

EK – H: DENETİM GÖRÜŞÜ

Örnek Anonim Şirketine:

6 Temmuz 2019 tarihinde yayımlanarak yürürlüğe giren Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi uyarınca yayımlanan Bilgi ve İletişim Güvenliği Rehberi'nin 1.0 sürümüne yönelik uyum denetimlerini gerçekleştirmek üzere sayılı ve tarihli resmi yazı ile görevlendirilmiş bulunuyoruz.

Örnek Anonim Şirketi Yönetimi, Bilgi ve İletişim Güvenliği Rehberi'nde yer verilen usul ve esaslar çerçevesindeki uygulama sürecini ve varlık gruplarına uygulanması gereken tedbirleri yerine getirmekle sorumludur.

Bilgi ve İletişim Güvenliği Rehberi uyum denetimini gerçekleştiren denetim ekibi olarak sorumluluğumuz, gerçekleştirdiğimiz denetim çalışmalarına istinaden Rehber uygulama sürecinin ve varlık gruplarına uygulanan tedbirlerin etkinliğine yönelik görüş bildirmektir.

Denetim çalışmaları, Bilgi ve İletişim Güvenliği Denetim Rehberi'nde yer alan usul ve esaslara uygun olarak planlanmış, Bilgi ve İletişim Güvenliği Rehberi uygulama sürecinin ve varlık gruplarına uygulanması gereken tedbirlerin etkinliğini ölçmeye makul güvence sağlayacak şekilde yürütülmüştür. Denetim çalışmaları Örnek Anonim Şirketinin sunduğu bilgi, belge, yazılı ve sözlü beyanlar çerçevesinde Bilgi ve İletişim Güvenliği Denetim Rehberi'nde yer alan denetim yöntemleri ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Yapılan denetimde, tedbirlerin yerine getirilmesi amacıyla uygulanan kontrollerin doğasında bulunan kısıtlar nedeniyle eksikliklerin tespit edilememe riski bulunmaktadır. Bunlarla birlikte, Örnek Anonim Şirketi bilgi sistemleri yapısının veya mevcut şartların değişmesi durumunda bulguların ve bulgularla ilişkili risklerin değişikliğe uğrama olasılığı vardır.

Gerçekleştirilen denetim çalışmaları sonucunda topladığımız kanıtlar ve elde ettiğimiz bulgular neticesinde:

Bilgi ve İletişim Güvenliği Rehberi uygulama sürecinde:

- a) Kurum varlık gruplarının, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanma durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."
- b) Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanma durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."
- c) Varlık grupları tanımlama çalışmalarının varsa bilgi güvenliği yönetim sistemi kapsamında oluşturulan varlık envanteri ile ilişkilendirilme durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."
- ç) Varlık grupları kritiklik derecelerinin Rehberde uygun olarak belirlenme durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."
- d) Varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."

- e) Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirlerinin varlık grubu ile uygun bir şekilde eşleştirilmesi “kısmen gerçekleştirilmiştir”, “**tamamen gerçekleştirilmiştir**”, “hiç gerçekleştirilmemiştir.”
- f) Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması “kısmen gerçekleştirilmiştir”, “**tamamen gerçekleştirilmiştir**”, “hiç gerçekleştirilmemiştir.”
- g) Telafi edici kontrollerin dokümanite edilmesi “**kısmen gerçekleştirilmiştir**”, “tamamen gerçekleştirilmiştir”, “hiç gerçekleştirilmemiştir.”
- ğ) Rehber uygulama yol haritasının oluşturulma durumu “kısmen gerçekleştirilmiştir”, “**tamamen gerçekleştirilmiştir**”, “hiç gerçekleştirilmemiştir.”

Denetim kapsamındaki varlık gruplarına Bilgi ve İletişim Güvenliği Rehberi’nde yer alan tedbirlerden uygulanması gerekenlerin etkinlik durumu aşağıdaki tabloda yer almaktadır.

Varlık Grubu Ana Başlığı No (3.1., 3.2., 3.3., 3.4., 3.5., 3.6.)	Varlık Grubu No	Uygulanması Gereken Toplam Tedbir Sayısı	Tedbirlerin Etkinlik Durumu		
			Etkin Olan Tedbir Sayısı	Etkin Olmayan Tedbir Sayısı	Kısmen Etkin Tedbir Sayısı
3.1	V1				
3.1	V2				
3.2	V3				
3.3	V4				
3.4	V5				
3.5	V6				
3.6	V7				

Düzenlenme Yeri ve Tarihi: **Örnek A.Ş. Çankaya Yerleşkesi Merkez Bina /**

Denetim Koordinatörü:

Denetçi (ler)

İmza:

İmza: