Türkiye Cumhuriyeti Cumhurba?kanl??? Dijital Dönü?üm Ofisi, Bilgi ve ?leti?im Güvenli?i Denetim Rehberi'ni Yay?mlad?

24 Ara 2021

6 Temmuz 2019 tarihinde yay?mlanarak yürürlü?e giren Bilgi ve ?leti?im Güvenli?i Tedbirleri konulu Cumhurba?kanl??? Genelgesi uyar?nca, kamu kurumlar? ve kritik altyap? hizmeti veren i?letmeler, kar??la??lan güvenlik risklerinin azalt?lmas?, etkisiz k?l?nmas? ve özellikle gizlili?i, bütünlü?ü veya eri?ilebilirli?i bozuldu?unda milli güvenli?i tehdit edebilecek veya kamu düzeninin bozulmas?na yol açabilecek kritik türdeki verilerin güvenli?inin sa?lanmas? amac?yla belirli güvenlik tedbirlerini uygulamakla yükümlü k?l?nm??t?.

Bu do?rultuda, 27 Temmuz 2020 tarihinde Türkiye Cumhuriyeti Cumhurba?kanl??? Dijital Dönü?üm Ofisi taraf?ndan farkl? güvenlik seviyelerinde tedbirler içeren Bilgi ve ?leti?im Güvenli?i Rehberi ("**Rehber**") yay?mlanm??t?r. Kurumlar?n Rehber'e uyum sa?larken yerine getirmesi gereken ad?mlardan biri olan denetim süreci de Rehber ile düzenlenmektedir.

Rehber kapsam?nda yer alan kurumlar?n belirli çal??malar? yerine getirmeleri beklenmektedir. Bu çal??malar?n; planlama, uygulama, de?i?iklikleri yönetme, kontrol etme ve önlem alma süreçlerini içeren bir çerçevede yürütülmesi gerekmektedir. Kontrol etme ve önlem alma sürecinin bir parças? olan denetimin y?lda en az bir kez gerçekle?tirilmesi amac?yla kurumlar taraf?ndan gerekli planlamalar yap?lmas? ve i?letilmesi öngörülmü?tür.

27 Ekim 2021 tarihinde ise, denetimin ba??ms?z bir ?ekilde planlanmas?, yürütülmesi ve raporlanmas? konular?nda kurumlara ve denetçilere yol göstermek amac?yla Bilgi ve ?leti?im Güvenli?i Denetim Rehberi ("**Denetim Rehberi**") haz?rlanm??t?r.

Denetim Rehberi ile;

- Kurumlara Rehber'in yay?m tarihi olan 27 Temmuz 2020 itibar?yla 24 ayl?k bir uyum süresi verilmi?tir. ?lk y?l denetimlerinde kurumlar denetim faaliyetleri ile ilgili haz?rl?k çal??malar?na en geç 24 ayl?k sürenin sonunda ba?lamal?d?r. Ancak uyum çal??malar?n? 24 aydan önce tamamlayan kurumlara denetim faaliyetleri için gerekli haz?rl?k çal??malar?na uyum süresinin dolmas?n? beklemeden ba?layabilme imkan? tan?nm??t?r.
- Rehber kapsam?ndaki tüm kurumlarda, denetim faaliyetlerinin öncelikli olarak iç denetim birimlerinde görev alan ve bilgi teknolojileri alan?nda denetim yapmak üzere görevlendirilen iç denetçiler taraf?ndan gerçekle?tirilmesi esast?r. Kritik altyap? hizmeti veren i?letmelerde, düzenleyici ve denetleyici kurumlar ilgili mevzuatlar? çerçevesinde bu Denetim Rehberi'ne uygun ?ekilde ayr?ca denetim faaliyetleri gerçekle?tirebilir.
- ?ç denetim birimlerinin bulunmad??? ya da iç denetim birimi olmas?na ra?men denetimi yürütecek yeterlik ve yetkinlikte denetçiye sahip olunmad??? hâllerde denetim faaliyetlerinin ba??ms?z bir ?ekilde yürütülmesini sa?lamak üzere kurum içi di?er personel, di?er kamu kurum ve kurulu?lar?ndan görevlendirilecek personel veya hizmet al?m? yolu ile denetim faaliyeti gerçekle?tirilebilir.
- Kurumun halihaz?rda uymakla yükümlü oldu?u mevzuat do?rultusunda ISO/IEC 27001 uyumlu Bilgi Güvenli?i Yönetim Sistemi ("**BGYS**") kurulum, i?letim ve belgelendirme yükümlülü?ünün bulunmas? ve bu yükümlülük çerçevesinde BGYS kapsam? ile Denetim Rehberi uyum kapsam?n?n ayn? olmas? durumunda, BGYS iç tetkik çal??malar? ile Denetim Rehberi uyum denetimleri tek bir denetim alt?nda yürütülebilir. Ancak denetim çal??malar? sonucunda Türkiye Cumhuriyeti Cumhurba?kanl??? Dijital Dönü?üm Ofisi iletilmesi gereken bilgi ve belgeler bu dokümanda tan?ml? formatlara uygun olarak

olu?turulmal?d?r. Bu ?ekilde gerçekle?tirilecek denetimlerde https://cbddo.gov.tr/ adresinde yay?mlanacak tedbir e?le?tirme tablolar?ndan faydalan?labilir.

- Kurum ile firma ve denetçiler için denetim hizmet al?m sözle?mesinde uyulmas? gereken asgari yükümlülükler a?a??daki gibidir:
- Denetim hizmetini, Belgelendirme Program? kapsam?nda yetkilendirilmi? firmalardan almak.
- Denetim hizmeti al?nacak firmadan art arda üçten fazla denetim hizmeti almam?? olmak.
- Sözle?mede denetimin amac?na, kapsam?na ve sözle?menin feshine ili?kin ?artlara yer vermek.
- Kurumun bilgi güvenli?i gereksinimlerine uygun olarak Denetim Rehberi'nde yer alan "Tedarikçi ?li?kileri Güvenli?i" ba?l??? alt?ndaki tedbirlere sözle?mede yer vermek.
- Rehber uyum denetiminde uygulanacak metodoloji; denetimin planlanmas?, denetim prosedürlerinin uygulanmas? ve sonuçlar?n raporlanmas? olmak üzere üç ana süreç ekseninde ilerlemektedir. ?lk a?ama olan denetimin planlamas?nda denetim ekibi belirlenmelidir. Daha sonra kurumun anla??lmas? ve onu izleyen ad?m olarak denetim kapsam?n?n belirlenmesi gerekir. Kapsam belirlendikten sonra, denetim stratejisi ve program?n?n olu?turulmas? gerekmektedir. Bunlar tamamland?ktan sonra denetim prosedürünün uygulanmas?na geçilir. Bu a?amada ilk önce rehber uygulama sürecinin ve tedbirlerin etkinli?i de?erlendirilir. Son olarak bulgular tespit edilir, de?erlendirilir ve izlenir. Bütün bu a?amalar?n sonunda ise bir denetim raporu haz?rlan?r ve kuruma sunulur. Denetim raporunu olu?turan belgelerin ekler dahil her sayfas?, denetim ekibinde yer alan denetçiler taraf?ndan 5070 say?l? Elektronik ?mza Kanunu hükümlerine göre olu?turulan güvenli elektronik imza ile imzalanarak rapor nihai hâline getirilir. Denetim ekibi yaln?zca denetim kapsam?n?, kuruma teslim edilen denetim dosyas?n?n boyutunu, dosyan?n özet (hash) bilgisini ve teslim edilme tarihini içeren bilgileri taraflarca tutanak alt?na alarak elektronik ortamda saklamal?d?r. Denetim ekibi bunlar?n d???nda herhangi bir belge, doküman veya sair bilgiyi kurum d???na ç?karmamal?d?r. Denetim sonuçlar? ile yap?lan düzeltici ve önleyici faaliyetler, Denetim Rehberi'nde belirtilen usul ve esaslara göre bir rapor hâlinde Türkiye Cumhuriyeti Cumhurba?kanl??? Dijital Dönü?üm Ofisi'ne iletilecektir.
- Rehber uyum denetimi kapsam?nda denetim ekibinde yer alan denetçilerin/uzmanlar?n denetim çal??malar? süresince elde etti?i veya üretti?i bilgiler ile kulland?klar? bilgi varl?klar?n?n kullanma esaslar?n?n belirtilmesi, sorumluluklar?n?n tan?mlanmas? ve ilgili ki?iye sorumluluklar?n?n bildirilmesi amac?yla 6698 Say?l? Ki?isel Verilerin Korunmas? Kanunu kapsam?nda bir gizlilik taahhütnamesi imzalanmas? gerekir.

Denetim Rehberi'nin tamam?na bu ba?lant?dan ula?abilirsiniz.

Related Attorneys

- BURCU TUZCU ERS?N, LL.M.
- CEYLAN NEC?PO?LU, PH.D, LL.M.