T.C. ÇALIŞMA VE
SOSYAL GÜVENLİK BAKANLIĞI

Sayı:2 MAYIS-AĞUSTOS 2022

ÇALIŞMA VE SOSYAL GÜVENLİK BAKANLIĞI İÇ DENETİM BAŞKANLIĞI


# İÇ DENETİM BÜLTENİ

Merhaba,

Bakanlığımız ayrılma sonrası, sahip olduğu oldukça köklü kurumsal hafızası ve yönetsel tecrübesiyle, faaliyetlerini etkin ve sürdürülebilir bir anlayışla devam ettirmektedir. Covid-19'un tüm insanlar ve ülke yönetimleri üzerindeki olumsuz etkisi, yönetilebilir ve kontrol edilebilir sınırlar içerisinde, azalma eğilimi göstermektedir. Salgının, hem kamu hem de özel sektör hizmetlerini baskıladığını ve kurumları yeni risklerle yüz yüze getirdiğini gördük. İç denetim fonksiyonu, doğası gereği risk esaslı çalışır ve kurumun stratejik amaçlarına ulaşmasında karşılaşması muhtemel tehditleri ve bazen de fırsatları değerlendirerek, üst yöneticilere ve çalışanlara değer katmayı ve yürütülen faaliyetlerin geliştirilmesini amaçlar.

İç Denetim Başkanlığımız 2022 programını ve güvence ve danışmanlık faaliyetlerini; kurumsal kapasitenin güçlendirilmesini, yönetici ve çalışanlarda risk ve kontrol kavramlarına yönelik farkındalık ve bilinç düzeyinin artırılmasını, sunulan hizmet kalitesinin etkin ve etkili bir yönetim anlayışıyla yükseltilmesini, birimlerin örgütsel yapılarının, dinamik süreçlerinin ve aslında bir bütün olarak iç kontrol sistemlerinin makul güvence verecek şekilde yönetilmesini ve yönlendirilmesini hedefleyerek, birimlerin de talepleri doğrultusunda, ağırlıklı olarak danışmanlık fonksiyonu üzerinden kurgulamıştır. Faaliyetlerimizin Bakanlığımıza değer katacağına inanıyoruz.

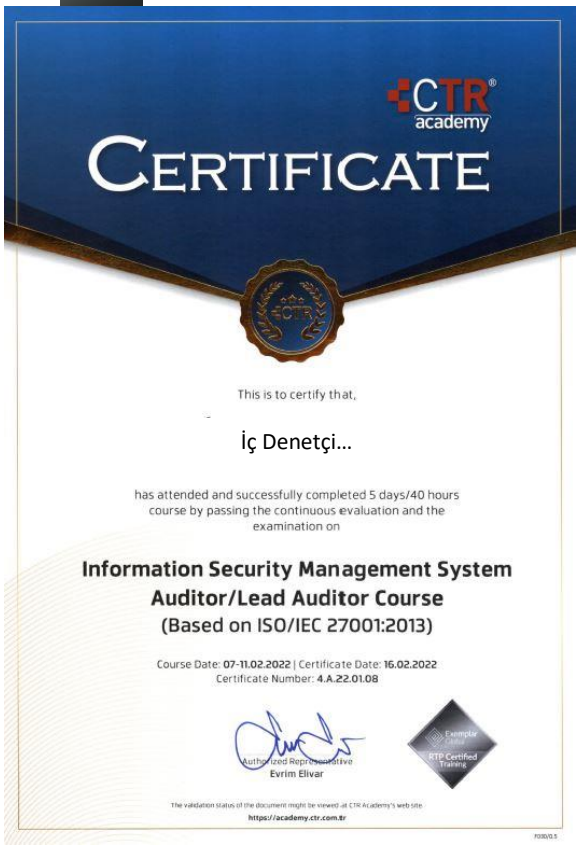
Fatih ALTUN

İç Denetim Başkanı

İÇ DENETİM

# BİZDEN HABERLER

1




Başkanlığımız İç Denetçilerinden Sadık DEMİRKAN, Mustafa ÜNVEREN, Zafer DEMİRCİ, Burak GÖNENCAN, Volkan ÖZBAY, Çetin SONKAYA ve Şerif OLGUN ÖZEN 07-11.02.2022-15.05.2022 tarihlerinde düzenlenen Exemplar Global Onaylı ISO 27001 Bilgi Güvenliği Yönetim Sistemi Baş Denetçi Eğitimine (Çevrimiçi) katılmış olup, yapılan performans değerlendirmeleri ve yazılı sınav sonucu ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Baş Denetçi Sertifikasını almaya hak kazanmışlardır.

İç Denetçilerimizi Başkanlığımız adına, eğitim süresince göstermiş oldukları ilgi, özveri ve çaba için tebrik eder, başarılarının devamını dileriz.

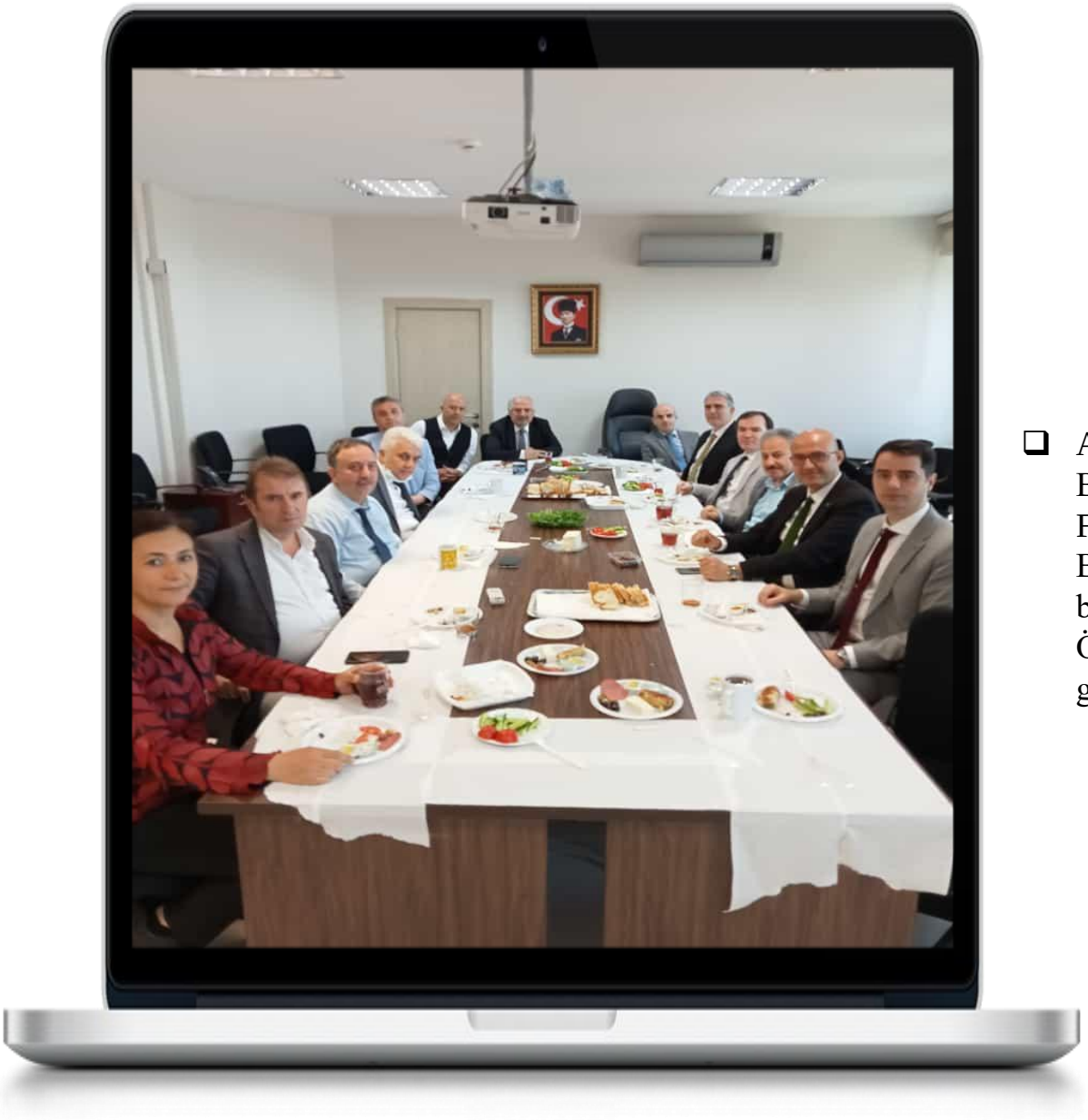
# BİZDEN HABERLER

2

- Başkanlığımıza yeni bir iç denetçi arkadaşımız daha katıldı. 18.04.2022 tarihi itibariyle aramıza katılan iç denetçi Hasan Hayri Nayir beye başarılar diliyoruz.

- Başkanlığımız tarafından yeni başlayan uzman yardımcılarına Şubat ayı içerisinde 2 grup şeklinde Bilgi Güvenliği Farkındalığı ve İç Denetim Başkanlığı' nın İdari yapılanması konularında iç denetçi Tolga ÖZBİLGE tarafından sunum gerçekleştirilmiştir.


# BİZDEN HABERLER



- Aile ve Sosyal Hizmetler Bakanlığı İç Denetim Başkanı sayın Yaşar ÖKTEM ve şube müdürü sayın Ferhat BAYGÜL 10.05.2021 tarihinde Başkanlığımızı ziyaret etmişlerdir. İki Bakanlığın birleştiği dönemde başkanımız olan sayın ÖKTEM'le iç denetim konusunda değerlendirme ve görüş alış verişinde bulunuldu.

Sadık DEMİRKAN CIA, CGAP, ISO 27001 BD
İç Denetçi
Tolga ÖZBİLGE, CIA, CISA
İç Denetçi
Burak GÖNENCAN CIA, ISO 27001 BD
İç Denetçi

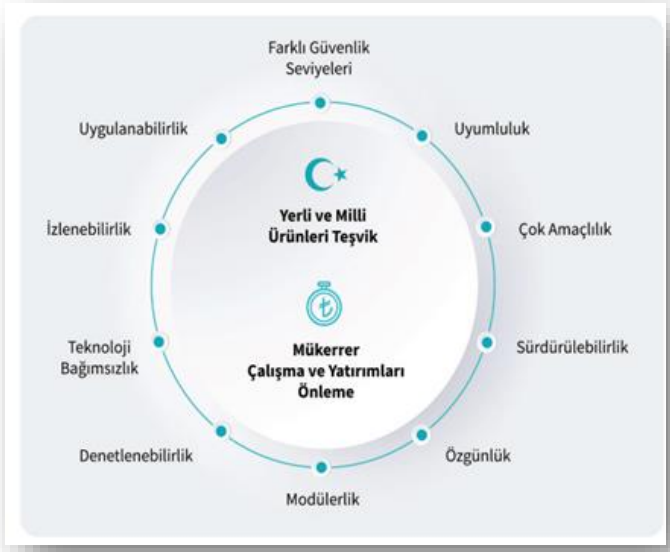
# BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİNİ TANIYALIM

Günümüz dünyasında dijital teknolojilerin baş döndürücü bir hızla gelişimi, ekonomik ve sosyal hayatın yanında güvenlik tanım ve kavramlarını da etkileyerek geleceğe dönük güvenlik bakış açılarını kökten değiştirmiştir. Özellikle uzmanlar tarafından, gelecek on yıl içerisinde gerçekleşmesi beklenen dijital dönüşümün pandemi sürecinde bir yıl gibi kısa bir süre sonuçlandığı düşünülmektedir. Dolayısıyla bu kadar hızlı bir dönüşüm güvenlik alanındaki ihtiyaçları da ciddi oranda artırmış bulunmaktadır.

Bu kapsamda bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle kritik bilgi/verinin gizliliğinin, bütünlüğünün veya erişilebilirliğinin bozulmasına karşın kamu düzeninin bozulmasını veya milli güvenliğin tehdit edebilmesini engelleyebilecek asgari güvenlik tedbirlerinin belirlenmesini ve söz konusu bu tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanması amacıyla, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı tarafından **"Bilgi ve İletişim Güvenliği Rehberi" (Şekil-1)** hazırlanmıştır.

Bu sayımızda, bir farkındalık oluşturması amacıyla Rehber ile ilgili bilgilendirmeleri kısaca soru-cevap şeklinde siz değerli Bakanlık çalışanlarımızla paylaşmak istedik.


Şekil-1




Şekil-2

**Bilgi ve İletişim Güvenliği Rehberi'nin hazırlanması fikri nasıl ortaya çıktı?**

Rehber, Ulusal Siber Güvenlik dayanıklılığımızı geliştirmeye yönelik olarak 21 temel maddeden oluşan ve 06.07.2019 tarihinde yayımlanan 2019/12 sayılı Cumhurbaşkanlığı Genelgesinin 21 inci maddesine istinaden hazırlanmıştır. Genelgenin ilgili maddesinde Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından verilecek katkı ile farklı güvenlik seviyelerini içeren Bilgi ve İletişim Güvenliği Rehberi'nin hazırlanarak yayımlanacağı belirtilmiştir. Bu çerçevede ilgili Genelge, Bilgi ve İletişim Güvenliği Rehberi'ne mevzuatsal dayanak teşkil etmektedir.

**Bilgi ve İletişim Güvenliği Rehberi'nin oluşturulmasındaki temel amaç nedir ve Rehber hangi kurumları kapsamaktadır?**

Rehber, bilgi güvenliği risklerinin azaltılması veya ortadan kaldırılması ve milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve uygulanmasını amaçlamaktadır. Ayrıca rehberin uygulanması sonucunda beklenen 12 hedef tanımlanmıştır (Şekil-2).

Sadık DEMİRKAN-İç Denetçi
Tolga ÖZBİLGE -İç Denetçi
Burak GÖNENCAN-İç Denetçi

# BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİNİ TANIYALIM

Rehber, bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraftan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı sektörlerinden "Elektronik Haberleşme", "Enerji", "Su Yönetimi", "Ulaştırma", "Bankacılık ve Finans" sektörleri ile nüfus, sağlık, güvenlik gibi alanlarda "Kritik Kamu Hizmetleri" sunan işletmeleri kapsamaktadır. Kısacası bilgi işlem birimi olan herkes bu rehbere uymak zorundadır.

**Bilgi ve İletişim Güvenliği Rehberine uyum süreci nasıl işlemektedir?**

Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi'nin 06.07.2019 tarih ve 30823 sayılı Resmi Gazete 'de yayımlanması neticesinde, Bilgi ve İletişim Güvenliği Rehberi hazırlık çalışmaları tamamlanarak 27 Temmuz 2020 tarihinde yayımlanmıştır. Rehbere uyum konusunda denetim faaliyetlerinin yürütülmesi çerçevesinde, kurum ve kuruluşlara yol göstermesi amacıyla da Bilgi ve İletişim Güvenliği Denetim Rehberi hazırlanarak 10 Ekim 2021 tarihinde yayımlanmıştır.

Rehber uyum süreci, her yönetim sisteminde olduğu gibi bir uyum planı (Şekil-2) ile başlamaktadır, daha sonra plan çerçevesinde oluşturulan yol haritasının uygulanmasından ve son olarak uygulamaların nasıl yürütüldüğünü denetlediğimiz denetim maddelerinden oluşmaktadır. Rehbere uyum süreci olarak kurum ve kuruluşlara ve kritik alt yapı hizmeti veren işletmelere 24 ay süre tanınmış olup, bu süre 27 Temmuz 2022 tarihi itibariyle sona erecektir.


**Rehberin içeriğinde neler yer almaktadır?**

Rehber içeriği dört ana bölümden oluşmaktadır.

**1. Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci:** Rehber uygulama süreci, bilgi güvenliği yönetim süreçlerine alternatif olarak uygulanacak bir süreç olarak hazırlanmamış olup mevcut bilgi güvenliği yönetim süreçlerine teknik olarak katkı sağlayacak tedbirleri ve faaliyetleri içermektedir.

**2. Varlık Gruplarına Yönelik Güvenlik Tedbirleri**: Her bir varlık grubuna dâhil olduğu ana başlığa göre uygulanacak olan asgari güvenlik tedbirleri belirlenmiş ve detaylandırılmıştır.

**3. Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri**: Uygulama ve teknoloji alanlarına özel güvenlik tedbirleri tanımlanmış ve detaylandırılmıştır.

**4. Sıkılaştırma Tedbirleri:** İşletim sistemi, veri tabanı ve sunucular için sıkılaştırma tedbirlerini içermektedir.

Rehber genel olarak dört alana odaklanıyor gibi görünse de Uygulama ve Teknoloji Alanlarına Yönelik Güvenlik Tedbirleri ve Sıkılaştırma Tedbirleri Varlık Gruplarına Uygulanan Tedbirlerin bir alt başlığı olarak düşünülebilir.

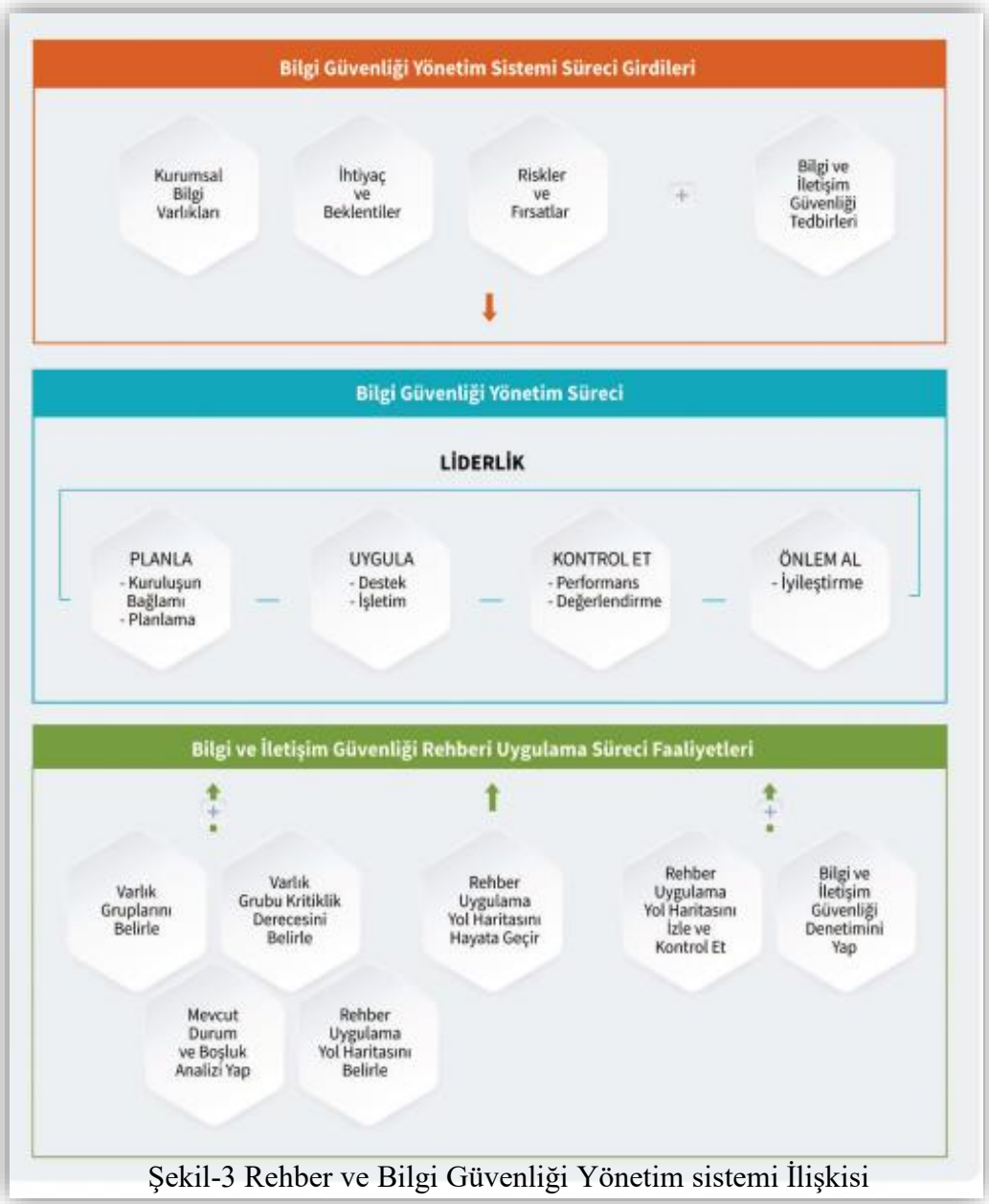
Sadık DEMİRKAN-İç Denetçi
Tolga ÖZBİLGE -İç Denetçi
Burak GÖNENCAN-İç Denetçi



**Bilgi Güvenliği Yönetim Sistemi ile Rehber arasında nasıl bir ilişki vardır?**

Rehber'e uyum sağlamakla yükümlü kurum ve kuruluşlar mevcut bilgi güvenliği yönetim sistemi kapsamında uyguladıkları kontrollere, Rehber'de yer alan bilgi ve iletişim güvenliği tedbirlerini de ekleyerek daha güçlü bir bilgi güvenliği yönetim sistemi elde edeceklerdir.

Rehber, BGYS'deki risk analiz faaliyetleri sonrasında uygulanacak kontrollere, her varlık grubu ve kritiklik derecesi özelinde tedbirler sunarak daha güvenilir ve ayakları yere basan bir bilgi güvenliği yönetim sistemi kurulmasını sağlar. Bunlarla birlikte Rehberde yer alan denetim soruları BGYS kapsamında gerçekleştirilecek iç tetkik faaliyetlerini destekleyerek kurum, kuruluş ve işletmeler için daha güvenilir bir iç kontrol ortamı oluşturulmasına zemin hazırlar. TS EN ISO/IEC 27001:2017 kapsamında kurum ve kuruluşların yaptıkları çalışmaların Rehberde tam olarak hangi çalışmaya karşılık geldiği Rehberde net olarak belirtilmiştir. Bu bağlamda, kurum ve kuruluşlara Rehber uyum süreci ile BGYS süreçlerinin entegrasyonu çalışmalarında yardımcı olması amacıyla ilgili Standardın kontrolleri ile Rehberde tanımlanan tedbirler arasındaki ilişkiyi ortaya koyan bir eşleştirme tablosu sunulmuştur.




Şekil-3 Rehber ve Bilgi Güvenliği Yönetim sistemi İlişkisi

**Rehber'in Uygulama Süreci Nasıl Gerçekleşecektir?**

Rehberin çıkış noktası tıpkı TS EN ISO/IEC 27001'de olduğu gibi varlık grupları üzerinedir. Bakanlığımızda öncelikle planlama kapsamında varlık grubu belirleme çalışmaları gerçekleştirilecek ve söz konusu varlık grubu ile etkileşim içinde bulunan kişiler tarafından alınan ortak karar neticesinde varlık gruplarının kritiklik derecesi belirlenecektir. Varlık gruplarına bilgi güvenliğini sağlamak amacıyla ne tür tedbirlerin uygulandığı mevcut durum analizi çalışmaları yapılarak ve devamında her bir varlık grubu için Rehber içeriğinde yer alan tedbirlerden uygulanmayanların belirlendiği boşluk analizi çalışması gerçekleştirilecektir. Planlama evresinin son aşamasında ise mevcut durum ve boşluk analizi çalışmaları göz önünde bulundurularak Rehber'e uyum sağlamak amacıyla bir yol haritası oluşturulacaktır. Rehber uygulama yol haritası, dönemsel olarak belirlenen hedefler dikkate alınarak Bakanlığımız personeli tarafından uygulama aşamasında hayata geçirilecektir. Kontrol etme ve önlem alma aşamasında Rehber'de yer alan tedbirlerin uygulanma sürecinde Rehber uygulama yol haritasına uygun olarak ilerlenip ilerlenmediği kontrol edilir. Değişiklik yönetimi aşamasında ise Bilgi ve İletişim Güvenliği Rehberinde kurumun varlık gruplarında, varlık grubu ile ilgili teknoloji alanlarında veya varlık gruplarını etkileyen mevzuat, standart ya da ikincil düzenlemelerde gerçekleştirilecek düzenlemeler göz önünde bulundurulmaktadır.

**Bilgi ve İletişim Güvenliği Rehberinin denetimi Bakanlığımızda nasıl gerçekleştirilecektir?**

Rehberde yer alan güvenlik tedbirlerinin uygulanmasına ilişkin denetimler, en az yılda bir kez olmak üzere, Bakanlığımız İç Denetim Başkanlığı bünyesindeki TS EN ISO/IEC 27001 Başdenetçi veya CISA (Certified Information Systems Auditor/Sertifikalı Bilgi Sistemleri Denetçisi) sertifikalarından en az birine sahip ya da bilgi sistemleri denetimi alanında eğitim almış en az iki iç denetçiden oluşturulan denetim ekibi tarafından gerçekleştirilecektir (Tablo-1). Denetim çalışmalarının 31 Aralık 2022 tarihine kadar tamamlanıp, denetim sonuçları ile düzeltici faaliyetleri içeren raporun iki ay içerisinde Dijital Dönüşüm Ofis'ine iletilmesi gerekmektedir. İlk yıl denetim raporu imza tarihini takip eden bir yıllık süre sonunda denetim çalışmaları tekrarlanarak, denetim sonuçlarının her yıl Dijital Dönüşüm Ofis Başkanlığı'na iletilmesi gerekmektedir.

Sadık DEMİRKAN-İç Denetçi
Tolga ÖZBİLGE -İç Denetçi
Burak GÖNENCAN-İç Denetçi



| No. | FAALİYET ADI | ROL ADI | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | İÇ PAYDAŞLAR | | | | | | | | DIŞ PAYDAŞLAR | | | | |
| | | Kurumun En Üst Düzey Yöneticisi | Bilgi Güvenliği Yöneticisi | Bilgi Sistemleri Yöneticisi | İç Denetçi | İlgili Birim Yöneticileri | İlgili Birim Uzman Personeli | Kurumsal SOME Yöneticisi | Varlık Grubu Koordinatörü | Dış Denetim Personeli | DDO | Bağlı/İlgili/İlişkili Üst Kurum | İlgili Düzenleyici ve Denetleyici Kurum | Teknik Danışman |
| 1 | Varlık Gruplarını Belirle | O | S | S | B | S | S | B | D | | | | | D |
| 2 | Varlık Grubu Kritiklik Derecesi Belirle | O | S | S | | S | S | B | D | | | | | D |
| 3 | Mevcut Durum ve Boşluk Analizi Yap | O | S | S | B | S | S | S | D | | | | | D |
| 4 | Rehber Uygulama Yol Haritası Belirle | O | S | S | | B | S | S | D | | | | | D |
| 5 | Rehber Uygulama Yol Haritasını Hayata Geçir | O | S | S | | S | S | S | B | | | | | |
| 6 | Bilgi ve İletişim Güvenliği Denetimi Yap | O | B | B | S | B | | B | D | S | S,B | B | B | |
| 7 | Rehber Uygulama Yol Haritasını İzle ve Kontrol Et | O | S | S | | S | S | S | B | | | | | D |
| 8 | Bilgi ve İletişim Güvenliği Rehber Değişikliklerini Yönet | O | S | S | B | S | S | B | D | | | | | D |
| 9 | Varlık Gruplarının Değişikliklerini Yönet | O | S | S | B | S | S | B | D | | | | | D |

**Denetim faaliyetlerini gerçekleştirmeyen kurum ve kuruluşlara yaptırım uygulanacak mıdır?**

Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi üzerinden kurum ve kuruluşların yaptıkları beyan ve bildirimlere ilişkin bilgiler esas alınarak Dijital Dönüşüm Ofisi Başkanlığı tarafından gözetim faaliyetleri gerçekleştirilecektir.

Rehber uyum faaliyetlerinin ve denetimlerin gerçekleştirilmemesi nedeniyle bir zafiyet oluşması durumunda hâlihazırda ilgili mevzuatta belirlenen yaptırımlar geçerli olacaktır. Oluşabilecek zararın boyutu ve etkisi göz önünde bulundurularak kurum içi adli veya idari soruşturma süreçleri işletilebilecektir.

Tablo-1 Bilgi ve İletişim Güvenliği Rehberi Uygulama Süreci için Sorumluluk Atama Matrisi

Zafer DEMİRCİ CIA, ISO 27001 BD
İç Denetçi

# Kişisel Verilerin Korunması Kavramının Tarihsel Gelişimi

Kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Tarihin her safhasında nispi önemi olmasının yanında bilgi toplumu olan çağımız dünyasında verinin, özellikle de kişisel verinin önemi çok yüksek boyutlara ulaşmıştır. Kişisel verinin önemi aynı zamanda kişisel verinin muhafazası ve uygun şekilde işlenmesini de önemli hale getirmiştir.

Kişisel verilerin korunması konusunda tarihsel gelişimin anlaşılması Kişisel Verileri Koruma Kanunu ve uygulamasının daha iyi anlaşılmasını ve değerlendirilmesini sağlayacaktır. Bu çalışmada Avrupa'da ve Türkiye'de kişisel verilerin korunmasına ilişkin sürecin tarihsel gelişimi hakkında kısa bir bilgilendirme yapılmıştır.*

**1. Avrupa Konseyi Düzenlemeleri**

**a.** Avrupa İnsan Hakları Sözleşmesinin İlgili Hükümleri Ülkemizin de kurucu üyeleri arasında bulunduğu Avrupa Konseyi tarafından hazırlanan ve 4 Kasım 1950'de Roma'da imzalanıp 3 Eylül 1953'te yürürlüğe giren İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (AİHS), kişisel verilerin işlenmesi hakkında doğrudan bir düzenleme içermemekle birlikte Avrupa İnsan Hakları Mahkemesi, geliştirdiği içtihatlarıyla kişisel verileri koruma altına almıştır. Diğer taraftan AİHS'nin "Özel ve Aile Hayatına Saygı Hakkı" başlıklı 8. maddesi "1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir…" şeklindedir. Bu madde ile kişisel verilerin korunmasına doğrudan atıf yapılmamakla birlikte, esasen özel hayata ve aile hayatına saygı hakkı kapsamında yer alan kişisel veriler hukuken koruma altına alınmıştır.

**b.** 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Avrupa Konseyi, 1970'li yıllardan itibaren kişisel verilerin korunması alanında çalışmalar yapmıştır. Yapılan çalışmalar neticesinde 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Türkiye, 28 Ocak 1981 tarihinde bu sözleşmeyi imzalayan ilk ülkelerden birisi olmuş; bu Sözleşme, 17 Mart 2016 tarih ve 29656 sayılı Resmi Gazete'de yayımlanarak iç hukuka dâhil edilmiştir. Bugün 108 sayılı Sözleşme olarak da bilinen Sözleşmenin temel amacı; her üye ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik yollarla işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır.

**c.** 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol

Bu protokolde taraf devletler, ülkelerinde uygulanmak üzere kişisel verilerin korunması alanında görevlerini tam bağımsızlıkla yerine getirecek denetleyici makam kurmayı taahhüt etmiştir. Türkiye, bu protokolü 8 Kasım 2001 tarihinde imzalamıştır. Protokol, 5 Mayıs 2016 tarih ve 29703 sayılı Resmi Gazete'de yayımlanarak iç hukuka dâhil edilmiştir.

**Kaynak: KVK Kurumu*

**2. Avrupa Birliği Düzenlemeleri**

**a. 95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktif**

Avrupa Birliğinde kişisel verilerin korunmasına ilişkin 1990'lı yıllarda başlayan çalışmalar neticesinde 1995 yılında Avrupa Parlamentosu ve Avrupa Konseyi "Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif"i kabul etmiştir. Direktifin temel amacı, Avrupa Birliği üye ülkelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılmasıdır. Bu kapsamda AB üyesi ülkeler, kişisel verilerin korunmasına ilişkin kanuni düzenlemelerini bu Direktifi esas alarak yapmışlardır. 6698 sayılı Kanun da temel olarak bu Direktif esas alınarak hazırlanmıştır. Diğer taraftan, Avrupa Birliği 95/46 sayılı Direktifi esas alarak sektörel bazlı düzenlemeler de yapmıştır. Bu düzenlemelerden en önemlisi, 2002/58/EC sayılı "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Özel Hayatın Gizliliğinin Korunmasına İlişkin Direktif"tir.

**b. 2016/679 Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)**

Avrupa Birliği, kişisel verilerin korunması alanında ortaya çıkan ihtiyaçları karşılamak üzere 2012 yılında yeni bir tüzük çalışması başlatmıştır. Avrupa Parlamentosu, Avrupa Konseyi ve Avrupa Komisyonu tarafından yapılan tüzük 2016 yılında kabul edilmiş olup, 25 Mayıs 2018 tarihinde 95/46 sayılı Direktif'i ilga ederek yürürlüğe girmiştir.

**3. Ulusal Düzenlemeler**

**1. Anayasa**

2010 yılında 5982 sayılı Kanun'la yapılan Anayasa değişikliği ile Anayasa'nın 20. maddesine ilave bir fıkra eklenmiştir. Söz konusu fıkrada; "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; 15 kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." hükmüne yer verilmiştir.

**2. 6698 Sayılı Kişisel Verilerin Korunması Kanunu**

Anayasada da, kişisel verilerin korunmasıyla ilgili detaylı düzenlemelerin kanunla yapılacağı belirtilmektedir. Bu kapsamda 26 Aralık 2014 tarihinde "Kişisel Verilerin Korunması Kanunu Tasarısı" TBMM Başkanlığına sunulmuştur. Tasarı, 24 Mart 2016 tarihinde kanunlaşmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir.

**3. 5237 Sayılı Türk Ceza Kanunu**

5237 sayılı Türk Ceza Kanununun 135. maddesinde, kişisel verilerin kaydedilmesi, 136. maddesinde, verileri hukuka aykırı olarak verme veya ele geçirme, 138. maddesinde, verileri yok etmeme fiilleri suç olarak düzenlenmiştir. Ayrıca Kanunun 140. maddesinde bu suçlarla ilgili olarak tüzel kişiler hakkında güvenlik tedbiri uygulanacağı hüküm altına alınmıştır.

Tolga ÖZBİLGE, CIA, CISA
İç Denetçi

## IPCC-HÜKÜMETLERARASI İKLİM DEĞİŞİKLİĞİ PANELİ

IPCC yani Hükümetler Arası İklim Değişikliği Paneli, Birleşmiş Milletler'e bağlı olarak faaliyet gösteren iki uzman kuruluş olan Dünya Meteoroloji Örgütü (WMO) ve Birleşmiş Milletler Çevre Programı üye ülkelerinden oluşan Uluslararası bir paneldir. 1988 yılından beri faaliyetlerine devam eden kuruluşa üye 195 adet ülke yer almaktadır. Ülkemiz de bu ülkelerden bir tanesidir. 2007 yılında panel Nobel barış ödülü almıştır.

Panelin amacı;

- İklim değişikliği konusunda mevcut bilimsel, teknik ve sosyo-ekonomik bilgi ve çalışmaları değerlendirmek,
- İklim değişikliğiyle mücadele ve iklim değişikliğine uyum konularında karar vericilere yol göstermek,
- Birleşmiş Milletler İklim Değişikliği Çerçeve Sözleşmesi (BMİDÇS)'ne iklim değişikliği ve politikalarıyla ilgili konularda amaçlarına uygun bilgi vermek ve belirli konularda özel rapor ya da teknik değerlendirmeler hazırlamak olarak belirtilmiştir.

Her 5 ila 7 yılda bir, dünyanın iklim sisteminin bugün geldiği duruma ilişkin derlenen Değerlendirme Raporları paylaşılmaktadır. Bu raporlardan ilki 1990 (Birinci Değerlendirme Raporu) yılında olmak üzere toplam 6 adet değerlendirme raporu ve ellinin üzerinde çalışma grupları ve özel raporlar yayınlamıştır. En son değerlendirme raporları AR6 (Çalışma Grubu I) Ağustos 2021' de ve AR6 (Çalışma Grubu III) Nisan 2022' de yayımlamıştır.

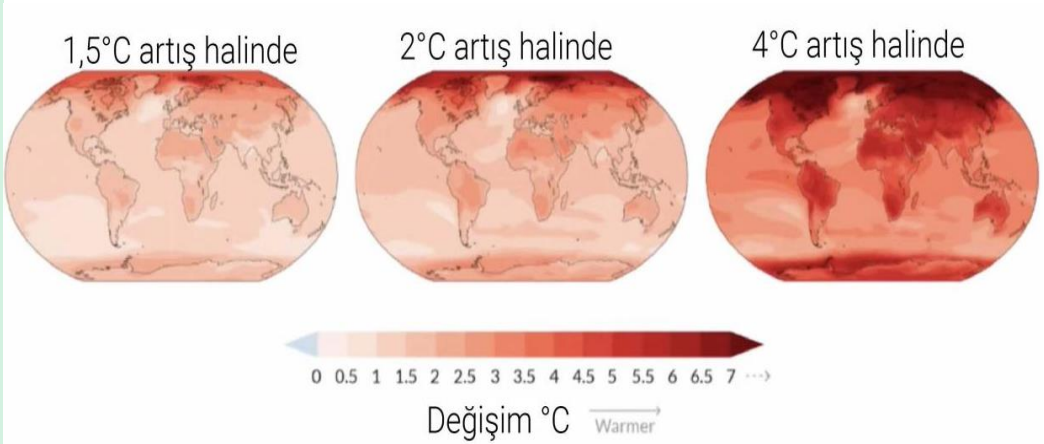
Söz konusu raporlar, Çalışma Grubu I Fiziksel bilim tabanı, Çalışma Grubu II (Etkiler, Uyum ve Hassasiyet, Çalışma Grubu III (WGIII) İklim Değişikliği Zarar Azaltma Raporu kapsayacak şekilde, daha çok politika yapıcılar ve karar vericiler gibi son kullanıcılara yönelik olarak hazırlamış olup, 30 bin sayfadan fazla çalışmanın 900 bilim insanın değerlendirmesiyle hazırlanmıştır.

En son yayımlanan AR6 raporlarında iklim değişikliği ile ilgili çok dikkat çekici sonuçlar ortaya konulmuştur.

- İnsan faaliyetlerinden kaynaklanan sera gazlarının 1850-1900 yıllarına kıyasla 2010-2019 yılları arasında küresel ısınmayı yaklaşık 1,1 °C artırdığını ve küresel sıcaklığın gelecek 20 yıl içinde 1,5 °C artmasının hatta bu rakamın da aşılmasının beklendiğini tespit etti.

Tolga ÖZBİLGE
İç Denetçi

- Afrika kıtasında şu anda dünya ortalamasının üstünde yüksek ısınma ve deniz seviyesi artışı görülüyor. Önümüzdeki 10 yıl içinde, Afrika'da daha sık ve yoğun yakıcı sıcaklıkların (günümüze göre 2050 yılında beş kata kadar daha yüksek) yanı sıra daha ağır yağışlar, daha sık ve yoğun kuraklıklar ve daha yaygın ve şiddetli kıyı taşkınları görülecek. Ayrıca, buzullar ve kar örtüsü yok olmaya devam edecek.
- İklim değişikliğinin yol açtığı veya daha şiddetli hale getirdiği aşırı hava olayları geniş kapsamlı ve şiddetli hasarlara yol açtı. Dünyanın 2021 yılında karşı karşıya kaldığı aşırı hava olaylarının çoğunun insan kaynaklı iklim değişikliği ile ilişkili olduğu tespit edildi. 2021'in Haziran ayında Pasifik Kıyısında yaşanan yakıcı sıcaklığın iklim değişikliği olmadan ortaya çıkmasının neredeyse imkânsız olduğu belirlendi.
- Sadece artan sıcaklıkların beraberinde getirdiği iklim tehlikeleri nedeniyle 3,5 milyar kişinin medeniyete beşiklik yapmış iklim kuşaklarının dışında yaşamaya mecbur kalacağı öngörülüyor. 2018 yılında Dünya Bankası üç bölgeden (Latin Amerika, Sahra Altı Afrika ve Güneydoğu Asya) 2050 yılına kadar iklim nedeniyle 143 milyon insanın göç edeceği tahmininde bulundu.




- Deniz seviyesindeki yükseliş (yılda 12 milimetre hızında) nedeniyle batı Pasifik'te şu ana kadar sekiz ada sular altında kaldı. İki ada daha kaybolma tehlikesiyle karşı karşıya.
- Artan sıcaklıklar, gıda üretimini etkilemeye devam edecek ve 2050 yılına kadar ısınmanın miktarına bağlı olarak tahıl maliyetlerini tahminen %29'u bulan oranlarda artıracak. Bu fiyat artışları, dünya genelinde tüketicileri etkileyecek ve özellikle düşük gelirli tüketiciler yetersiz beslenme riskiyle karşı karşıya kalacak.

- İklim değişikliğinin ve toprağın niteliğini yitirmesinin bir sonucu olarak bir milyon hayvan ve bitki türü şu anda yok olma tehdidiyle karşı karşıya. Uluslararası Doğayı Koruma Birliği'nin (IUCN) Nesli Tükenme Tehlikesi Altında Olan Türlerin Kırmızı Listesi'nde yer alan en az 10.967 türü etkiliyor. Bramble Cay melomys (bir kemirgen cinsi), iklim değişikliğinin doğrudan bir sonucu olarak nesli tükendiği bildirilen ilk memeli.
- Bir araştırmaya göre, sera gazı emisyonlarının mevcut ivmeyle artmaya devam etmesi durumunda dünya genelinde 215 milyon kentli 35 °C'nin üstünde ortalama yaz sıcaklıklarına maruz kalacak.

Pervin TEKİN-MHU
Derya MUSAPAŞAOĞLU-MHU
Strateji Geliştirme Başkanlığı

# BAKANLIĞIMIZDA İÇ KONTROL SİSTEMİNE YÖNELİK ÇALIŞMALAR

## BAKANLIĞIMIZDA İÇ KONTROL SİSTEMİNE YÖNELİK ÇALIŞMALAR

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun AB normlarına uygun olarak düzenlenmesi ve hayata geçirilmesiyle birlikte, kamu sektöründe kurulması ve yapılandırılması öngörülen iç kontrol sistemine yönelik çalışmalar, Hazine ve Maliye Bakanlığı koordinasyonu ve sorumluluğunda hızlandırılmıştır. Bu Kanuna istinaden süreç içerisinde yayınlanan ikincil ve üçüncül düzenlemeler sonrası*, tüm kamu sektöründe olduğu gibi, Bakanlığımızda da iç kontrol sistemine yönelik faaliyetler Strateji Geliştirme Başkanlığı'nın koordinasyonu ve gözetiminde başlatılmıştır. Dünden bugüne iç kontrol sistemine ilişkin Bakanlığımız bünyesinde gerçekleştirilen ana faaliyet ve durumlar kronolojik olarak şekilde verilmektedir.

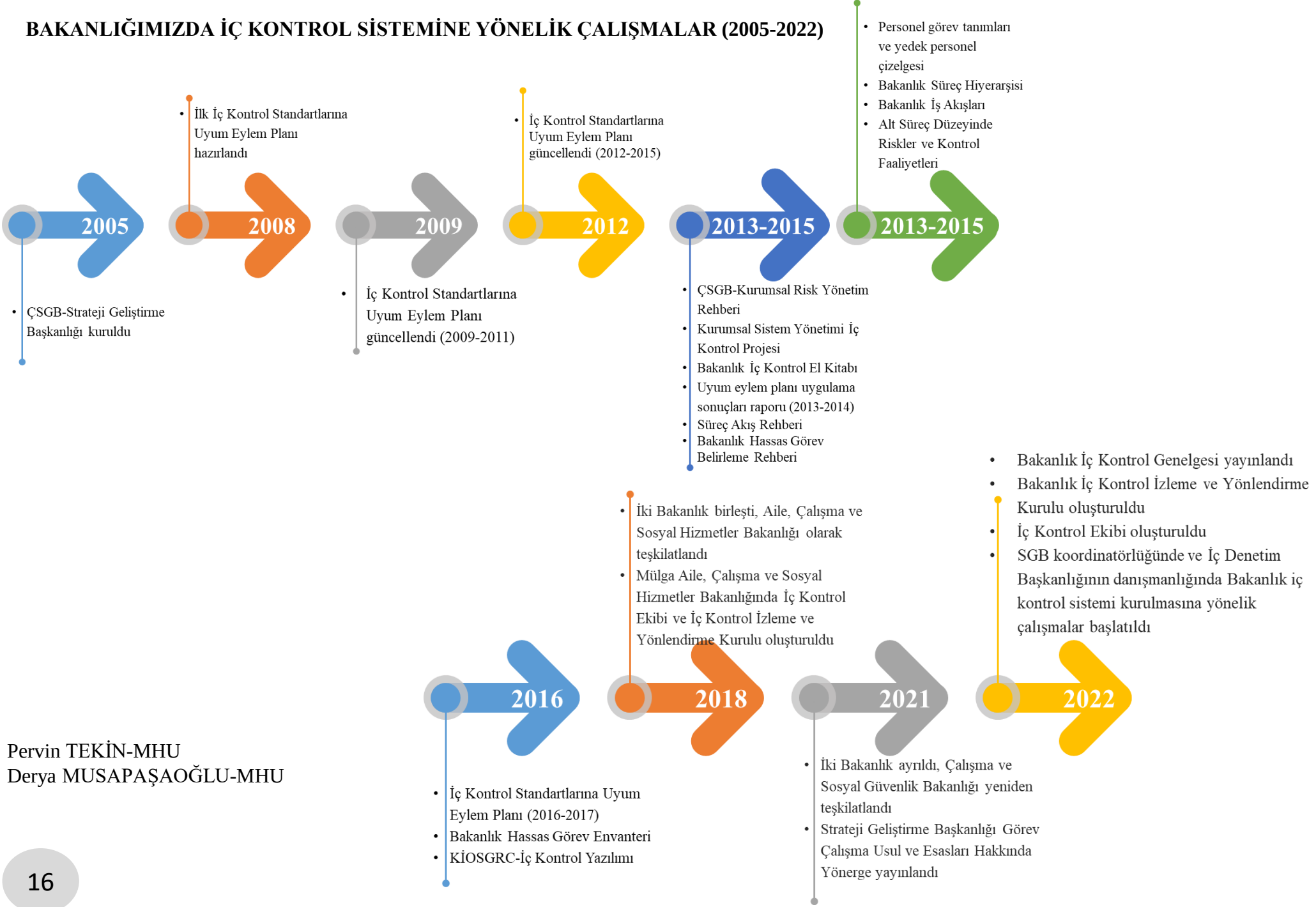
* Hazine ve Maliye Bakanlığı tarafından bu Kanuna istinaden şu ikincil ve üçüncül düzey düzenlemeler yapılmıştır:

- *İç Kontrol ve Ön Mali Kontrole İlişkin Usul ve Esaslar*
- *Üst Yöneticiler İçin İç Kontrol ve İç Denetim Rehberi*
- *Kamu İç Kontrol Standartları Tebliği*
- *Üst yönetici Rehberi*
- *Kamu İç Kontrol Standartlarına Uyum Eylem Planı Rehberi*


*COSO KÜPÜ, 2013*

Yaklaşık 14 yıllık bir tecrübeyle, iç kontrol sistemine yönelik çalışmalarımız Bakanlığımız bünyesinde aktif olarak yürütülmektedir. Kontrol ortamı bileşeninin öngördüğü ve şart koştuğu ilkelere yönelik dokümantasyon çalışmalarının zamanla iyi bir şekilde yürütüldüğü anlaşılmaktadır. Tekrar başlattığımız süreçte, iç kontrole yönelik Bakanlığımız faaliyetlerine özgü sistem kurgu ve mimarisine, bu yönde istenen politika ve prosedürlerin hazırlanmasına, hazırlanmış olanların güncellenmesi çalışmalarına, birimlerin sahip oldukları birikimle hızla tepki vereceği düşünülmektedir. İç kontrol sistemine yönelik çalışmalarda ana hedefin, kavramın tüm bileşenlerinin mevcut ve işler durumda olmasının sağlanması ve en önemlisi de yönetimin ve çalışanların sorumluluğunda olan sahiplenme ve yaşatma ilkesinin, sürdürülebilir bir anlayışla yönetim felsefesi ve iş yapma tarzına yansıtılması olmalıdır.

# BAKANLIĞIMIZDA İÇ KONTROL SİSTEMİNE YÖNELİK ÇALIŞMALAR (2005-2022)




Pervin TEKİN-MHU
Derya MUSAPAŞAOĞLU-MHU

# SORU/CEVAP

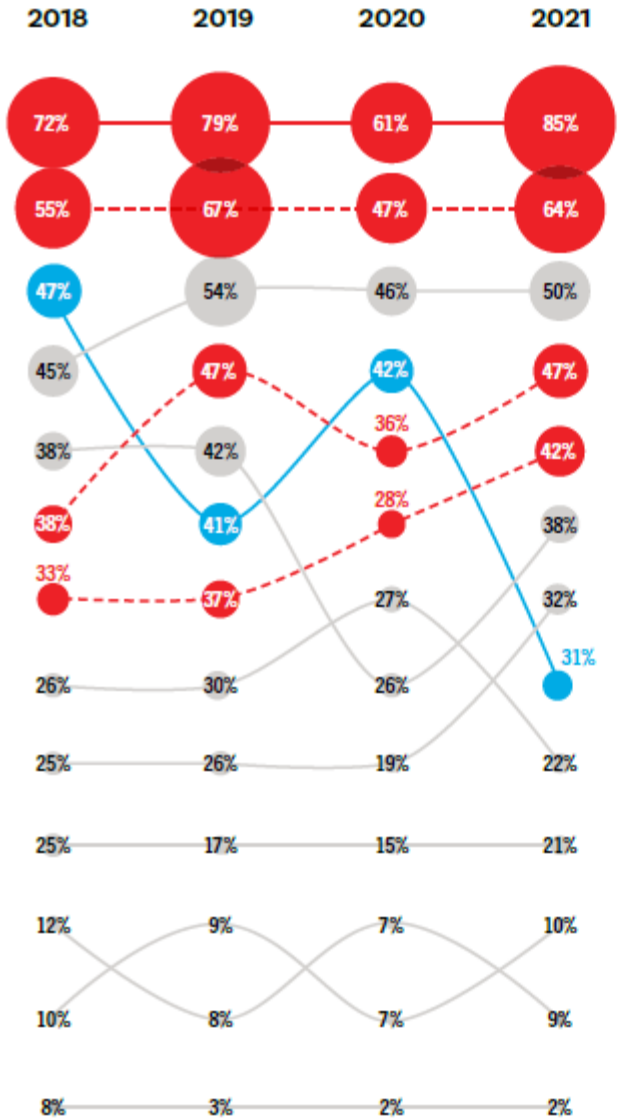
İç denetçiler birimlerimizde güvence ve danışmanlık hizmeti verirlerken, süreç boyunca, özellikle de açılış toplantılarında birim yöneticilerine ve çalışanlarına, iç denetçilerin bağımsızlığına ve objektifliğine ısrarla vurgu yapmaktadırlar. İç denetim faaliyetinin kurum içi bağımsızlığı ve iç denetçilerin objektifliği mesleki uygulamaları açısından nasıl tanımlanmaktadır?

İç denetim faaliyetinin bağımsızlığı ve tarafsızlığı konusu, hem İç Denetim Yönergemizde, hem de IIA Uluslararası İç Denetim Standartlarında (Standart) yer almaktadır. Standardın 1100-Bağımszılık ve Objektiflik maddesinde, "iç denetim faaliyeti bağımsız olmak zorundadır ve iç denetçiler görevlerini yaparken objektif davranmak zorundadır" standart hükmü yer almaktadır.

Bağımsızlık, mesleğimiz açısından iç denetim faaliyetinin sorumluluklarını tarafsız olarak yerine getirme kabiliyetini tehdit eden şartlardan uzak olması anlamına gelmektedir. Kurum içerisinde iç denetim faaliyetinin sorumluluğunu etkili bir şekilde yerine getirmesi açısından istenen, teşkilat içerisinde üst yönetime (Bakana) doğrudan bağlı olması ve çifte raporlama ilişkisinin sağlıklı bir şekilde oluşturulmasıdır. İç denetim faaliyetimizin Bakanlık içerisinde, üst yönetime doğrudan fonksiyonel raporlama yapması, diğer birimlere de idari raporlama yaparak görevlerini sürdürmesi, standartlarda da belirtildiği gibi kurumsal bağımsızlığımızın etkili olan en önemli göstergelerindendir.

İç denetçilerin objektifliği, görevlerini iş sonucunda çıkan ürüne (örneğin raporlamaları) gerçekten ve dürüst bir şekilde inanacakları ve bu ürünün kalitesinden önemli bir taviz vermeyecekleri şekilde yapmalarını sağlayan tarafsız bir zihinsel tutumu ifade eder. İç denetçilerin objektifliği denetim konularına ilişkin karar ve yargılarını başkalarınınkilere bağlamamalarını gerektirir. Objektifliğe yönelik tehditler denetçi, görev, fonksiyon ve kurum seviyesinde ele alınır ve değerlendirilir. Örneğin, bir iç denetçinin iç kontrol sistemi tasarlaması, uygulaması ve yürütmesi, yönetim adına risk iştahını veya risk toleransını belirlemesi, yönetim adına karar alması durumunda objektifliğinin bozulacağı varsayılır.

## Yüksek/Çok Yüksek olarak derecelendirilen Risk Alanlarının Eğilimi




Sibergüvenlik

BT (diğer seçenekler kapsamında değil)

Uygunluk/Düzenleyici (ICFR hariç)

Üçüncü-taraf ilişkiler

KRY ve ilgili süreçler

Yönetişim ve kültür

Sahtecilik

Operasyonel

Maliyet/harcama azaltımı

Mali (ICFR hariç)

Sürdürebilirlik/mali olmayan raporlama

Mali olmayan raporlama (ICFR dahil)

Dış denetim desteği

2018 yılından beri yüzde 10+ artanlar
2018 yılından beri yüzde 10+ azalanlar
----Noktalı çizgi yüzde 10 civarındaki bir değişikliğe işaret etmektedir

*Operasyonel risk, kamu sektöründe önemini kaybetmekte, 2018'den bu yana sıra ve yüzde olarak önemli ölçüde düşmektedir.*

*Siber güvenlik, BT, üçüncü taraf ilişkileri ve KRY artan risk seviyeleriyle onun yerini almaktadır.*

| Temsil Edilen Endüstriler | |
|---|---|
| Educational services -Eğitim hizmetleri | 32% |
| Public administration -Kamu idaresi | 32% |
| Health care and social assistance-Sağlık hizmeti ve sosyal yardım | 9% |
| Utilities-Kamu hizmetleri | 9% |
| Other -Diğer | 18% |

***Kaynak**: The IIA's North American Pulse of Internal Audit Survey-2022*
*ICFR= Mali Raporlamaya ilişkin İç Kontroller*
*Sadece kamu sektörü (mali hizmetler hariç)*
*2018 için n=94, 2019 için n=135, 2020 için n=142, 2021 için n=111*

*Soru: Aşağıdaki riskli alanlar içerisinde kurumunuzun risk düzeyini nasıl tanımlarsınız?*

# IIA-Uluslararası İç Denetim Standartları Terimler Sözlüğünden…

## Güvence Hizmetleri (Assurance Services)

Kurumun risk yönetimi, kontrol ve yönetişim süreçlerine dair bağımsız bir değerlendirme sağlamak amacıyla delillerin objektif bir şekilde incelenmesidir. Mali yapıya, performansa, mevzuat ve düzenlemelere uyuma, bilgi sistemleri güvenliğine ve ihtimam denetimine (due diligence; ayrıntılı durum tespit çalışması) yönelik görevler bu kapsamdaki örneklerdir.

İÇ DENETİM

GÜVENCE

İÇ DENETİM

# İÇ DENETİM BAŞKANLIĞI

## DEĞER KATMAK İÇİN VARIZ…

**TEMEL FAALİYETİMİZ**

- **Güvence**
- **Danışmanlık**

**Bize Ulaşın**:
Telefon: +90 (312) 296 73 50