

Telekomünikasyon Kuruluşları için Bilgi Güvenliği Yönetim Sistemi Aracı (TABGYS)

Dünyada ve ülkemizde gün geçtikçe kullanımı yaygınlaşan ISO/IEC 27011 Bilgi teknolojileri – Güvenlik teknikleri – Telekomünikasyon Kuruluşları için ISO/IEC 27002 Tabanlı Bilgi Güvenliği Yönetimi Rehberi Standardı'nın zorunluluklarını yerine getirmek bilgi ve tecrübe ister. Danışmanlık hizmet maliyeti yüksektir. Bu nedenle yaygınlaşması zor olmaktadır. Ayrıca, süreçlerin karmaşıklığı nedeniyle danışmanlık alma veya uzman personel çalıştırma zorunlulukları vardır.

Cymsoft'un ISO/IEC 27011 Telekomünikasyon Kuruluşları için ISO/IEC 27002 Tabanlı Bilgi Güvenliği Yönetimi Sistemi'nin tesis edilmesindeki bilgi ve tecrübesinin somut göstergesi olan BGYS Aracı TUBİTAK AR-GE desteği ile gerçekleştirilen bir araçtır. ISO/IEC 27011'in tüm süreçlerinin kolaylıkla gerçekleştirilebilmesi amacıyla geliştirilmiş yapay zekâ tabanlı bir yazılımdır.

ISO/IEC 27011 Standardı'nın zorunluluklarını tümüyle karşılayarak standarda uyumluluğu sağlar.

Bilgi Güvenliği Yönetimi Sürecindeki;

- Kapsam,
- Bilgi Güvenliği Politikası,
- Varlık Envanteri,
- Risk Değerlendirme Metodolojisi,
- Risk Analizi,
- Risk Yönetimi,
- Mevcut Durum (GAP) Analizi,
- Zorunlu Prosedürler,
- Doküman Yönetimi
- Koruma Kontrolleri,
- Uyum İzleyici,
- Düzenleyici ve Önleyici Faaliyetlerin Takibi

Modüllerini kapsamaktadır.

Mevcut Durum (GAP) Analizi

- Kurumun ISO/IEC 27011 Bilgi Güvenliği Yönetim Sistemine uyumluluğunu belirlemek için Kontrol Maddeleri'nin nasıl uygulanacağını belirten ve ISO/IEC 27002 Standardında yer alan anlaşılması zor ve karmaşık kurallar yapısını, kullanılmasını ve anlaşılmasını kolay bir hale getiren test uygulaması,
- Test uygulamasının altyapısını teşkil eden ISO/IEC 27011 Kontrol Maddesi Yönetimi ve bu maddelere karşılık gelen uygulamalar için ISO/IEC 27002 Kural Yönetimi,
- ISO/IEC 27011 ve ISO/IEC 27002 Standartları gereksinimlerine göre güncellenebilir kural tabanı,
- Test sonucunda Standarda göre uyumluluk ve uyumsuzlukların dokümantasyonu,
- Test sonuçlarına göre ISO/IEC 27011 zorunlu prosedürlerinin otomatik dokümantasyonuna yönelik alt yapı hazırlanması,
- Kurumun Bilgi Güvenliği Yönetim Sistemine uyumluluğunun görsel olarak izlenmesini sağlayan "Olgunluk Seviyesi-Maturity Model" gösterimi,



TABGYS ile;

ISO/IEC 27000 Standart ailesinin anlaşılması zor ve karmaşık yapısı yapay zekâ uygulamaları ile kullanılması ve anlaşılması kolay bir hale getirilmiştir. BGYS kurulumunda Maliyet Düşürücü ve Standart/Kalite Yükseltici özelliğe sahiptir.

TABGYS'nin ayırt edici Özellikleri;

- Ağ üzerinde çalışan donanım varlıklarının tespit edilmesi ve elle varlık girişi yapılabilmesi,
- Varlıkların bir varlık grubu (üst varlık) altında toplanarak değerlendirilmesi,
- Varlıkların değerlerinin 3 farklı yöntemle hesaplanabilmesi,
- Dört adet niteliksel (Octave Allegro dahil) ve bir adet niceliksel olmak üzere beş farklı risk değerlendirme metodolojisi kullanabilme özelliği,
- Varlıkların türlerine göre (varlık grupları dahil) tehdit ve zafiyetlerinin ve risk değerlerinin otomatik belirlenmesi,
- Kendi varlık türlerini ekleyebilme,
- Sistem üzerinde tanımlanmış ve kategorilere ayrılmış güncellenebilir bilgi varlık türleri ve bunlarla ilişkilendirilmiş güncellenebilir tehditler ve zafiyetler,
- Varlıklara yönelik tehditlere göre korumaların otomatik belirlenmesi,
- Kendi korumalarını ekleyebilme ve tehditlerle ilişkilendirme,
- Varlık envanteri, risk değerlendirme raporu ve uygulanabilirlik bildirgesinin hazırlanması,
- Mevcut durum tespiti (GAP analizi) yapabilmesi,
- Standardının zorunlu dokümantasyonunun otomatik hazırlanması,
- Türkçe menü ve yardım,
- Farklı dil seçenekleriyle kullanabilme,
- Farklı yetki seviyelerinde kullanıcı rolleri belirleme,
- Kullanıcıları farklı yetki seviyelerindeki rollere atama ve LDAP (Aktif Dizin) ile bütünsel etkin Kullanıcı Yönetimi,
- Kurumsal unvan, sektör, logo, adres bilgileri, hiyerarşik kurum birimleri ve iş süreçleri tanımlama,
- İş süreçlerini varlıklar ve birimlerle ilişkilendirme,
- Tüm çalışanların kullanabileceği web tabanlı yazılım.
- Maliyet avantajı.



Varlık Envanteri

- Yerel alan ağına bağlı yazılım ve donanım varlıklarının envanterinin otomatik olarak çıkartılarak veri tabanına eklenmesi,
- Bilgi varlıklarının yerel ağ üzerinden tespit edilmesinin istenmediği durumlarda yazılıma uygun formattaki bir Excel tablosundan veri tabanına varlık envanteri aktarma,
- Yerel alan ağına bağlı olmayan bilgi varlıklarının varlık girişi ara yüzü yardımıyla veri tabanına girilmesi,
- Varlıkların birden fazla iş sürecine atanması veya iş süreçlerinin birden fazla varlıkla ilişkilendirilmesi,
- Aynı nitelikteki varlıkların tek bir grup altında toplanması ve yönetilmesi için varlık grubu tanımlama,
- Varlığın kategorisi, varlık grubu, bulunduğu yer, sorumlusu, varlık açıklaması, emanetçisinin takip edilebileceği ve süreçlerle ilişkilendirildiği bir ara yüz,
- Varlıkların gizlilik, bütünlük ve erişilebilirlik değerlerinin tek tek varlık bazında veya grup bazında en yüksek, toplam veya çarpım yöntemlerinden seçimlik olarak biriyle belirlenmesi,
- Varlıkların birim bazında sahipliğinin takibi, kategori ve süreç bazında listelenmesi,
- Varlık envanterinin detaylı dokümantasyonu,

Risk Yönetimi

- Varlıkların önceden belirlenen kategorilerine uygun zafiyet ve ilişkili tehditlerinin kullanıcı müdahalesi olmadan sistem tarafından otomatik olarak atanması,
- Zafiyet ve tehditlere karşı korumalar tanımlama,
- Niceliksel ve niteliksel olmak üzere beş risk değerlendirme metodolojisini dinamik olarak seçme imkânı;
 - ◆ ISO/IEC 27005 Risk Değerlendirme Metodu-1,
 - ◆ ISO/IEC 27005 Risk Değerlendirme Metodu-2,
 - ◆ Muhtemel Risk Değerlendirme Metodu,
 - ◆ Octave Allegro Risk Değerlendirme Metodu,
 - ◆ Niceliksel Risk Değerlendirme Metodu,
- Farklı Risk Değerlendirme Metodlarıyla; Varlık Değeri (Asset Value-AV), Açığa Çıkma faktörü (Exposure Factor-EF), Tek Kayıp Beklentisi (Single Loss Expectancy - SLE), Yıllık Olma Sıklığı (Annualized Rate of Occurrence -ARO), Yıllık Kayıp Beklentisi (Annualized Loss Expectancy - ALE) değerlerini dikkate alan risk analizi uygulaması,
- Seçilen risk değerlendirme metodolojisine uygun olarak risk analizi yapabileceği kolaylığı,
- ISO/IEC 27011'e uygun Risk Değerlendirme Raporu'nun Excel formatında dokümantasyonu.
- Kurumun Bilgi Varlıklarının kategorilerine göre risk durumlarını görsel olarak ifade eden "Risk Analizi Tablosu" gösterimi.



Koruma Kontrolleri

- Kurumun BGYS'nin zaman içerisinde daha iyi bir seviyeye çıkartılması için;
 - Mevcut Durum Analizi sonucu ortaya çıkan eksiklikler ile uyumsuzlukları listeleme,
 - Bu eksikliklerin ISO/IEC 27011 Standardının hangi kontrol maddesi ve ISO/IEC 27002 gereksinimleri ile giderilebileceğini belirleme.

Doküman Yönetimi

- Kullanıcı yetkilerine göre; doküman ekleme, çıkarma ve görüntüleme işlemleri,
- Dokümanların tarih esaslı versiyonlanarak saklanması, geçerli olan son versiyonunun web sayfası üzerinde yayınlanması,
- ISO/IEC 27011 belgelendirmesi için zorunlu olan aşağıdaki dokümantasyonun yazılım tarafından otomatik olarak üretilmesi, dokümanların sadece yönetici (Administrator) yetkisi verilen kullanıcılar tarafından değiştirilebilmesi,
- Hazırlanan dokümanların yayınlanması, kurum yerel portalinden erişilebilecek BGYS portalini üzerinden tüm yetkililerin kullanımına sunulması,
- Gereksinim duyulabilecek doküman şablonları,
- Yazılım aracılığı ile üretilen dokümantasyon;
 - ◆ Bilgi Güvenliği politikası,
 - ◆ BYGS Kapsam dokümanı,
 - ◆ BGYS'ni destekleyen kontrol ve prosedürler;
 - ✓ Risk Değerlendirme prosedürü,
 - ✓ BGYS Organizasyonu prosedürü,
 - ✓ İnsan Kaynakları prosedürü,
 - ✓ Varlık Yönetimi prosedürü,
 - ✓ Erişim Kontrolü prosedürü,
 - ✓ Fiziksel ve Çevresel Güvenlik prosedürü,
 - ✓ Haberleşme ve İşletim Güvenliği prosedürü,
 - ✓ Sistem Temini, Geliştirme ve Bakımı prosedürü,
 - ✓ Bilgi Güvenliği İhlal Yönetimi prosedürü,
 - ✓ İş sürekliliği Yönetiminin Bilgi Güvenliği Hususları prosedürü,
 - ✓ Uyum prosedürü,
 - ✓ İş Sürekliliği Planı,
 - ◆ Varlık Envanteri listesi,
 - ◆ Risk Analizi raporu,
 - ◆ Risk Değerlendirme raporu,
 - ◆ Uygulanabilirlik Beyannamesi,
 - ◆ BGYS faaliyetlerinin etkin işletilmesi ve gereksinimlere uygunluğunun kanıtı olan kayıtlar;
 - ✓ İç Denetim prosedürü,
 - ✓ Dokümanların ve Kayıtların Kontrolü prosedürü,
 - ✓ DÖF prosedürü,
 - ✓ Doküman listesi,
 - ✓ İç Denetim Soru listeleri,
 - ✓ Yönetimin Gözden Geçirme Toplantı Tutanağı taslağı.

Uyum İzleyici

- Bilgi Güvenliği Yönetim Sisteminin Planla, Uygula, Kontrol et ve Önlem Al süreçlerinin her birinde hazırlanması gereken dokümanların varlığını son versiyonlarını dikkate alarak kontrol ve takip etme.
- Üst yönetim için BGYS'nin izlenmesini sağlama

İç Denetim

Standart gereğince yılda asgari bir kez yapılması gereken iç denetimlere ait;

- Denetlenecek birimler,
- Denetçilerin seçimi,
- Denetim soru listelerini sistem üzerinden belirleme planlama ve takip etme,

Düzenleyici ve Önleyici Faaliyetlerin Takibi

- Açılan Düzenleyici ve Önleyici Formların (DÖF) Bilgi Güvenliği Yöneticisi tarafından uygun görülmesi, ilgili personele yönlendirilmesi, termin verilmesi, takibi ve kapatılmasını sağlama.
- DÖF'ların Yönetimin Gözden Geçirmesi tutanağında otomatik olarak özetlenmesi.