|  |  |
| --- | --- |
| **Firma - Kuruluş Unvanı & Company - Organization Title** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BGYS kapsamında yer alan ama denetimde özel (gizlilik) arz eden dokümanlar, bölümler, uygulamalar ve tesisleriniz hakkında bilgi veriniz.  NOT: Gizlilik arz eden doküman, bölümler, uygulama ve tesislerinizin varlığı BGYS denetiminin etkinliğini etkileyecek düzeyde ise gerekli düzenlemeler yapılmadan denetimin yapılamayacağı bilgisi tarafınıza iletilecektir.) &Provide information about the documents, departments, applications and facilities within the scope of ISMS but which are private (confidential) in the audit. NOTE: If the presence of your documents, departments, applications and facilities that are confidential will affect the effectiveness of the ISMS audit, you will be informed that the audit cannot be carried out without the necessary arrangements.) | | | | |
|  | | | | |
| BGYS Kapsamı İçindeki Prosesler-Departmanlar/Çalışan Sayıları  (tüm faaliyetler için yapılan başvurularda doldurulma zorunluluğu yoktur. FR.01 de belirtilen toplam çalışan sayısı üzerinden işlem yapılacaktır. BGYS için kapsamda olmasa dahi satınalma, IK ve idari işler bölümünde çalışan personel gerçekleştirilen faaliyetlere dahil olduğundan mutlaka belirtiniz.) (Processes-Departments / Number of Employees Under BGYS There is no obligation to be filled in applications made for all activities. Transactions will be made on the total number of employees specified in FR.01. Even if it is not in scope for BGYS , please state that the personnel working in the procurement, HR and administrative affairs department are included in the activities performed.) | Proses - Departman Adı & Process - Department Name | Çalışan Sayısı & Number of Employess | Proses - Departman Adı & Process - Department Name | Çalışan Sayısı & Number of Employess |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| BGYS Kapsamı içerisindeki toplam çalışan sayısı  Total number of employees within the scope of BGYS | | |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Hariç tutulan standart maddeleri  Excluded standard items |  | *Uygulanabilirlik Bildirgesi (SoA) doküman no ve son revizyon no & Statement of Applicability (SoA) document number and last revision number and date* |  |

|  |  |
| --- | --- |
| **20000-1 Kapsamında Gerçekleştirilen Hizmetler & Services Performed within the Scope of 20000-1** | |
| A.1 E-posta servisi & Email service | A.2 SMS servisi & SMS service |
| A.3 Kimlik doğrulama & Authentication | A.4 Hosting hizmeti & hosting service |
| A.5 Veri merkezi hizmeti & data center service | A.6 Yazılım bakım ve destek & Software maintenance and support |
| A.7 Sistem destek servisi & System support service | A.8 Network destek & Network support |
| A.9 Çağrı merkezi & Call center | A.10 Donanım teknik servis & Hardware technical service |
| A.11 Bulut hizmeti & cloud service | A.12 Uzaktan erişim platformu & remote access platform |
| A.13 SOC (Güvenlik) Hizmetleri & SOC (Security) Services | A.14 E Ticaret & E-Commerce |
| A.15 Yazılım Geliştirme & Software development | A.16 E-imza, Dijital imza & E-signature, Digital signature |
| A.17 E-fatura, E-defter, E-arşiv & E-invoice, E-book, E-archive | Diğer & Other................................ |

|  |  |  |
| --- | --- | --- |
| 27701 başvurularınız için lütfen size uygun başvuru durumunu seçiniz. & For your 27701 applications, please select the application status that suits you. | | |
| ISO 27001 ve 27701 ilk belgelendirme & ISO 27001 and 27701 initial certification | ISO 27001 sertifikası mevcuttur. (\*) 27001 gözetim denetimine entegre ISO 27701 tetkiki talep edilmektedir. & ISO 27001 certificate is available. (\*) ISO 27701 audit integrated with 27001 surveillance audit is requested. | ISO 27001 sertifikası mevcuttur. (\*) 27001 gözetim denetimden bağımsız ISO 27701 tetkiki talep edilmektedir. & ISO 27001 certificate is available. (\*) ISO 27701 audit independent from 27001 surveillance audit is requested. |
| 27701 kapsamında kişisel veriler için firmanıza uygun seçeneği işaretleyiniz. (\*\*) & Please tick the option appropriate for your company for personal data under 27701. (\*\*) | | |
| Elde edilen kişisel veriler için; veri işleme faaliyeti gerçekleştirilmektedir. & For the personal data obtained; data processing is carried out. | Elde edilen kişisel veriler için veri sorumluluğu vardır. & There is data responsibility for the personal data obtained. | Elde edilen kişisel veriler için hem veri sorumlusu hem de veri işleme prosesleri yürütülmektedir. & For the personal data obtained, both the data controller and the data processing processes are carried out. |

(\*) ISO 27701 başvurularında, IQM Belgelendirmeden alınmış bir ISO 27001 sertifikanız bulunmalı veya ISO 27001 ve ISO 27701 için birlikte başvurmanız gerekmektedir. Farklı bir belgelendirme kuruluşundan alınan ISO 27001 belgeniz var ise lütfen IQM belgelendirme operasyon sorumlusu ile iletişime geçiniz. & (\*) For ISO 27701 applications, you must have an ISO 27001 certificate obtained from IQM Certification or you must apply for ISO 27001 and ISO 27701 together. If you have an ISO 27001 certificate from a different certification body, please contact the IQM certification operation officer.

(\*\*) Veri Sorumlusu (PII Processor): veri sorumlusu, kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder. & (\*\*) Data Controller (PII Processor): means the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

Veri İşleyen (PII Controller): veri işleyen; veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, veri sorumlusunun organizasyonu dışındaki gerçek veya tüzel kişiler olarak tanımlanmaktadır. & Data Processor (PII Controller): data processor; It is defined as natural or legal persons outside the organization of the data controller, who process personal data on behalf of the data controller, based on the authority given by the data controller.

NOT 1: Aşağıdaki tabloda bulunan sorular denetim sürenizin belirlenebilmesi için çalışan sayınıza ek olarak hesaplamaya dahil edilen parametlerdir. Her soru için yan bölümde verilen açıklamalardan işletmenize uygun olanı işaretleyiniz. Tablodaki sorulara verdiğiniz cevaplar aşama 1 denetimi sırasında baş denetçi tarafından yerinde doğrulanacaktır**.** & The quest**i**ons **i**n the follow**i**ng table are parameters **i**ncluded to your employee number to add**i**t**i**on to your aud**i**t per**i**od. For every quest**i**ons, mark what **i**s su**i**table for your bus**i**ness from the explanat**i**ons **i**n the s**i**de sect**i**on. Your answers to the quest**i**ons **i**n the table w**i**ll be prov**i**ded **i**nstalled by the head aud**i**tor dur**i**ng the stage 1 aud**i**t.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Denetim Sürelerinin Belirlenmesi için Kuruluş Teknik Bilgileri & Organizational Technical Information for Determining Audit Periods* | | | | |
| S. N | İlgili Standart(lar) | Faktör | Evet / Var | Hayır / Yok |
| 1 | 27001, 27701 | Firmanızda birçok farklı yapıda BT platformları, sunucular, işletim sistemleri, veri tabanları ve ağlar kullanılmakta mıdır? & Are many different types of IT platforms, servers, operating systems, databases and networks used in your company? (+5) |  |  |
| 2 | 27001, 27701, 20000-1 | Önemli faaliyetlerde ve büyük oranda (en az 2 dış kaynaklı proses) dış kaynaklı proses kullanılıyor mu? İlgili taraflara yüksek oranda bağımlılığa sahip misiniz? & Are outsourced processes used in significant activities and to a large extent (at least 2 outsourced processes)? Do you have a high dependency on interested parties? (+5) |  |  |
| 3 | 27001, 27701 | Firmanızda belgelendirme kapsamında faaliyetlerin yürütülmesi sırasında çok sayıda teknolojik alan kullanımı (en az 15) & Use of a large number of technological fields during the execution of activities within the scope of certification in your company (at least 15) (+5) |  |  |
| 4 | 27001, 27701 | Ana ve/veya bilgi güvenliğini direk etkileyen faaliyetlerde kurum içi veya dış kaynak olarak bilgi sistem geliştirme faaliyeti uygulanıyor mu? & Is information system development activity implemented as an internal or external source in activities that directly affect the main and/or information security? (+5) |  |  |
| 5 | 27001, 27701 | Afet kurtarma sahalarınız yüksek kullanılabilirlik gereksinimleri içermekte midir? Örneğin 7/24 hizmet, birkaç alternatif durum kurtarma sahası, Birkaç data center & Do your disaster recovery sites have high availability requirements? For example, 24/7 service, several alternative disaster recovery sites, several data centers (+5) |  |  |
| 6 | 27001, 27701, 20000-1 | Faaliyetleriniz sırasında yüksek düzeyde yasal gereklilik uygulanıyor mu? (örneğin; telekomünikasyon, sağlık, enerji, finans sektörü gibi) & Are high legal requirements enforced during your operations? (for example; telecommunications, health, energy, financial sector, etc.) (+5) |  |  |
| 7 | 27001, 27701, 20000-1 | Belgelendirme kapsamınızın onaylanması için geçici sahaları ziyaret etmeyi gerektiren faaliyetlere sahip misiniz? (Kalıcı şubeler bu kapsamında dışındadır) & Do you have activities that require visiting temporary sites to validate your certification scope? (Permanent branches are excluded from this scope) (+5) |  |  |
| 8 | 27001, 27701, 20000-1 | Karmaşık lokasyonlarda birden fazla çalışma sahalarında faaliyet gerçekleştiriyor musunuz? & Do you operate at multiple sites in complex locations? (+5) |  |  |
| 9 | 27001, 27701, 20000-1 | Farklı dilde konuşan personellere sahip misiniz? Denetim sırasında tercüman gereksinimi bulunmakta mı? Dokümanlarınızın en azından bir kısmı farklı dillerde mi oluşturulmuş? & Do you have staff who speak different languages? Is there a need for an interpreter during the audit? Are at least some of your documents created in different languages? (+5) |  |  |
| 10 | 27001, 27701 | Birden fazla ana faaliyete sahip misiniz? (en az 3 ana faaliyet) & Do you have more than one main activity? (at least 3 main activities) (+5) |  |  |
| 11 | 27001, 27701, 20000-1 | Yüksek risklere sahip proses/faaliyetlere sahip misiniz? & Do you have high risk processes/activities? (+5) |  |  |
| 12 | 27001, 27701, 20000-1 | Tek bir ana faaliyet mi yürütüyorsunuz? & Do you run a single core business? (-5) |  |  |
| 13 | 27001, 27701, 20000-1 | Personelinizin önemli bir bölümü aynı ve/veya benzer ve basit görevleri yürütmekte midir? & Do a significant portion of your staff perform the same and/or similar and simple tasks? (-5) |  |  |
| 14 | 27001, 27701 | Düşük risklere sahip proses/faaliyetlere sahip misiniz? & Do you have low risk processes/activities? (-5) |  |  |
| 15 | 27001, 27701, 20000-1 | IQM Belgelendirmeden daha önce alınmış farklı sertifikalarınız var mı? & Do you have different certificates obtained from IQM Certification before? (-5) |  |  |
| 16 | 27001, 27701, 20000-1 | Farklı bir uygunluk değerlendirme kuruluşundan alınmış 27001, 27701 veya 20000-1 sertifikanız var mı? & Do you have a 27001, 27701 or 22301 certificate from a different conformity assessment body? (-5) |  |  |
| 17 | 27001, 27701 | 1 yıldan uzun süredir yönetim sistemi işletiyor musunuz? & Have you been operating management system for more than 1 years? |  |  |
| 18 | 27701 | Personelinize ait kişisel veriler yurt dışına çıkarılıyor/paylaşılıyor mu? Yurt dışında saklanıyor mu? & Are personal data of your personnel exported/shared abroad? Is it hiding abroad? (+5) |  |  |
| 19 | 27701 | Firmanızda son 3 yıl içerisinde kişisel veri kaybı yaşandı mı? & Has your company experienced any personal data loss in the last 3 years? (+5) |  |  |
| 20 | 27701 | Son 3 yıl içerisinde kişisel verilerin yönetimi ile ilgili dava, şikayet veya negatif geri bildirim alındı mı? & Have you received lawsuits, complaints or negative feedback regarding the management of personal data in the last 3 years? (+5) |  |  |
| 21 | 27701 | Satış ve pazarlama faaliyetleri için kişisel veri işliyor musunuz? & Do you process personal data for sales and marketing activities? (+5) |  |  |
| 22 | 27701 | Verbis yükümlülüğünüz var mı? & Do you have a verbis obligation? (+5) |  |  |
| 23 | 27701 | Hassas (özel nitelikli) kişisel veri işliyor musunuz? & Do you process sensitive (special quality) personal data? (+5) |  |  |
| 24 | 27701 | Kişisel verilerin korunması kanunu kapsamına ek olarak farklı yasal yükümlülükleriniz var mı? & Do you have different legal obligations in addition to the scope of personal data protection law? (+5) |  |  |
| 25 | 27701 | Müşterilere veya tedarikçi/taşeronlara ait kişisel veri işliyor musunuz? & Do you process personal data of customers or suppliers/subcontractors? (+5) |  |  |
| 26 | 20000-1 | HYS ve Hizmetlerinizdeki değişim oranı düşük olması. & The low rate of change in your SMS and Services. (-5) |  |  |
| 27 | 20000-1 | HYS hizmetlerindeki değişim oranının yüksek olması. & High rate of change in SMS services. (+5) |  |  |
| 28 | 20000-1 | Hizmetlerin sağlanması için çalışan; tedarikçiler, tedarikçi rolündeki iç gruplar veya müşteriler gibi ilgili taraflara düşük seviyede bağlılığa sahip misiniz? & working for the provision of services; Do you have a low level of commitment to relevant parties such as suppliers, internal groups in the supplier role, or customers? (-5) |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Kişisel Veri Depolama Alanı & Personal Data Storage** | Bulut & Cloud | Lokal Sunucu & Local Server | Hem Bulut Hem de Lokal Sunucu & Both cloud and local server | Taşeron Tarafından Yürütülüyor. & It's Run By A Subcontractor. |

NOT 2: ISO 27001 standardında hali hazırda belgeli firmaların ek olarak gözetim döngüsünden bağımsız 27701 talep etmeleri ve tetkikleri başarılı bir şekilde tamamlamaları durumunda hazırlanacak olan ISO 27701 sertifikası, ISO 27001 sertifikası geçerlilik tarihine uygun olarak düzenlenecektir. Gerçekleştirilecek olan ilk ISO 27001 ara tetkikinde bir yıl tamamlanmamış olmasına rağmen ISO 27701 tetkiki de gerçekleştirilecektir. & If companies already certified in the ISO 27001 standard additionally request 27701 independent of the surveillance cycle and complete the audits successfully, the ISO 27701 certificate to be prepared will be issued in accordance with the ISO 27001 certificate validity date. Although one year has not been completed in the first ISO 27001 interim audit, the ISO 27701 audit will also be carried out.

Aşağıda listelenmiş olan teknolojik alanlardan firmanizda kullanilanlari ve alt yapi gerekliliklerinden ve uygulamalardan kendi bünyenizde gerçekleştirdiklerinizi işaretleyiniz. Aşağidakilerden farkli bir teknolojik alan kullanma durumunuzda diğer bölümünü işaretleyerek teknolojik alan tanimini yapiniz.& Sıgn the followıng technologıcal fıelds used ın your company and your own realızatıon from the ınfrastructure requırements and applıcatıons. If you use a dıfferent technologıcal fıeld from the followıng, make the technologıcal fıeld descrıptıon by markıng the other sectıon

|  |  |
| --- | --- |
| **Teknolojik Alan Grubu Technological Area Group** | |
| Alt Yapı Background | **Ağ Yönetimi & Network Management**  Yerel ağlar & Local networks  Geniş alan ağları & Wide area networks  Kablosuz Ağ Teknolojileri & Wireless network technologies  İletişim Teknolojileri (mobil ağ, Karasal Ağ gibi) & Communication technologies (such as mobile network,Teressial network) |
| **Güvenlik Yönetimi Security Management**  Güvenlik Sistemleri (Firewall, proxy, IPS, IDS gibi) & Security Systems ( such as Firewall, proxy, IPS, IDS )  Log yönetimi & Log management  Kriptografi (SSL, VPN gibi) & Crytography (SSL, VPN )  Teknik Açıklık Analizi (kısıtlamalar, tarama testleri, penetrasyon testleri, zafiyet değerlendirmeleri) & Technical Vulnerability Analysis (restrictions, screening tests, penetration tests, vulnerability assessments) |
| **Sistem Yönetimi System Management**  Sunucular & Servers  Storage & Storage  Yedeklilik Sistemleri (load balancer gibi) & Redundancy Systems (load balancer)  Masaüstü yönetimi & Desktop management  Veri merkezleri (iklimlendirme, kesintisiz güç sistemleri gibi) & Data centers (such as air conditioning, uninterrupted power systems)  Sunucu işletim sistemleri & Server operating systems  Yedeklilik Sistemleri & Redundancy Systems  Sanallaştırma & Virtualization |
| Uygulama Temini & Implementation supply | Software Geliştirme & Software improvement  Özelleştirilmiş Yazılım Temini & Customized Software Supply  Paket Programlar & Package Programs |
| Uygulama Yönetimi & Implementation Management | Kurumsal Kaynak Planlama (ERP) & Enterprise Resource Planning (ERP)  Endüstriyel kontrol sistemleri & Industrial control systems  Doküman Yönetim Sistemi & Document Management System  Mobil uygulamalar & Mobile apps  Web tabanlı uygulamalar & Web based applications  Elektronik mesajlaşma & Electronic messaging  CRM  Elektronik Devre Tasarımları & Electronic Circuit Designs  Tasarım ve Modelleme uygulamaları (CAD-CAM) (Örneğin autocad, 3Dmax gibi) & Design and Modeling applications (CAD-CAM) (eg autocad, 3Dmax ) |
| Veri Yönetimi & Data Management | Veri tabanları sistemleri (oracle, ms sql, ibm db 2 gibi ) & Database systems (oracle, ms sql, ibm db 2 )  Veri yönetimi teknikleri (Büyük veri, veri madenciliği, İş zekası) & Data management techniques (Big data, data mining, Business intelligence) |
| Hizmet Yönetimi & Labor  Management | E-fatura & E-billing  E-arşiv & E-Archive  E-defter & E-Notebook  Elektronik Ticaret (Online ödeme sistemleri) & Electronic trade (Online payment systems)  IT Hizmet Yönetimi & IT service management  E-imza & E-Sıgnature |
| Diğer  Other | ………………………………………………….. |

|  |  |
| --- | --- |
| Firma Temsilcisi Adı / Soyadı / Unvan  **Company Representative Name / Surname / Tıtle** | Tarih / İmza / Kaşe  Date / Sıgnature / Stamp |