Bilgi Güvenliği Yönetim Sistemi Aracı (sBGYS)

Dünyada ve ülkemizde gün geçtikçe kullanımı yaygınlaşan ISO/IEC 27001:2017 Standardının 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.
Cyberverse'un ISO/IEC 27001:2017 Bilgi Güvenliği Yönetim Sistemi'nin tesis edilmesindeki bilgi ve tecrübesinin somut göstergesi olan BGYS Aracı TUBİTAK AR-GE desteği ile gerçekleştirilen bir araçtır.
ISO/IEC 27001'in tüm süreçlerinin kolaylıkla gerçekleştirilebilmesi amacıyla geliştirilmiş yapay zekâ tabanlı bir yazılımdır.
ISO/IEC 27001:2017 Standardının zorunluluklarını tümüyle karşılayarak standarda uyumluluğu sağlar.
Bilgi Güvenliği Yönetimi Sürecindeki;

- Kapsam,
- Bilgi Güvenliği Politikası,
- Varlık Envanteri (sDDO ile uyumlu),
- 5 farklı Risk Değerlendirme metodolojisi,
- Risk Analizi,
- Risk Yönetimi, Risk Değerlendirme Raporu,
- Mevcut Durum (GAP) Analizi
- Zorunlu Prosedürler,
- Doküman Yönetimi
- Koruma Kontrolleri
- Düzenleyici Faaliyetlerin Takibi
- Doküman Listesi,
- Yönetimin Gözden Geçirme Toplantı Tutanağı,
- Uygulanabilirlik Beyannamesi.
- Ve daha birçok kolaylıklar.

Modüllerini kapsamaktadır.

Mevcut Durum (GAP) Analizi

- Kurumun ISO/IEC 27001 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, kullanılması ve anlaşılmasını kolay bir hale getiren test uygulaması,
- Test uygulamasının altyapısını teşkil eden ISO/IEC 27001 Kontrol Maddesi Yönetimi ve bu maddelere karşılık gelen uygulamalar için ISO/IEC 27002 Kural Yönetimi,
- ISO/IEC 27001 ve ISO/IEC 27002 Standartları gereksinimlerine göre güncellenebilir kural tabanı,
- Test sonucunda Standarda göre uyumluluk ve uyumsuzlukların gösterimi ve ISO/IEC 27001 zorunlu prosedürlerinin otomatik dokümantasyonuna yönelik alt yapı hazırlanması,
- Kurumun Bilgi Güvenliği Yönetim Sistemine uyumluluğunun görsel olarak izlenmesini sağlayan "Olgunluk Seviyesi-Maturity Model" gösterimi,

sBGYS ile;

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

sBGYS'nin ayırt edici Özellikleri;

- Ağ üzerinde çalışan donanım varlıklarının tespit edilmesine yönelik üçüncü taraf yazılımlarla entegrasyon için API, Excel şablonu ve elle varlık girişi yapılabilmesi,
- Varlıkların bir varlık grubu (üst varlık) altında toplanarak değerlendirilmesi,
- Varlıkların değerlerinin Dört farklı yöntemle hesaplanabilmesi,
- Varlıkların türlerine göre (varlık grupları dahil) tehdit ve zafiyetlerinin ve risk değerlerinin otomatik belirlenmesi,
- Kendi varlık kategorilerini ekleyebilme,
- Sistem üzerinde tanımlanmış ve kategorilere ayrılmış güncellenebilir bilgi varlık türleri ve bunlarla ilişkilendirilmiş güncellenebilir tehditler ve zafiyetler,
- Varlıklara yönelik tehditlere göre korumaların 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 bütünleşik etkin Kullanıcı Yönetimi,
- Kurumsal unvan, sektör, logo, adres bilgileri, hiyerarşik kurum birimleri ve iş süreçleri tanımlama,
- İş süreçlerini varlıklar ve birimlerle ilişkilendirme,
- Kullanıcı dostu web tabanlı yazılım.

sBGYS Modülleri

Varlık Envanteri Modülü

- Varlıklarının envanterinin Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi varlık envanteri ile ortak kullanılabilmesi,
- Bilgi varlıklarının yazılım ile sunulan bir Excel şablonundan veri tabanına varlık envanteri aktarma veya 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 Modülü

- ISO/IEC 27005 : 2014 Information technology — Security techniques — Information security risk management standardına uygun olarak hazırlanan Risk Yönetimi Modülü ile ;
- 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
- Farklı Risk Değerlendirme Metotlarıyla; Varlık Değeri (Asset Value-AV), Açığa çıkma faktörü (Exposure Factor-EF), Tek kayıp beklentisi (Single Loss Expectancy - SLE), Yıllık olma sıklığı (Annualized Rate of Occurence –ARO), Yıllık kayıp beklentisi (Annualized Loss Expectancy - ALE) değerlerini dikkate alan risk analizi uygulaması,
- ISO/IEC 27001'e uygun Risk Değerlendirme Raporu'nun Excel formatında dokümantasyonu.

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 27001:2017 Standardının hangi kontrol maddesi ve ISO/IEC 27002:2013 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 27001 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 portali üzerinden tüm yetkililerin kullanımına sunulması,
- Gereksinim duyulabilecek doküman şablonları,
- Yazılım aracılığı ile üretilecek 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,
    - √ Kriptografi prosedürü,
    - √ Fiziksel ve çevresel güvenlik prosedürü,
    - √ İşletim güvenliği prosedürü,
    - √ Haberleşme güvenliği prosedürü,
    - √ Sistem temini, geliştirme ve bakımı prosedürü,
    - √ Tedarikçi ilişkileri prosedürü,
    - √ Bilgi güvenliği ihlal 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,
    - √ BGYS Organizasyonu Prosedürü,
    - √ Dokümanların ve Kayıtların Kontrolü Prosedürü,
    - √ DÖF Prosedürü,
    - √ Doküman listesi,
    - √ İç denetim soru listeleri,
    - √ Yönetimin gözden geçirme toplantı tutanağı taslağı,

İç Denetim Modülü

Guidelines for auditing management systems (ISO 19011:2018) Standına uygun olarak hazırlanmış iç denetim modülü ile;

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

Aksiyonların ve Düzenleyici Faaliyetlerin Takibi

- Açılan Aksiyonları ve Düzenleyici faaliyetlerin Bilgi Güvenliği Yöneticisi tarafından uygun görülmesi, ilgili personele yönlendirilmesi, termin verilmesi, takibi ve kapatılmasını sağlama.