

Bilgi Güvenliđi Danışmanlığı

ISO/IEC 27001:2013 BİLGİ TEKNOLOJİSİ – GÜVENLİK TEKNİKLERİ – BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMLERİ – GEREKSİNİMLER STANDARDI KURULUMU DANIŞMANLIĐI

ISO 27001:2013 Standardı; bilgi güvenliđi yönetim sistemi'nin kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları ortaya koymak amacıyla hazırlanmıştır. Bilgi güvenliđi yönetim sisteminin benimsenmesi, kuruluş için stratejik bir karardır. Kuruluşun bilgi güvenliđi yönetim sisteminin kurulması ve uygulanmasında, kuruluşun ihtiyaç ve amaçları, güvenlik gereksinimleri, kullanılan kurumsal prosesler, kurumun boyutu ve yapısı etkilidir. Tüm bu etkileyen faktörlerin zaman içinde değışmesi beklenir.

Bilgi güvenliđi yönetim sistemi, bilginin gizliliđi, bütünlüğü ve erişilebilirliğini risk yönetimi prosesini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiđine dair güvence verir.

Danışmanlık hizmetimiz; kapsam çalışması, boşluk analizi, risk analizi, sistem dokümantasyonunun hazırlanması, uygunluk beyanının oluşturulması, bilgi güvenliđi farkındalık eğitimleri ve iç denetim adımlarının tümünü kapsamaktadır. Ayrıca sistemin iyileştirilmesine ve geliştirilmesine yönelik hizmetler de sağlanmaktadır. Kurumların bu hizmetlerin tümünden veya bir kısmından yararlanması, efor ve zamandan tasarruf ederek kısa sürede etkin bir BGYS kurması mümkün olmaktadır. Cymsoft Bilgi Güvenliđi Sistemi kurulumu aşamasında AR-GE ürünü olan SISMS yazılımı kullanarak zaman ve iş gücünden tasarruf sağlamaktadır. Danışmanlık hizmetimizin detayları için mikro sitemizi ziyaret edebilirsiniz.

BS10012 - KİŞİSEL BİLGİ YÖNETİM SİSTEMİ İÇİN VERİ KORUMA STANDARDI KURULUMU DANIŞMANLIĐI

Bu Uluslararası standardının hedefi kuruluşların, sürdürülebilir ve veri koruma mevzuatı ile uyumluluđu geliştiren bir altyapı sağlayan bir kişisel bilgi yönetim bilgi sistemini, tüm yönetim sisteminin bir parçası olarak ortaya koyabilmelerini sağlamaktır.

Bu Uluslararası Standard, veri koruma mevzuatı ile uyumluluđu ve iyi bir uygulamayı sürdürmek ve geliştirmek için alt yapıya sahip bir Kişisel Bilgi Yönetim Sistemi (KBYS)'nin gereksinimleri belirler.

Bu standart her ölçek ve sektördeki kuruluşların kullanımı içindir. Bir kuruluşta KBYS'ni başlatmaktan, sürdürmekten ve geliştirmekten sorumlu kişilerin kullanımını amaçlar. Kişisel bilginin yönetimi için yönetimde güven sağlayan, iç ve dış kullanıcılar için iyi bir uygulama ve veri koruma mevzuatı ile etkin bir uyumu oluşturan bir ortak yolu amaçlar.

ISO/IEC 27031 - BİLGİ TEKNOLOJİLERİ - GÜVENLİK TEKNİKLERİ - İŞ SÜREKLİLİĞİ İÇİN BİLGİ VE İLETİŞİM TEKNOLOJİLERİ HAZIRLIK PRENSİPLERİ STANDARDI KURULUMU DANIŞMANLIĞI

Bu Uluslararası Standart iş sürekliliği için bilgi ve iletişim teknolojileri (ICT) hazırlığının konsept ve prensiplerini belirlemekte ve iş sürekliliğini sağlamak için bir kuruluşun ICT hazırlığını geliştirmeye yönelik tüm koşulları (performans kriteri, tasarım ve uygulama gibi) tanımlamak ve belirlemek için ilgili süreçleri ve bir metot yapısını sağlamaktadır.

Standart güvenlik dâhil kritik iş fonksiyonlarının devamlılığını etkileyebilecek acil olayların, kazaların ve bağlantılı kesintilerin ortaya çıkması durumunda iş operasyonlarını desteklemek için ICT hizmetleri/altyapılarının hazır durumda bulunmasına gereksinim duyan ve iş sürekliliği için ICT hazırlık (IRBC) programını geliştiren herhangi bir kurum (özel, devlete ait, devlete ait olmayan, büyüklüğüne bakılmaksızın)'a uygulanabilmektedir.

ISO/IEC 27799 - SAĞLIK İNFORMATİĞİ - ISO/IEC 27002 KULLANILARAK SAĞLIKTA BİLGİ GÜVENLİĞİ YÖNETİMİ STANDARDI KURULUMU DANIŞMANLIĞI

Bu uluslararası standart sağlık bilgisinin güvenliğinden sorumlu olanlar, sağlık kuruluşları ve bu başlık altında bir rehber gereksinim duyan diğer sağlık bilgisi koruyanları (güvenlik danışmanları, denetçiler, satıcılar ve üçüncü taraf servis sağlayıcıları vb.) için ortaya konmuştur. Standart bilgi güvenliği yönetiminin pratik uygulamalarını belirleyen ISO/IEC 27002 standardının, sağlık çevrelerinde tutarlı bir şekilde ve sağlık sektörünün karşılaştığı güvenlik güçlüklerine karşı uygulanmasını sağlar. Kişisel sağlık bilgisinin gizliliği, bütünlüğü ve erişilebilirliğinin en iyi şekilde nasıl korunacağı konusunda tek rehberdir.

ISO/IEC 27011 - BİLGİ TEKNOLOJİLERİ-GÜVENLİK TEKNİKLERİ - TELEKOMÜNİKASYON KURULUŞLARI İÇİN ISO/IEC 27002 TABANLI BİLGİ GÜVENLİĞİ YÖNETİM REHBERİ KURULUMU DANIŞMANLIĞI

ISO/IEC 27011 Telekom Sektörüne özel olarak hazırlanmış güvenlik standardıdır. Bu uluslararası standard, telekom sektöründe yer alan kurumların, bilgi güvenliğinin en temel gereksinimleri olan “gizlilik”, “bütünlük” ve “erişilebilirlik” ilkelerini sağlayarak, ortak asgari düzeyde bir bilgi güvenliğine sahip olduklarını ispat etmelerine yardımcı olmak amacıyla oluşturulmuştur.

ISO/IEC 27011 standardı, ISO/IEC 27002 standardı baz alınarak, Telekom sektörüne özel bir Bilgi Güvenliği Yönetim Sistemi kurmak, gerçekleştirmek, sürdürmek ve geliştirmek için oluşturulmuş bir uygulama rehberidir.

ISO 27011 standardı ile neler sağlanmış olur?

- Telekomünikasyon kurumları için kabul edilmiş uluslararası hedeflere uygun bir bilgi güvenliği yönetim sisteminin oluşturulması,
- Telekomünikasyon araçlarının ve servislerinin gizliliği, bütünlüğü ve erişilebilirliği garanti altına alınarak, bilgi güvenliğinin sağlanması,

- Bilgi güvenliğine yönelik kapsamlı ve sistematik bir yönetim sisteminin benimsenmesi,
- Güvenli süreç ve kontroller ile telekomünikasyon hizmetlerindeki mevcut risklerin minimize edilmesi,
- Kullanıcıların telekom hizmetlerine güveninin artırılması ile kurumlar için rekabet avantajı.

ISO/IEC 27019 - BİLGİ TEKNOLOJİLERİ - GÜVENLİK TEKNİKLERİ – ENERJİ ALT YAPILARI İÇİN BİLGİ GÜVENLİĞİ YÖNETİM KURULUMU DANIŞMANLIĞI

ISO 27019:2013 standardı; bilgi güvenliği gereksinimlerinin enerji altyapıları başta olmak üzere kontrol sistemleri/otomasyon altyapıları uygulanabilir hale getirilmesini amaçlamaktadır. Bu alt yapılara örnek olarak elektrik üretimi, dağıtımı ve iletimi, doğalgaz iletimi işlemlerini gerçekleştiren endüstriyel kontrol sistemleri verilebilir. Bu altyapılara ilişkin bilgi güvenliği ihtiyaçları bilinen Bilgi Teknolojileri altyapılarından farklılık gösterebilmektedir.

24 Şubat 2017 tarihli ve 29989 sayılı Resmi Gazetede yayımlanan yönetmelik değişikliği ile “Elektrik Piyasası Lisans Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik” uyarınca kurulu gücü 100 MW ve üzerinde olan tesisler için ISO/IEC 27001 belgesinin yanında ISO/IEC TR 27019 rehber dokümanını da referans almaları zorunluluğu getirilmiştir. ISO IEC 27001 Bilgi Güvenliği Yönetim Sistemi standardına uyum zorunlu hale gelmiştir.