KATEGORİ 1 · UYUM VE SÜRDÜRÜLEBİLİRLİK DANIŞMANLIKLARI

Bilgi Güvenliği Yönetim Sistemi (BGYS) Uyum Danışmanlığı ve İç Tetkik

ISO/IEC 27001

Kopyala-yapıştır şablon değil; kurumun iş süreçlerine, organizasyon yapısına ve risk iştahına göre tasarlanmış, belgelendirme denetiminde sıfır majör bulgu hedefleyen yaşayan bir BGYS mimarisi.

ISO 27001 danışmanlığı · BGYS kurulumu · Uygulanabilirlik Bildirgesi · SoA · bilgi varlıkları envanteri · ISO 27001 iç tetkik

KATEGORİ
Uyum ve Sürdürülebilirlik Danışmanlıkları

TİPİK SÜRE
Tipik program 4–8 ay (kapsam büyüklüğüne göre) · Yıllık iç tetkik döngüsü

KİMLER İÇİN
Kamu ihalelerine giren, kurumsal müşterilere hizmet veren veya regüle sektörlerde faaliyet gösteren tüm kuruluşlar; yazılım ve bulut hizmet sağlayıcıları, çağrı merkezleri, veri merkezleri ve MSSP'ler.

1 Hizmetin Tanımı

Bu hizmet, kurumunuzun bilgi varlıklarını korumak, siber riskleri sistematik olarak yönetmek ve uluslararası geçerliliğe sahip ISO/IEC 27001 standardına uyum sağlamak amacıyla tasarlanmış uçtan uca bir danışmanlık modelidir. Bu süreç, sadece kâğıt üzerinde kalan bir evrak çalışması değil; insan, süreç ve teknoloji sacayaklarını kurum kültürünüze entegre eden, yaşayan ve siber dayanıklılığınızı artıran bir yönetişim sisteminin kurulmasını kapsar.

2 Neden Gereklidir?

Siber saldırıların, veri ihlallerinin ve fidye yazılımı vakalarının hızla arttığı günümüzde bilgi varlıklarının korunması yalnızca teknik ekiplerin değil, tepe yönetimin asli sorumluluğudur. Bunun yanı sıra kamu ihalelerine katılım; KVKK, BİGR, BDDK, EPDK gibi regülatif mercilere uyum ve global markalarla iş ortaklıkları yapabilmek için ISO 27001 sertifikasyonu artık isteğe bağlı bir prestij değil, zorunlu bir ticari ve sözleşmesel kriter hâline gelmiştir.

YAPTIRIM VE RİSK EŞİĞİ
Doğrudan bir idari para cezası öngörülmemekle birlikte; sertifikasyon eksikliği kamu ihalelerinde elenme, kurumsal müşteri sözleşmelerinin feshi ve tedarikçi denetimlerinde "çalışılamaz" kararı gibi doğrudan ticari kayıplara yol açar.

3 Yasal ve Normatif Dayanak

ISO/IEC 27001 · ISO/IEC 27002 · ISO/IEC 27005 · Kamu ihale teknik şartnameleri · Müşteri ve tedarik zinciri sözleşme şartları

4 Sağladığı Katma Değer

Gerçekçi ve yaşayan sistem

İnternetten kopyala-yapıştır şablonlar yerine; kurumun iş süreçlerine, organizasyonel yapısına ve risk iştahına tam uygun, günlük operasyonları hantallaştırmayan dinamik bir BGYS mimarisi tasarlanır.

Entegre GRC yaklaşımı

ISO 27001'in Yüksek Seviye Yapısı (High-Level Structure) kullanılarak sisteminiz KVKK, BİGR, ISO 27701 ve ISO 9001 gibi diğer standartlarla aynı çatı altında birleştirilir; denetim yorgunluğu ve efor israfı önlenir.

Denetime tam hazırlık — sıfır uygunsuzluk hedefi

ISO 27001 Başdenetçisi yetkinliğine sahip uzmanlarımızca yapılan bağımsız iç tetkik simülasyonları sayesinde dış belgelendirme kuruluşlarının denetimlerinde majör bulgu riski ortadan kaldırılır.

5 Hizmet Kapsamı ve Metodoloji

AŞAMA 1

Mevcut Durum Analizi ve Kapsam Belirleme

Kurum organizasyonunun analiz edilmesi, BGYS sınırlarının net olarak çizilmesi ve standardın gereklilikleri ile mevcut durum arasındaki boşlukların (Gap Analysis) tespit edilmesi.

AŞAMA 2

Varlık ve Risk Yönetimi

Bilgi varlıklarının envanterinin çıkarılması, CIA ilkeleri doğrultusunda siber güvenlik risklerinin analiz edilmesi ve Risk İşleme Planının oluşturulması.

AŞAMA 3

Dokümantasyon ve Uygulama

Uygulanabilirlik Bildirgesi (SoA) temel alınarak; kurum kültürüne ve operasyonel işleyişine uygun BGYS politikalarının, prosedürlerinin, yönergelerinin ve form setlerinin uçtan uca / sıfırdan hazırlanması.

AŞAMA 4

Eğitim ve İşletim

Tüm çalışanlara yönelik bilgi güvenliği farkındalık eğitimleri, olay/ihlal yönetimi, iş sürekliliği tatbikatları ve teknik güvenlik kontrollerinin sahada hayata geçirilmesi.

AŞAMA 5

İç Tetkik ve YGG

Sistem performansının tarafsız ve bağımsız denetçilerimizce iç tetkik ile ölçülmesi, eksikliklerin DÖF ile kapatılması ve Yönetimi Gözden Geçirme toplantısına refakat edilmesi.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ Mevcut Durum (Gap) Analizi Raporu ve Proje Yol Haritası
- ✓ Detaylı Bilgi Varlıkları Envanteri ve BGYS Risk Değerlendirme / Risk İşleme Matrisi
- ✓ Uygulanabilirlik Bildirgesi (SoA — Statement of Applicability)
- ✓ Kuruma özel entegre BGYS dokümantasyon seti (politika, prosedür, talimat)

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Akredite belgelendirme kuruluşlarının ISO 27001 Aşama 1 ve Aşama 2 denetimlerinden sorunsuz geçilerek resmî sertifika edinilir.
- ✓ Bilgi güvenliği, yalnızca BT departmanının sorumluluğundaki teknik bir mesele olmaktan çıkıp tüm organizasyona yayılan sürdürülebilir bir yönetişim kültürüne dönüşür.

- ✓ Personel bilgi güvenliği farkındalık eğitim kayıtları ve sınav sonuçları
- ✓ Bağımsız iç tetkik raporu, DÖF kayıt formları ve YGG toplantı tutanakları
- ✓ Siber olaylara ve iş kesintilerine karşı reaktif kararlar yerine; önceden planlanmış, test edilmiş ve yasal merciler karşısında kanıtlanabilir bir güvenlik altyapısı kurulur.

7 Sık Sorulan Sorular

Belgeyi siz mi veriyorsunuz?

Hayır. Belgelendirme, akredite bir belgelendirme kuruluşunun yetkisindedir. Biz sistemi kurar, iç tetkiki bağımsız olarak yürütür ve Aşama 1–2 denetimlerine refakat ederiz. Bu ayrım, standardın tarafsızlık gereğidir.

Ne kadar doküman üretiliyor?

Doküman sayısı bir başarı ölçütü değildir. Kapsam ve SoA kararlarına göre işletilebilir en yalın set hedeflenir; amaç, operasyonu yavaşlatmayan ve gerçekten kullanılan bir yapı kurmaktır.

Mevcut KVKK çalışmamızla birleştirilebilir mi?

Evet. Ortak varlık envanteri, ortak risk metodolojisi ve ortak politika iskeleti üzerinden birleştirme yapılır; bu, iki ayrı proje maliyetini tek bir programa indirir.

8 Etiketler

ISO 27001 danışmanlığı · BGYS kurulumu · Uygulanabilirlik Bildirgesi · SoA · bilgi varlıkları envanteri · ISO 27001 iç tetkik · risk işleme planı · belgelendirme denetimi hazırlığı

Bu hizmet, tam hizmet kataloğunun bir parçasıdır. Diğer 11 hizmet ve bütüncül paketler hakkında bilgi için Genel Broşür'e başvurabilirsiniz. Bu doküman bilgilendirme amaçlıdır; hukuki mütalaa veya taahhüt niteliği taşımaz.