KATEGORİ 2 · BÜTÜNCÜL PAKETLER

Kurumsal Olgunluk, GRC ve Siber Dayanıklılık Programı

12 Ay

KVKK, ISO 27001/27701/42001 ve 7545 sayılı Kanun yükümlülüklerini tek yönetişim şemsiyesinde birleştiren; GRC ile teknik güvenceyi (sızma testi, tehdit avcılığı, SOME desteği) aynı programda buluşturan 12 aylık bütünleşik model.

GRC danışmanlığı | kurumsal olgunluk programı | siber dayanıklılık | entegre yönetim sistemi | KPI KRI | tehdit avcılığı

KATEGORİ
Bütüncül Paketler

TİPİK SÜRE
12 ay · Aylık ilerleme raporlaması · Yenilenebilir

KİMLER İÇİN
Birden fazla regülasyona aynı anda tabi olan orta ve büyük ölçekli kuruluşlar, holdingler, grup şirketleri ve hızlı büyüyen teknoloji şirketleri.

1 Hizmetin Tanımı

Bu hizmet; KVKK, ISO 27001, ISO 27701, ISO 42001, 7545 sayılı Siber Güvenlik Kanunu ve Siber Güvenlik Başkanlığı mevzuatlarına uyum sağlanması, bilgi güvenliği altyapısının uluslararası standartlara uygun tesis edilmesi ve siber olaylara karşı teknik dayanıklılığın artırılması amacıyla tasarlanmış 12 ay süreli bütünleşik bir stratejik danışmanlık ve yönetişim modelidir. Reaktif süreçler yerine riskleri önceden öngören, operasyonel sürekliliği güvence altına alan ve 12 ayın sonunda kurum içi kaynaklarla sürdürülebilir bir ekosistem yaratan proaktif bir çözüm ortaklığıdır.

2 Neden Gereklidir?

Günümüz tehdit ortamında GRC ile teknik siber güvenliğin birbirinden bağımsız yapılar olarak ele alınması, kurumlarda operasyonel güvenlik zafiyetlerine ve izlenebilirlik eksikliklerine yol açmaktadır. KVKK, ISO standartları, 7545 sayılı Kanun ve Siber Güvenlik Başkanlığı regülasyonları gibi birbirinden farklı gereksinimler süreç karmaşasına, bütçe israfına ve efor mükerrerliğine neden olmaktadır. Bu yapıyı bütüncül bir yaklaşımla konsolide etmek, stratejik bir komite kültürü oluşturmak ve krizlerde uzman yönlendirmesine sahip olmak kaçınılmazdır.

YAPTIRIM VE RİSK EŞİĞİ
Program, 7545 sayılı Kanun'un 1.000.000 ₺ – 10.000.000 ₺ ve KVKK'nın 17.092.242 ₺'ye ulaşan idari para cezası bantlarının tamamına karşı tek seferde kapsamlı bir savunma hattı kurar.

3 Yasal ve Normatif Dayanak

7545 sayılı Siber Güvenlik Kanunu | 6698 sayılı KVKK | ISO/IEC 27001 | ISO/IEC 27701 | ISO/IEC 42001 | Siber Güvenlik Başkanlığı düzenlemeleri

4 Sağladığı Katma Değer

Maliyet ve efor optimizasyonu

KVKK, ISO standartları ve yasal regülasyonlar merkezi bir yönetim yapısında birleştirilir; tekil varlık envanteri ve konsolide risk kütükleri oluşturularak farklı birimlerin mükerrer efor harcaması ve aynı süreçler için çoklu bütçe tahsis edilmesi önlenir.

Sinerjik değer üretimi

Sızma testleri ve zafiyet taramalarıyla elde edilen teknik bulgular, doğrudan iş süreçleri ve kurumsal risk analizleri ile entegre edilerek teorik politikaların sahadaki etkinliği doğrulanır.

İş hedefleriyle hizalanma ve yönetsel vizyon

Siber güvenlik süreçleri, GRC yönlendirme komitelerinin teşkiliyle stratejik bir bileşen olarak konumlandırılır; güvenlik yatırımları şeffaf KPI/KRI metrikleri üzerinden izlenebilir hâle gelir.

Proaktif güvenlik yaklaşımına geçiş

Geleneksel çevre güvenliğinin ötesinde; Sıfır Güven mimarisi, tehdit avcılığı, SOME desteği ve siber tatbikatlarla altyapı sürekli hazır durumda tutulur.

5 Hizmet Kapsamı ve Metodoloji

Genel bakış: TEK ÇATI Kurumsal GRC ve Siber Dayanıklılık Programı KVKK ISO 27001 ISO 27701 ISO 42001 7545 s. Kanun Teknik Güvence SONUÇ Tekil varlık envanteri · konsolide risk kütüğü · ortak politika seti · tek KPI panosu

BLOK 1

Kurumsal Olgunluk ve GRC Paketi

Ulusal Siber Güvenlik Mevzuatı (7545 sayılı Kanun) uyum düzeyi değerlendirmesi ve etki analizi. ISO 27001, ISO 42001 ve KVKK gereksinimlerini karşılayan bütünleşik politika/prosedür setinin tasarımı. GRC/BG/KVKK komitesi kurulumuna metodolojik rehberlik ve operasyonel KPI/KRI tanımlanması. Temel varlık/süreç envanteri ve yerleşik/bulut sistemleri kapsayan bütünleşik risk analizi metodolojisinin işletilmesi. ISO 42001 YZ Yönetim Sistemi danışmanlığı. İç/dış denetim hazırlığı ve tedarikçi zinciri güvenlik denetimleri. İş Sürekliliği (BCP/DRP) çerçevesinin tasarımı, düzeltici faaliyet mimari desteği ve GRC yazılım seçimi danışmanlığı. Siber güvenlik farkındalık programı ve ihlal vakaları için kök neden analizleri.

BLOK 2

Siber Dayanıklılık ve Teknik Güvence Paketi

Genişletilmiş Black/Grey-Box sızma testi (web, mobil uygulama, API servisleri, dış/iç ağ). Olası kriz anlarında SOME ekiplerine aktif müdahale desteği (SLA dâhilinde olay yeri inceleme, izole etme, adli bilişim). Yeni nesil güvenlik mimarisi (Zero Trust, IAM, SOC use-case senaryoları) ve loglama danışmanlığı. Dağıtık yapılar için "Güvenli Lokasyon BT Güvenlik Standardı" tasarımı. Güvenlik teknolojilerinin test ve entegrasyon (health-check/baseline) incelemesi. Sosyal mühendislik testleri, 50 kritik uç noktada kanıt/iz analizi ve tehdit avcılığı (Compromise Assessment). Masa başı siber tatbikat kriz yönetimi moderasyonu.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ Kurumsal Mevcut Durum Raporu, Risk Analizi ve önceliklendirilmiş iyileştirme planı
- ✓ GRC Komite Yapısı Dokümanı (RACI matrisi dâhil) ve bütünleşik bilgi güvenliği politika/prosedür seti
- ✓ İş Sürekliliği (BCP) ve Felaket Kurtarma (DRP) çerçeve dokümanı
- ✓ İç denetim raporları ve tedarikçi güvenlik denetim raporu
- ✓ Genişletilmiş sızma testi ve güvenlik teknolojileri değerlendirme raporları
- ✓ Sosyal mühendislik, farkındalık ve siber tatbikat raporları

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Kurumsal operasyonlar; KVKK, ISO standartları ve 7545 sayılı Kanun gibi regülatif yükümlülüklerle tam uyumlu ve operasyonel esnekliği sağlayan bir yönetişim şemsiyesi altına alınır.
- ✓ Geleneksel BT eksikliklerinin ötesine geçen, siber tehditleri proaktif olarak izleyen ve açıkları operasyonel süreçlerine entegre ederek kapatabilen dirençli bir yapı kurulur.
- ✓ Yatırımlar mükerrer regülasyon eforlarından ve çakışan güvenlik teknolojilerinden kurtarılarak; şeffaf KPI'larla izlenen ve kurum içi kaynaklarla sürdürülebilen bütüncül bir ekosisteme dönüştürülür.

- ✓ Yönetici özeti formatında aylık ilerleme raporları ve kapanış değerlendirmesi

7 Sık Sorulan Sorular

Neden 12 ay?

Yönetişim yapısının kurulması, risklerin işlenmesi, teknik testlerin bulgularının kapatılması ve bir tam denetim döngüsünün tamamlanması için gereken asgari süre budur. Daha kısa programlar dokümantasyon üretir, kültür üretmez.

Var olan ekibimizin yerini mi alıyorsunuz?

Hayır. Program, know-how transferi esasına dayanır; 12 ayın sonunda sistemin kurum içi kaynaklarla sürdürülebilmesi açık hedeftir.

Blokları ayrı ayrı alabilir miyiz?

Alınabilir; ancak paketin asıl değeri, teknik bulguların doğrudan risk kütüğüne ve yönetim raporlamasına akmasından doğar. Ayrıştırma bu sinerjiyi zayıflatır.

8 Etiketler

GRC danışmanlığı · kurumsal olgunluk programı · siber dayanıklılık · entegre yönetim sistemi · KPI KRI · tehdit avcılığı · compromise assessment · masa başı tatbikat · Zero Trust

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.