KATEGORİ 3 · DENETİM HİZMETLERİ

Bilgi ve İletişim Güvenliği Rehberi (BİGR) Uyum Denetim Hizmeti

TSE Yetkili

Siber Güvenlik Başkanlığı'nın Denetim Rehberi metodolojisine tam uyumlu, TSE yetkili firma ve BİGR D1/D2 başdenetçileri tarafından yürütülen, BİGDES'e yüklenmeye hazır resmî denetim dosyası üreten bağımsız denetim.

BİGR denetimi · TSE yetkili denetim firması · BİGR başdenetçi · BİGDES raporlama · Ek-A Ek-H formları · tasarım ve işletim etkinliği

KATEGORİ
Denetim Hizmetleri

TİPİK SÜRE
Kapsam büyüklüğüne göre 3–8 hafta · Yılda en az bir kez tekrarlanır

KİMLER İÇİN
BİGR kapsamındaki tüm kamu kurum ve kuruluşları ile kritik altyapı işletmecileri; yıllık denetim yükümlülüğü doğmuş her kurum.

1 Hizmetin Tanımı

Bu hizmet, Siber Güvenlik Başkanlığı tarafından yayımlanan "Bilgi ve İletişim Güvenliği Denetim Rehberi" metodolojisine tam uyumlu olarak; kamu kurumları ve kritik altyapı işletmecilerinin BİGR uyum süreçlerinin bağımsız, tarafsız ve kanıta dayalı olarak incelenmesi faaliyetidir. TSE tarafından "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Firma" olarak yetkilendirilmiş; BİGR D1/D2 Başdenetçi ve ISO 27001 Başdenetçi sertifikalarına sahip uzman kadromuz tarafından yürütülen denetim, kurumunuzun güvenlik tedbirlerinin tasarım ve işletim etkinliğini test ederek resmî makamlara makul güvence sunmayı amaçlar.

2 Neden Gereklidir?

Cumhurbaşkanlığı Genelgesi ve Siber Güvenlik Başkanlığı regülasyonları uyarınca, BİGR kapsamındaki kurum ve kuruluşların uyum uygulamalarını yılda en az bir defa denetlemesi ve sonuçlarını resmî formatta (Ek-A'dan Ek-H'ye kadar olan formlar) Başkanlığa iletmesi yasal bir zorunluluktur. Bu denetimler; millî güvenliği tehdit edebilecek verilerin korunması, kurumun siber dayanıklılığının ölçülmesi ve mevcut kontrollerin gerçekten işe yarayıp yaramadığının bağımsız bir gözle kanıtlanması için kritik öneme sahiptir.

YAPTIRIM VE RİSK EŞİĞİ

Yıllık denetim yükümlülüğünün yerine getirilmemesi ve BİGDES bildirimlerinin eksik/gecikmeli yapılması 7545 sayılı Kanun kapsamında idari para cezasına konudur; denetim yükümlülüklerine aykırılıkta 100.000 ₺ – 1.000.000 ₺, ticari şirketlerde brüt satış hasılatının %5'ine kadar ceza uygulanabilir.

3 Yasal ve Normatif Dayanak

- Bilgi ve İletişim Güvenliği Denetim Rehberi
- 7545 sayılı Siber Güvenlik Kanunu
- 2019/12 sayılı Cumhurbaşkanlığı Genelgesi
- TSE yetkilendirme kriterleri

4 Sağladığı Katma Değer

Resmî metodoloji ile tam uyum

Siber Güvenlik Başkanlığı'nın zorunlu tuttuğu Denetim Rehberi'ndeki 3 ana süreç (Planlama, Uygulama, Raporlama) harfiyen işletilir. Raporun reddedilme veya eksik bulunma riski sıfıra indirilir.

Kanıta dayalı ve objektif değerlendirme

Güvenlik kontrolleri sadece kâğıt üzerinde değil; mülakat, gözden geçirme, güvenlik denetimi, sızma testi ve kaynak kod analizi gibi yöntemlerle ve istatistiki örneklem (sampling) kurallarına uygun olarak sahada doğrulanır.

Tasarım ve işletim etkinliğinin ölçülmesi

Bir güvenlik kuralının sadece yazılıp yazılmadığı (tasarım etkinliği) değil, sahada fiilen uygulanıp uygulanmadığı (işletim etkinliği) test edilerek kuruma gerçekçi bir güvenlik fotoğrafı sunulur.

Uluslararası bağımsızlık ve etik ilkeler

Denetim, daha önce kuruma danışmanlık vermemiş; tarafsızlık ve gizlilik taahhütnameleriyle sürece dâhil olan yetkili denetçilerle, görevler ayrılığı (segregation of duties) prensibiyle yürütülür.

5 Hizmet Kapsamı ve Metodoloji

AŞAMA 1

Denetimin Planlanması ve Kapsamın Belirlenmesi

Kurumun iş süreçlerinin anlaşılması; ağ, sistem, uygulama, IoT ve personel gibi varlık gruplarının önemlilik ve risk kriterlerine (Delfi metodu vb.) göre incelenmesi. Resmî şablonlara uygun denetim ekibi (Ek-A) ve denetim kapsamının (Ek-B) atanması.

AŞAMA 2

Rehber Uygulama Süreci Etkinliğinin Denetlenmesi

Kurumun BİGR uyumu için yaptığı hazırlıkların (varlık gruplandırmalarının doğruluğu, kritiklik anketlerinin uygunluğu, telafi edici kontrollerin dokümantasyonu ve yol haritasının ilerleyişi) metodolojik olarak incelenmesi ve Ek-E formuna işlenmesi.

AŞAMA 3

Tedbirlerin Etkinliğinin Değerlendirilmesi (Saha Çalışması)

Seçilen örneklemler üzerinden teknik ve idari kontrollerin test edilmesi. Güvenlik duvarı kurallarından fiziksel sunucu odalarına ve sızma testi sonuçlarına kadar kontrollerin "Etkin, Kısmen Etkin, Etkin Değil" olarak değerlendirilmesi ve Ek-F formuna işlenmesi.

AŞAMA 4

Bulguların Tespiti ve Derecelendirilmesi

Tespit edilen idari veya teknik eksikliklerin kurumdaki risk etkisine göre (Çok Yüksek, Yüksek, Orta, Düşük) resmî etiketleme standartlarıyla (örn. U01, T04) sınıflandırılması ve kök nedenlerinin belirlenmesi.

6 Teslimatlar, Çıktılar ve Başarı Kriterleri

TESLİMATLAR VE ÇIKTILAR

- ✓ BİGR Resmî Denetim Raporu — yönetici özeti, kapsam, metodoloji ve makul güvence beyanını içeren imzalı ana rapor
- ✓ Denetim Ekibi Bilgisi (Ek-A) ve Varlık Grupları / Kapsam Dosyası (Ek-B)
- ✓ Rehber Uygulama Süreci (Ek-E) ve Tedbir Etkinlik (Ek-F) durum raporları
- ✓ Resmî Bulgu Tablosu (Ek-G) — yasal etiketleme formatıyla kodlanmış uygunsuzluk listesi
- ✓ İmzalı Denetim Görüşü (Ek-H) — denetim ekibi ve kurum üst yöneticisi tarafından imzalanan kapanış tutanağı

HEDEFLENEN ÇIKTI / BAŞARI KRİTERİ

- ✓ Siber Güvenlik Başkanlığı'nın zorunlu kıldığı yıllık bağımsız BİGR denetim yükümlülüğü, yetkili bir kurum aracılığıyla ve tüm yasal format (Ek-A/H) beklentileri karşılanarak eksiksiz yerine getirilir.
- ✓ Kâğıt üzerindeki uyum çalışmalarının işletim düzeyinde ne kadar etkili olduğu somut kanıtlarla (sızma testi, konfigürasyon analizi, mülakat) doğrulanır.
- ✓ Zayıf halkalar ve "Çok Yüksek/Yüksek" riskli bulgular resmî bir raporla kayıt altına alınarak, sonraki yıl yatırımları için üst yönetime net bir DÖF yol haritası sunulur.

- ✓ Bütünlüğü hash değeri ile korunmuş, BİGDES'e yüklenmeye hazır resmî denetim dosyası

7 Sık Sorulan Sorular

Danışmanlığımızı da siz yaptınız, denetimi de yapabilir misiniz?

Hayır. Denetim Rehberi ve uluslararası denetim etiği, aynı kuruma hem danışmanlık hem denetim verilmesini yasaklar. Bu ayrımı korumak, raporun geçerliliğinin ön şartıdır.

Denetim kaç gün sürer?

Süre; varlık grubu sayısına, kritiklik derecelerine ve lokasyon sayısına göre belirlenir. Örneklem büyüklüğü istatistiki kurallara göre hesaplanır, keyfî olarak daraltılamaz.

Bulgular çıkarsa denetimden kalmış mı oluruz?

Denetim bir sınav değil, bir tespit sürecidir. Bulguların varlığı beklenen bir durumdur; önemli olan bunların derecelendirilmesi ve DÖF planına bağlanmasıdır.

8 Etiketler

BİGR denetimi · TSE yetkili denetim firması · BİGR başdenetçi · BİGDES raporlama · Ek-A Ek-H formları · tasarım ve işletim etkinliği · örnekleme sampling · makul güvence

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.