-devlet bilgileri vb) ***ISO 27001 / 27701 başvurusu için*	
Kapsam dahilinde varsa kontroller için ziyaret etmemiz gereken başka yer var mıdır? (lokasyonlar, data-center, yazılım geliştirme, teknopark, Ar-Ge ofisleri, Felaket Kurtarma Merkezi vb)	
Faaliyet gösterdiğiniz sektörü aşağıdakilerle sınırlı kalmayarak belirtiniz. Seçim birden çok olabilir. *(Sağlık sektörü, hizmet (istihdam) sektörü, finans sektörü, ulaştırma (lojistik) sektörü, savunma sanayi, enerji sektörü)*	
İç denetimlerde çıkan uygunsuzluk sayısı nedir? (veya bir önceki denetimde çıkan uygunsuzluk sayısı)	
Kurumsal yazılım uygulamaları sayısı nedir? Nelerdir?	
Yapay zekâ destekli yazılım uygulamaları sayısı nedir? Nelerdir? Detay veriniz?	
Bilgi teknolojileri birimindeki çalışan sayısı nedir?	
PC / laptop ve kullanıcı sayısı nedir?	
Başvuru standardı *(ISO/IEC 20000-1, ISO 22301, ISO/IEC 27001, ISO/IEC 27701, ISO 42001)* kapsamında eğitimler alındı mı? Evet ise alınan eğitimlerin isimleri nelerdir? (Ör: BGYS, KVYS, İSYS, BTHYS, YZYS vb.)	
Uymakla yükümlü olduğunuz yasal ve diğer düzenleyici hususları belirtiniz. **ISO/IEC 20000-1, ISO 22301, ISO/IEC 27001, ISO/IEC 27701, ISO 42001 her biri için ayrı ayrı*	
Kuruluşunuzda gizli veya hassas bilgiler içermesi sebebiyle denetim ekibine gösteremeyeceğiniz ISO/IEC 20000-1, ISO 22301, ISO/IEC 27001, ISO/IEC 27701, ISO 42001 alanlarınız, dokümanlarınız veya kayıtlarınız var mı? Varsa nelerdir? Not: **CyberCert A.Ş.** bu dokuman ve kayıtların eksikliğinde yönetim sisteminin yeterli bir şekilde denetlenip denetlenemeyeceğine karar verecektir. **CyberCert A.Ş.**, denetim için bazı dokuman ve kayıtlar önemli olup elde edilemiyorsa, ya da yeterli derecede erişim imkânı sağlanmadığı sürece bir denetim yapmayacaktır.	

YÖNETİM SİSTEMİNİZ		
Başka bir sistem ile entegre mi?	☐ Evet	☐ Hayır
Belgelendirilmiş bir Yönetim Sisteminiz var mı?	☐ Evet	☐ Hayır

Not: Sadece başvurunuz ile ilgili alanları doldurunuz. Başvuruya konu olmayan standart özel gerekliliklerini doldurma zorunluluğu yoktur?

ISO/IEC 20000-1, ISO 22301, ISO/IEC 27001 ISO/IEC 27701, ISO 42001 takımında/larında kaç görevli personel mevcut? Her standart için ayrı ayrı belirtiniz?		
Dokümantasyonunuz gözden geçirmeye hazır mı?	☐ Evet	☐ Hayır

ISO 22301 Başvurularına özel;

Ana Risk Kategorileriniz ve yaptığınız çalışmalar ile ilgili bilgi veriniz? **Ör:** - Siber riskler (siber saldırılar, veri ihlalleri, hizmet kesintileri) - Doğal afetler (deprem, sel, yangın, fırtına vb.) - Tedarik zinciri kesintileri (kritik tedarikçilerin iflası, lojistik sorunlar) - Teknoloji altyapısı arızaları (sunucu, ağ, yazılım hataları) - İnsan kaynaklı riskler (grev, iş gücü kaybı, insan hataları) - Enerji ve altyapı kesintileri (elektrik, su, telekomünikasyon) - Yasal ve düzenleyici uyumsuzluklar	
İş Etki Analizi (BIA) Özet Bilgileriniz? **Ör:** - Kritik iş süreçlerinin tanımlanması - Her süreç için maksimum toleranslı kesinti süresi (MTPD) - Kurtarma zamanı hedefi (RTO) ve kurtarma noktası hedefi (RPO) - Süreçlerin finansal, operasyonel ve yasal etkilerinin analizi - Süreçler arası bağımlılıkların belirlenmesi	

ISO 42001 Başvurularına özel;

Lütfen firmanızın yapay zeka kullanımı hakkında bilgi veriniz.	Yapay Zekâ Üreticisi ☐ Yapay Zekâ Geliştiricisi ☐	Yapay Zekâ Kullanıcısı ☐ Yapay Zekâ Entegre Kullanıcısı ☐
Ek-A kontrol listesinden hariç bırakılan maddeler hangileridir? Hariç bırakma gerekçelerini mutlaka belirtiniz.		

ISO/IEC 27001 ISO/IEC 27701 Başvurularına özel;

Aşağıdaki seçeneklerden firmanız için uygun olan maddeleri işaretleyiniz.

IT dışında İşletme ve organizasyonla ilgili	İşletme türü ve yasal zorunluluklar	**1.** ☐ Organizasyon, kritik olmayan ticaret sektörlerinde ve düzenlenmeyen sektörlerde çalışır * **2.** ☐ Organizasyon kritik iş alanlarında müşterilere sahiptir * **3.** ☐ Organizasyon kritik iş alanlarında çalışır *
	Süreç ve görevler	**1.** ☐ Standart ve tekrarlayan görevlerle standart süreçler; Aynı görevleri yerine getiren örgütün kontrolü altında çalışan birçok insan; Az sayıda ürün veya hizmet **2.** ☐ Yüksek sayıda ürün veya hizmet ile standart süreçler (ancak tekrarlama gerektirmeyen işlemler) **3.** ☐ Karmaşık süreçler, çok sayıda ürün ve hizmet, belgelendirme kapsamına giren birçok işletme birimi (BGYS, oldukça karmaşık işlemler veya nispeten yüksek sayı veya benzersiz faaliyetler kapsar)
	Yönetim Sisteminin kuruluş düzeyi	**1.** ☐ BGYS zaten iyi kurulmuş ve / veya diğer yönetim sistemleri mevcut **2.** ☐ Diğer yönetim sistemlerinin bazı unsurları uygulanmakta, diğerleri de uygulanmaktadır. **3.** ☐ Hiçbir şekilde uygulanan başka bir yönetim sistemi yok, BGYS yeni ve kurulmamış
Bilgi teknolojisi ortamıyla ilgili faktörler	BT altyapısı karmaşıklığı	**1.** ☐ Az yada çok standartlaştırılmış BT platformları, sunucular, işletim sistemleri, veri tabanları, ağlar vs. **2.** ☐ Birkaç farklı BT platformu, sunucu, işletim sistemi, veri tabanı, ağ **3.** ☐ Birçok farklı IT platformu, sunucu, işletim sistemi, veri tabanı, ağ
	Bulut hizmetlerini de içeren dış kaynak kullanımı ve tedarikçilere bağımlılık	1. ☐ Dış kaynak kullanımına veya tedarikçilerine çok az veya hiç bağımlılık yok 2. ☐ Dış ticarete ya da tedarikçilere, bazılarının önemli iş faaliyetleri değil de bazılarına bağımlılıkları. 3. ☐ Dış kaynak kullanımına veya tedarikçilerine yüksek bağımlılık, önemli ticari faaliyetler üzerinde büyük etki
	Bilgi Sistemi geliştirme	1. ☐ Hiçbiri veya çok sınırlı bir şirket içi sistem / uygulama geliştirme 2. ☐Bazı önemli iş amaçları için bazı kurum içi veya dışarıdan kaynaklanan sistem / uygulama geliştirme 3. ☐Önemli iş amaçları için geniş dâhili veya dışarıdan kaynaklanan sistem / uygulama geliştirme

İşletmenizin Risk Faktörleri

Gizlilik, bütünlük ve erişilebilirlik (GBE) gereksinimlerini karşılamak için bilgilerin kritiklik derecesi ve İlgili yönetim sisteminin karmaşıklığı nedir?	☐ Yalnızca küçük, hassas veya gizli bilgiler (Örneğin,sağlık, maaş bilgisi, personel özel bilgisi, Ar-Ge, tasarım, finansal bilgiler vb), düşük kullanılabilirlik gereksinimleri		
	☐ Bazı hassas / gizli bilgiler (Örneğin, maaş bilgisi, personel özel bilgisi, ar-ge, tasarım, finansal bilgiler vb) veya daha yüksek kullanılabilirlik gereksinimleri		
	☐ Daha yüksek miktarda hassas veya gizli bilgi (ör. Sağlık, kişisel olarak tanımlanabilir bilgiler vb) veya yüksek kullanılabilirlik gereksinimleri		
Kritik varlıkların sayısı nedir?	☐ Çok az kritik varlık (GBE açısından	☐ Birkaç ara yüzlü 2-3 basit iş süreci	☐ Birçok kritik varlık
İlgili yönetim sistemi kapsamındaki süreç ve hizmetlerin sayısı nedir?	☐ Az sayıda ara yüz ve birkaç iş birimi içeren yalnızca bir anahtar iş süreci ☐ Birkaç ara yüzlü 2-3 basit iş süreci ☐ Pek çok ara yüz ve iş birimi ile 2'den fazla karmaşık süreç		
İlgili yönetim sistemi kapsamında yapılan işin türü / türleri	☐ Düzenleyici gereklilikler olmaksızın düşük riskli iş ☐ Yüksek düzenleyici gereklilikler ☐ Sınırlı yasal gerekliliklerle (yalnızca) yüksek riskli iş		
İlgili yönetim sisteminin çeşitli bileşenlerinin uygulanmasında	☐ Düşük çeşitlilikle (BT platformları, sunucuları, işletim sistemleri, veri tabanları, ağlar, vb.) Çok yüksek standartlara sahip ortam		

Not: Sadece başvurunuz ile ilgili alanları doldurunuz. Başvuruya konu olmayan standart özel gerekliliklerini doldurma zorunluluğu yoktur?

kullanılan teknolojinin kapsamı ve çeşitliliği (örneğin; farklı IT platformlarının sayısı, ayrılmış ağların sayısı)	☐ Standartlaşmış ama farklı BT platformları, sunucuları, işletim sistemleri, veri tabanları ve ağları
	☐ Yüksek çeşitlilik veya BT karmaşıklığı (örneğin, birçok farklı ağ bölümü, sunucu türü veya veri tabanı sayısı, önemli uygulamalar sayısı) Bilinmeyen miktar veya ölçüde dış kaynak kullanımı Birkaç yönetilmeyen dış kaynak düzenlemeleri
Dış kaynak kullanımının kapsamı ve yönetim sistemi kapsamında kullanılan üçüncü taraf düzenlemeleri	☐ Dış kaynak kullanımı yok ve tedarikçilere az bağımlılık İyi tanımlanmış, yönetilen ve izlenen dış kaynak kullanımı düzenlemeleri İşveren, sertifikalı bir BGYS'ye sahiptir. İlgili bağımsız güvence raporları mevcuttur.
	☐ Kısmen yönetilen dış kaynak kullanımı düzenlemeleri
	☐ Dış ticarete veya tedarikçilere önemli ticari faaliyetler üzerinde büyük etkisi olan yüksek bağımlılık
Bilgi sistemi geliştirmenin kapsamı	☐ Dâhili/kurum içi sistem geliştirme yok Standartlaştırılmış yazılım platformlarının kullanımı
	☐ Karmaşık yapılandırma / parametreleştirme ile standartlaştırılmış yazılım platformlarının kullanımı (Oldukça yüksek) özel yazılım Bazı geliştirme faaliyetleri (kurum içi veya dış kaynaklı)
	☐ Önemli iş amaçlı devam eden çeşitli projelerle kapsamlı dâhili yazılım geliştirme faaliyetleri
Denetim yapılacak lokasyonların sayısı ve Felaket Kurtarma (DR) lokasyonlarının sayısı	☐ Düşük kullanılabilirlik gereksinimleri ve bir veya daha fazla alternatif DR lokasyonu
	☐ Orta veya Yüksek kullanılabilirlik gereksinimleri ve bir veya daha fazla alternatif DR lokasyonu
	☐ Yüksek kullanılabilirlik gereksinimleri, ör. 7/24 hizmet ☐ Birkaç alternatif DR lokasyonu ☐ Çeşitli Veri Merkezleri
Gözetim veya yeniden belgelendirme denetimi için BGYS ile ilgili değişiklik miktarı ve kapsamı	☐ Son yeniden belgelendirme denetiminden bu yana değişiklik yok
	☐ BGYS kapsamındaki veya SoA'daki küçük değişiklikler, ör. Bazı politikalar, belgeler vb. Yukarıdaki faktörlerde ufak değişiklikler
	☐ BGYS kapsamındaki veya SoA'daki büyük değişiklikler, ör. Yeni süreçler, yeni iş birimleri, alanlar, risk değerlendirme yönetim metodolojisi, politikalar, dokümantasyon, risk işleme Yukarıdaki faktörlerin büyük değişimleri
Daha önce İlgili yönetim sistemi gösterdiği performans	☐ Son zamanlarda sertifikalı ☐ Sertifikalı değil ancak çeşitli denetim ve iyileştirme döngülerinde tam olarak uygulanan İlgili yönetim sistemi: dokümante edilmiş iç denetimleri, yönetimin gözden geçirmesini ve etkin sürekli iyileştirme sistemini de içerecek şekilde
	☐ Son gözetim denetimi ☐ Sertifikalı değil ancak kısmen uygulanan İlgili yönetim sistemi: Bazı yönetim Sistem araçları mevcuttur ve uygulanır; Bazı sürekli iyileştirme süreçleri mevcut ancak kısmen belgelenmiştir.
	☐ Sertifikasyon yok ve son denetimler yok ☐ İlgili yönetim sisteminin yeni ve tam olarak kurulu değil. (örneğin, yönetim sistemine özel kontrol mekanizmalarının eksikliği, geliştirilmemiş sürekli iyileştirme süreçleri, geçici süreç yürütme)

İnternet üzerinden satış yapıyor musunuz?	☐ Evet. ☐ Hayır	Bulut Bilişim kullanıyor musunuz?	☐ Evet. ☐ Hayır
E-posta/Elektronik Dokümanlarda sayısal imzalama teknolojisi kullanıyor musunuz?	☐ Evet. ☐ Hayır	Mobil iletişim Teknolojileri ve Mobil Uygulamalar kullanıyor musunuz?	☐ Evet. ☐ Hayır
Smart Kart Teknolojisi kullanıyor musunuz?	☐ Evet. ☐ Hayır	Veri Madenciliği ve Veri Depolama yapıyor musunuz?	☐ Evet. ☐ Hayır
3D Secure Teknolojisi kullanıyor musunuz?	☐ Evet. ☐ Hayır	Yazılım Test Teknolojileri Kullanıyor musunuz?	☐ Evet. ☐ Hayır
Firmanızda belirtilen ağlardan hangileri kullanılıyor?	☐ Wired N. ☐ Wi-Fi N ☐ Mobil N	Veri Tabanı Sistemleri kullanıyor musunuz?	☐ Evet. ☐ Hayır
Elektronik kayıtlar tutuluyor mu? (Log, Depolama, Back up vs)	☐ Evet ☐ Hayır	Uydu Haberleşme Teknolojileri kullanıyor musunuz?	☐ Evet. ☐ Hayır
İnsan-Bilgisayar Etkileşimi uygulanıyor mu? / Is	☐ Evet ☐ Hayır	Yapay Zeka kullanıyor musunuz?	☐ Evet. ☐ Hayır
Bağımsız Karar Verme Sistemleri kullanıyor musunuz?	☐ Evet. ☐ Hayır	İletişim Sistemleri ve Uygulamaları kullanıyor musunuz?	☐ Evet. ☐ Hayır
E-altyapı kullanıyor musunuz?	☐ Evet. ☐ Hayır	Dijital Kütüphane kullanıyor musunuz?	☐ Evet. ☐ Hayır

BGYS kontrolleri için üst yönetimin desteği ve ayrılmış bütçesi mevcut mu?	
ISO/IEC 27001 ISO/IEC 27701 standartlarında Ek-A kontrol listesinden hariç bırakılan maddeler hangileridir? Her standart için ayrı belirtiniz? Hariç bırakma gerekçelerini mutlaka belirtiniz.	
Uygulanabilirlik Bildirgesi yayın tarihi ve son revizyonunu ve/veya Uygulanabilirlik Bildirgesi yanında kullandığınız diğer kontrol grupları/maddeleri varsa belirtiniz? Bildirgeniz (SOA) gözden geçirme için hazır mı?	
Kriptoloji Kullanılan şifreleme teknikleri belirtiniz. (Örneğin; DSA, Diffie – Hellman, DES vb.)	

Not: Sadece başvurunuz ile ilgili alanları doldurunuz. Başvuruya konu olmayan standart özel gerekliliklerini doldurma zorunluluğu yoktur?

Varsa yazılım geliştirme ekibindeki çalışan sayısı?	
Sunulan bilgi teknolojileri hizmetleri ile ilgili çalışan destek personel sayısı nedir?	
Sistem yöneticisi, network yöneticisi ve veri tabanı yöneticisi toplam sayısı nedir?	
Lütfen firmanızın Kişisel Verinin korunması kapsamında türünü belirtiniz. -Eğer firmanız hem veri sorumlusu hemde veri işleyen ise yukarıdaki kişi sayılarını ayrı ayrı yazınız. **ISO 27701 başvurusu için*	Veri Sorumlusu ☐ Veri İşleyen ☐

Eğer firmanız Veri Sorumlusu ise; Lütfen kaç kişinin verisini tuttuğunuzu belirtiniz. - Bu tip firmalar sadece kendi çalışanlarının ve varsa gerekli durumlarda müşterilere ait kişisel verileri saklayan firmalardır.		Eğer firmanız Veri İşliyor ise; Lütfen kaç kişinin verisini işlediğini belirtiniz. - Bu tip firmalar ise; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişilerin bilgilerini tutan firmalardır.	

ISO/IEC 20000-1 Başvurularına özel;

Sunulan bilgi teknolojileri hizmetleri ile ilgili kullanılan sunucular, veri tabanları ve ağları, yazılım dilleri, geliştiriciler vb.	
Genel olarak İç veya Dış Müşterinize Sunulan Bilgi Teknolojileri Hizmetlerini Yazınız	
İç veya dış Müşterinize Sunulan Bilgi Teknolojileri süreçlerini Yönetmek için Program kullanıyor musunuz?	Hayır ☐ Evet ☐ Cevabınız evet ise programın adını yazınız:
Bilgi Teknolojileri (BT) Hizmetlerinin Verildiği Taraflar	☐ Tüm Dış Müşteriler BT Hizmetlerimizden Yararlanabilmektedir. ☐ Tüm İç Müşteriler (Birimler) BT Hizmetlerimizden Yararlanabilmektedir. ☐ Bazı Dış Müşteriler (Sınırlı) BT Hizmetlerimizden Yararlanabilmektedir. * ☐ Bazı İç Müşteriler (Birimler) BT Hizmetlerimizden Yararlanabilmektedir. * *Aşağıdaki Tabloyu Doldurunuz

İç Müşteri ☐		İç Müşteri ☐	
Hizmet Verilen Birimler	Verilen Hizmet	Hizmet verilen Müşteriler	Verilen Hizmet

İç veya Dış Müşterinize Bilgi teknolojileri Hizmetleri sunumu konusunda Tedarikçi kullanıyor musunuz? :	☐ Hayır ☐ Evet Cevabınız Evet ise aşağıdaki tabloyu doldurunuz

Tedarikçi Ünvanı	Tedarikçinin Hizmet Sağladığı Lokasyon Adresi	Tedarikçinin Sağladığı Hizmet

*** Kritik ticaret sektörleri,** kritik kamu hizmetlerini etkileyebilecek, sağlık, güvenlik, ekonomi, imaj ve hükümetin ülkeye karşı büyük bir olumsuz etkisi olabilecek bir risk oluşturabilecek sektörlerdir.