Cumhurbaşkanlığı (Siber Güvenlik Başkanlığı)'ndan:

DENETİM YÖNETMELİĞİ

BİRİNCİ BÖLÜM
Başlangıç Hükümleri

Amaç

MADDE 1– (1) Bu yönetmeliğin amacı Siber Güvenlik Başkanlığı tarafından görev ve faaliyet alanında yapılacak denetim, inceleme ve gözetim faaliyetlerine ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2– (1) Bu yönetmelik 12/03/2025 tarihli ve 7545 sayılı Siber Güvenlik Kanunu kapsamındaki tarafların ilgili mevzuat kapsamındaki faaliyet ve işlemlerine ilişkin Başkanlık tarafından yürütülecek denetim, inceleme ve gözetim faaliyetlerini, kurum ve kuruluşların denetim ve gözetim yükümlülüklerini, denetçinin yetkileri ve yükümlülükleri ile denetlenen tarafın görev ve sorumluluklarına ilişkin hususları kapsar.

(2) 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu uyarınca yürütülen istihbari faaliyetler ile 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu uyarınca ilgili kurumların kendi uhdesinde yürütülen faaliyetler bu Yönetmelik kapsamı dışındadır.

Dayanak

MADDE 3– (1) Bu yönetmelik, 177 sayılı Cumhurbaşkanlığı Kararnamesi'nin 4 üncü ve 9 uncu maddesine, 12/03/2025 tarihli ve 7545 sayılı Siber Güvenlik Kanununun beşinci maddesinin birinci fıkrasının (h) bendi ve sekizinci maddesi ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 60/A maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4– (1) Bu yönetmelikte geçen;

a) Bağımsız denetçi: Başkanlık tarafından bağımsız denetim yapmakla yetkilendirilmiş ve belgelendirilmiş, tarafsız ve ilgili konuda uzmanlığa sahip gerçek kişiyi,

b) Bağımsız denetim: Kurum ve kuruluşların ilgili mevzuatta belirlenen yükümlülüklere uyum sağlamak üzere aldığı tedbirlerin, bağımsız denetim kuruluşları veya bağımsız denetçiler eliyle teknik ve idari yöntemlerle incelenmesi, doğrulanması ve raporlanması suretiyle uyumluluk, etkinlik ve yeterliliği hakkında görüş oluşturularak Başkanlığa makul güvence sağlayan denetim faaliyetini,

c) Bağımsız denetim kuruluşu: Başkanlık tarafından bağımsız denetim yapmakla yetkilendirilmiş ve belgelendirilmiş, tarafsız ve ilgili konuda uzmanlığa sahip tüzel kişiyi,

ç) Bağımsızlık Beyanı: Bağımsız denetçi veya bağımsız denetim kuruluşunun, denetlenecek tarafla arasında bağımsızlığını ve tarafsızlığını etkileyebilecek herhangi bir ilişki, çıkar veya menfaat bulunmadığını, Başkanlıkça belirlenen formatta yazılı olarak taahhüt ettiği belgeyi,

d) Başkan: Siber Güvenlik Başkanını,

e) Başkanlık: Siber Güvenlik Başkanlığını,

f) Bulgu: Denetim sonucunda tespit edilen mevzuata aykırılık, güvenlik zafiyeti, kontrol eksikliği veya iyileştirmeye açık hususu,

g) Denetçi: Başkan tarafından denetim faaliyetini icra etmekle görevlendirilmiş Başkanlık personelini,

ğ) Denetim: Denetlenen tarafların Kanun hükümleriyle ilgili faaliyet ve işlemlerinin, ilgili mevzuata ve Başkanlıkça belirlenen usul ve esaslara uygunluğunun yerinde, uzaktan veya elektronik ortamda incelenerek, yeterli ve uygun denetim kanıtlarının elde edilmesi amacıyla denetim tekniklerinin uygulanarak denetlenmesi ve değerlendirilerek rapora bağlanmasını,

h) Denetim ekibi: Başkan tarafından görevlendirilen, belirli bir denetim görevini yerine getirmek üzere, sorumlu denetçi ve onun sorumluluğu altında görev yapan denetçi veya denetçiler ile bilgisine ihtiyaç duyulabilecek uzman kişilerden oluşan ekibi,

ı) Denetim hizmet sağlayıcı: Siber güvenlik alanında faaliyet gösteren, organizasyonun operasyonel süreçlerini, bilgi sistemlerini veya yasal mevzuatlara uyumunu; ulusal/uluslararası standartlara göre incelemek, doğrulamak ve raporlamak üzere profesyonel ve bağımsız denetim hizmeti sunan ve sundukları siber güvenlik hizmeti nedeniyle Başkanlıkça yetkilendirilen tüzel kişilikler/şirketleri,

i) Denetim ölçütü: Denetimde uygunluğu değerlendirmek için esas alınan güvenlik kontrolü, mevzuat hükmü, standart, düzenleme veya gerekliliği,

j) Düzeltici faaliyet: Denetim sonucunda tespit edilen bulguların giderilmesine yönelik işlemleri,

k) Gözetim: Tarafların ilgili mevzuata uyumunun ve sürekli veya dönemsel olarak izlenmesi, değerlendirilmesi, risklerin belirlenmesi ve denetim faaliyetlerine girdi oluşturulmasına yönelik faaliyetleri,

l) Gözetim platformu: Taraflar ile sorumlu birimlerinin, gerçek ve tüzel kişilerin kayıt altına alınması, kullanıcılarının yetkilendirilmesi, gözetime ilişkin verilerin alınabilmesi ve analiz edilebilmesi için kullanılacak uyum ve denetim izleme sistemini,

m) Güvence: Tarafların Başkanlığın ilgili mevzuatındaki yükümlülüklerini yerine getirme durumuna ilişkin yapılan değerlendirme sonucunun; kullanılan yöntem, elde edilen kanıtların yeterliliği ve güvenilirliği ile değerlendirmeyi gerçekleştiren mekanizmanın bağımsızlığı ve yetkinliği dikkate alınarak güvenilirliğine duyulan güven düzeyini,

n) İç denetim: Kurum veya kuruluşun bilgi sistemleri, siber güvenlik, operasyonel ve yönetsel süreçler ile risk yönetimi, kontrol ve yönetişim mekanizmalarının mevzuata, Başkanlıkça belirlenen usul ve esaslara ve kurum içi politikalara uygunluğunu; bağımsız, nesnel ve sistematik bir şekilde değerlendirerek makul güvence sağlayan içsel denetim faaliyetini,

o) İlgili birim: Denetimin konusu ve kapsamı ile ilgili Başkanlığın hizmet birimi veya birimlerini,

ö) İlgili mevzuat: Başkanlığın görev ve yetki alanına ilişkin kanun, Cumhurbaşkanlığı kararnamesi ve bunlara dayanılarak yürürlüğe konulan yönetmelik, usul ve esaslar, standart ve diğer düzenleyici işlemleri,

p) Kanun: 12/3/2025 tarihli ve 7545 sayılı Siber Güvenlik Kanununu,

r) Kalite güvence sistemi: Denetim faaliyetlerinin, ilgili mevzuata, uluslararası standartlara, Başkanlıkça belirlenen usul, esas, metodoloji, standartlara, etik ilkelere uygun, etkin ve tutarlı şekilde yürütülmesini, denetim kalitesinin izlenmesini, uygulama birliğinin sağlanmasını ve sürekli iyileştirilmesini güvence altına almak üzere oluşturulan politika, yöntem, süreç ve uygulamalar bütününü,

s) Kamu kurumları: Devlet Teşkilatı Merkezi Kayıt Sistemi platformunda yer alan kurumları,

ş) Kontrol: Kurum ve kuruluşların, stratejik ve operasyonel hedeflerine ulaşmak, bilgi varlıklarını korumak, veri bütünlüğünü sağlamak, faaliyetlerin mevzuata uygunluğunu ve etkinliğini tesis etmek, iş sürekliliğini temin etmek ve risklerini yönetmek için uyguladığı politika, prosedür, süreç ve teknik önlemlerin bütününü,

t) Kritik altyapı: İşlediği bilginin veya verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,

u) Kritik altyapı sektörleri: İçeriği ve kapsamı Siber Güvenlik Kurulu ve Başkanlık düzenlemeleriyle belirlenen sektörleri,

ü) Komisyon: Denetim ve Yaptırım Değerlendirme Komisyonu,

v) Mahallinde inceleme: Denetlenen tarafın faaliyetlerinin ilgili mevzuata uygunluğunun değerlendirilmesi amacı ile ilgili gerçek veya tüzel kişiler ile bu kişilerin ad ve hesabına faaliyet yürütenlerin yönetim yerleri, binaları ve eklentileri gibi tesislerinde gerçekleştirilen yerinde kontrol ve tespit süreçlerini,

y) Makul güvence: Denetim çalışmasında gerekli teknik bilgi ve tecrübeye sahip deneçinin, denetim prosedürlerini uygulamak suretiyle elde ettiği güvenilir, uygun ve yeterli düzeyde kanıtlara dayanarak sunduğu kesin (mutlak) olmayan güvenceyi,

z) Öz değerlendirme: Kurum ve kuruluşların Başkanlığın ilgili mevzuat yükümlülüklerine uyum durumlarını belirlemek amacıyla gerçekleştirdikleri değerlendirme sürecini,

aa) Öz denetim: Kurum ve kuruluşlar tarafından, Başkanlığın ilgili mevzuat yükümlülüklerine uyum durumu ve uygulanma etkinliğine ilişkin kendi bünyelerinde gerçekleştirdikleri denetim faaliyetini,

bb) Sektörel SOME: Belirli bir kritik altyapı sektöründe faaliyet gösteren gerçek veya tüzel kişilere ilişkin düzenleme, denetim ve gözetim yapmak, idari yaptırım faaliyetlerini yürütmek, izin, lisans veya yetkilendirme vermek ya da benzeri kamu otoritesi görevlerini yürütmek üzere kanun veya diğer mevzuatla yetkilendirilen ve kendi görev alanı kapsamında siber güvenliğe ilişkin düzenleme, denetim veya gözetim ve yaptırım yetkisi bulunan, sektörel siber olaylara müdahale ekiplerini işleten kamu kurum ve kuruluşlarını,

cc) Sektörel denetim: Sektörel SOME'ler tarafından sektöre özel siber güvenlik mevzuatının uyum durumu ve uygulanma etkinliğine ilişkin kendi sorumluluk alanı kapsamında gerçekleştirilen denetim faaliyetini,

çç) Sınırlı güvence: Denetim çalışmasında gerekli teknik bilgi ve tecrübeye sahip denetçinin, makul güvenceye kıyasla daha sınırlı denetim prosedürlerini uygulamak suretiyle elde ettiği kanıtlara dayanarak sunduğu kesin(mutlak) olmayan güvenceyi,

dd) Sorumlu birim(ler): Kurum ve kuruluşların merkez, taşra veya yurt dışı teşkilatına bağlı alt birimlerinde ilgili mevzuat çerçevesinde uygulanan tedbirlerin etkin uygulandığına dair güvence oluşturan denetim birim(ler)ini,

ee) Sürekli gözetim: Denetim programının oluşturulmasına ve risk değerlendirmesine esas teşkil etmek üzere Başkanlıkça sürekli olarak yürütülen izleme faaliyetini,

ff) Takip denetimi: Düzeltici faaliyetlerin uygulanma durumunun doğrulanması amacıyla yapılan denetimi,

gg) Taraflar: Siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşları,

ğğ) Tedbir: Varlıklara yönelik ilgili mevzuat konusu kapsamındaki risklerin azaltılması veya ortadan kaldırılması için alınması gereken önlemlerin her birini,

hh) Uygunsuzluk: Tabi olunan mevzuat hükümlerinin, yürürlükteki yasal düzenlemelerin veya Başkanlık tarafından belirlenen usul, esas ve standartların kısmen veya tamamen yerine getirilmemesi, ihlal edilmesi ya da bu kurallardan sapılması durumunu,

ıı) Uzman: Denetim ekibine teknik bilgi ve uzmanlığıyla katkı sağlayan, Başkan tarafından görevlendirilen kişiyi,

ii) Uzaktan denetim: Başkanlık tarafından yürütülmekte olan denetimin; denetlenen taraf yetkilileri ile toplantıların gerçekleştirilmesi, denetime konu bilgi, belge ve verilerin alınması ve denetlenen tarafa ait sanal veya fiziki ortamların denetlenmesi dâhil diğer tüm denetim aşamalarının tamamının veya bir kısmının denetçi tarafından teknolojik araçlar ve bilgi teknolojileri vasıtasıyla uzaktan gerçekleştirilmesini
ifade eder.

(2) Bu Yönetmelikte geçen ve birinci fıkrada yer almayan tanımlar için Kanunda ve ilgili mevzuatta yer alan tanım ve kısaltmalar geçerlidir.

İKİNCİ BÖLÜM
Görev, Yetki ve Yükümlülükler

Başkanlığın görev ve yetkileri

MADDE 5– (1) Başkanlığın denetim, inceleme ve gözetim kapsamındaki görev ve yetkileri şunlardır:

a) Yıllık denetim programını oluşturmak, gözetim dönemlerini planlamak.

b) Denetim, inceleme ve gözetim çalışmalarını yürütmek.

c) Denetim kapsamında idari yaptırım ve/veya tedbir uygulanmasına karar verilmesi halinde bunlara ilişkin işlemleri yürütmek.

ç) Denetim ve inceleme sonuçları ile ilgili işlemleri yürütmek.

d) Yürütülen denetim ve gözetim faaliyetleri kapsamında, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyacağı her türlü bilgi ve belgeyi istemek, gerektiğinde görüşlerine başvurmak üzere Başkanın onayı ile diğer kamu kurum ve kuruluşlarından uzman personel talep etmek.

e) Denetimlerin etkin olarak yürütülmesini sağlamak üzere dijital altyapılar kullanmak.

f) Denetim faaliyetlerine ilişkin önemlilik ve öncelik ilkeleri ile denetimlere ilişkin risk değerlendirmelerinde dikkate alınacak ölçütleri, sınıflandırma ve uygulama esaslarını belirlemek.

g) Kurum ve kuruluşlar tarafından ilgili mevzuat çerçevesinde yürütülen uyum çalışmaları ve denetimlerinin gözetimini dijital altyapı üzerinden yürütmek.

ğ) Sektörel SOME' lerle kritik altyapı sektörlerine yönelik denetim ve gözetim çalışmalarını yürütmek.

ğ) Kurum ve kuruluşların Başkanlıkça belirlenen yükümlülüklere uyum seviyesinin belirlenmesi çalışmalarını yürütmek.

h) Bağımsız denetim kuruluşları ile bağımsız denetçilerin Başkanlık denetimlerinde görevlendirilmesi, denetimi ve gözetimine ilişkin iş ve işlemleri yürütmek.

ı) Denetim, inceleme ve gözetim faaliyetlerine ilişkin usul ve esasları belirlemek ve bunlara ilişkin rehber ve standartları hazırlamak.

(2) Birinci fıkradaki görev ve yetkiler kapsamında yürütülecek faaliyetler, Denetim ve Gözetim Daire Başkanlığı tarafından yerine getirilir.

Denetim ve Yaptırım Değerlendirme Komisyonu

MADDE 6– (1) Denetim sonucunun teknik, idari ve hukuki boyutları göz önünde tutularak alınması gereken tedbirlerin ve uygulanacak yaptırımların değerlendirilmesi amacıyla Denetim ve Yaptırım Değerlendirme Komisyonu oluşturulur.

(2) Komisyon başkan yardımcısı seviyesinde bir başkan ile en az daire başkanı seviyesinde üyeler ve gerektiğinde konuya ilişkin teknik, hukuki veya idari uzmanlık sağlayacak personelden oluşur. Komisyon başkanı ve üyeleri Başkan tarafından görevlendirilir.

(3) Komisyon denetim faaliyetleri sonucunda; düzeltici faaliyet uygulanması, teknik tedbir alınması, yetkilendirme veya görevlendirme süreçlerine ilişkin askıya alma, durdurma veya iptal işlemleri başlatılması, idari yaptırım uygulanması veya suç şüphesi bulunması hâlinde ilgili adli mercilere bildirimde bulunulması hususlarını değerlendirerek Başkana sunar.

(4) Komisyon gerekli gördüğü hallerde bulguların niteliğine göre ilgili birimlerin, uzmanların veya teknik çalışma gruplarının görüşüne başvurabilir. Alınan görüşler, Komisyonun değerlendirmesinde dikkate alınır ve değerlendirme gerekçesinde belirtilir.

(5) Komisyonun çalışma usul ve esasları Başkanlıkça belirlenir.

Denetim yetkisi ve nezaret usulü

MADDE 7– (1) Başkanlıkça yürütülecek denetimler; Başkanlık personeli ile yetkilendirilmiş bağımsız denetçiler veya bağımsız denetim kuruluşları tarafından yürütülür. Denetim yetkisi Başkan tarafından görevlendirilenler tarafından kullanılır.

(2) Kamu kurum ve kuruluşları ile kritik altyapılarda Başkanlıkça yürütülecek denetimlerin bağımsız denetçiler veya bağımsız denetim kuruluşları aracılığıyla gerçekleştirilmesi hâlinde, denetimler Başkanlık personelinin refakatinde yürütülür.

(3) Başkanlık refakatini gerektiren denetimlerde yürütülecek usul ve esaslar Başkanlıkça belirlenir.

Denetçinin yetkileri

MADDE 8- (1) Denetçi, yürüttüğü denetimin amacı ve kapsamı ile sınırlı olmak üzere görevini ifa ederken;

a) Denetlenen tarafın idari merkezlerine, tesislerine ve tüm eklentilerine doğrudan giriş yapmaya veya denetimi uzaktan erişim yöntemleriyle gerçekleştirmeye,

b) Denetlenen tarafa ait her türlü basılı ve elektronik belgeyi, bilgi sistemlerinde işlenen veya saklanan verileri ve kayıt (log) dosyalarını, bilgi ve iletişim ağlarını ve bunlara ait topoloji ve yapılandırma bilgilerini, kaynak kodları ile veri tabanı yapılarını, bilgi teknolojileri (BT) ve operasyonel teknoloji (OT) bileşenlerini ve bunlara ilişkin tesisler ve işletim süreçlerini, ilgili mevzuata konu faaliyetler kapsamında kullanılan dijital altyapıları ve bileşenleri incelemeye,

c) Denetlenen taraftan, belirlenen usul ve takvim çerçevesinde; sözlü veya yazılı açıklama ile her türlü bilgi ve belgenin teslim edilmesi ve/veya gönderilmesini istemeye,

ç) Denetim esnasında ilgili her türlü personelin yazılı veya sözlü beyanına başvurmaya,

d) Dijital veriler dâhil her türlü bilgi, belge, donanım ve cihazın incelenmesi neticesinde, tutanak düzenlemek suretiyle bunlardan suret veya numune almaya, denetlenen tarafın imzadan imtina etmesi durumunda bu şerhi tutanağa işlemeye,

e) Denetim süresince denetimin engellenmesi ya da delil karartma şüphesi durumunda kamu kurumlarından veya kolluk kuvvetlerinden iş birliği, kolaylık ve teknik yardım talebinde bulunmaya,

f) Göreviyle ilgili olarak diğer kamu kurumları ile tüm gerçek veya tüzel kişilerden gerekli bilgi ve belgeleri istemeye,

g) Canlı sistemler üzerinde hizmetleri kesintiye uğratmadan aktif veya pasif denetim ve inceleme faaliyetleri yürütmeye,

ğ) Denetim sırasında toplanan dijital delillerin ve log kayıtlarının uluslararası standartlara uygun olarak bütünlüğünü sağlayarak saklamaya yetkilidir.

Denetçinin yükümlülükleri

MADDE 9- (1) Denetçi, faaliyetlerini yürütürken;

a) Denetim etik ilkeleri çerçevesinde tarafsızlık, dürüstlük, şeffaflık ve kamu yararını gözetmeyi rehber edinir; hesap verebilirlik çerçevesinde hareket eder.

b) Uygulama, mevzuat ve denetim tekniklerindeki güncel gelişmeler ışığında mesleki bilgi ve becerisini sürekli geliştirir ve denetim faaliyetlerini gerekli mesleki özen ve dikkat içinde yürütür.

c) Denetimin kapsamını, amacını ve denetçi bilgisini içeren resmi görevlendirme belgesini beraberinde bulundurur.

ç) İncelediği kayıt ve belgelerin aslına müdahale etmez; donanım ve cihazların fiziksel veya yazılımsal durumunu korur.

d) Denetlenen tarafın operasyonel süreçlerine, yönetim kararlarına veya yürütme işlerine müdahale edemez.

e) Denetim sırasında elde edilen bilgilerin gizliliğine riayet eder. Söz konusu bilgilerin açıklanması için yasal veya mesleki bir hak veya görevin bulunması durumu saklı olmak kaydıyla, uygun ve belirli bir yetki olmaksızın bu tür bilgileri üçüncü kişilere açıklayamaz ve kendisi veya üçüncü kişilerin çıkarlarına kullanamaz.

f) Denetim konusu dışında kalan ancak mevzuata aykırı olduğu görülen durumların tespiti halinde gecikmeksizin Başkanlığa yazılı olarak bildirir.

g) Denetimin tarafsızlığını etkileyebilecek bir durumun bulunması hâlinde gecikmeksizin Başkanlığa yazılı olarak bildirir.

ğ) Denetim çalışmaları sırasında kurum veya kuruluşları olumsuz yönde etkileyebilecek hususlar ve bu yönetmeliğin 22 nci maddesinin birinci fıkrasında belirtilen acil durumların tespiti halinde, denetim çalışmalarının sonuçlanmasını beklemeksizin güvenli iletişim kanallarıyla Başkanlığı bilgilendirir.

Denetlenen tarafın görev ve sorumlulukları

MADDE 10- (1) Denetlenen tarafın görev ve sorumlulukları şunlardır:

a) Denetimin etkinliği adına yetkili temsilcilerin katılımını koordine etmek ve denetim heyetine uygun bir çalışma ortamı tesis etmek.

b) Denetim kapsamındaki tüm bilgi, belge ve beyanları; ticari sır veya gizlilik kısıtlaması olmaksızın, şeffaflık ilkesine uygun olarak, yazılı ve/veya sözlü olarak doğru ve eksiksiz bir şekilde belirlenen yöntem ve sürelere uygun olarak vermek ve yanıltıcı nitelikte beyanda bulunmamak.

c) İşletmeye ait fiziksel mekanlar ile dijital altyapının (yazılım ve/veya donanım) denetim kapsamında bilgi güvenliği ve siber olaylara müdahale gereklilikleri saklı kalmak kaydıyla erişimine açık tutulmasını sağlamak; denetim kapsamında talep edildiğinde söz konusu yer ve/veya sistemlerin çevrim içi ve/veya çevrim dışı erişimine ve uzaktan denetimin sağlıklı bir şekilde yürütülmesine imkân tanıyacak gerekli tüm altyapıyı sağlamak ve sistemleri denetim süresince çalışır vaziyette bulundurmak.

ç) Denetim ekibine gerekli kolaylığı sağlamak, denetimin sağlıklı yürütülmesini engelleyici davranışlardan kaçınmak.

(2) Denetlenen taraf denetimin konusu ve kapsamı hakkında bilgilendirilme, denetim sürecinde açıklama yapma, taslak denetim raporuna ilişkin görüş bildirme, sunulan bilgi ve belgelerin gizliliğinin korunmasını isteme ve ilgili mevzuat çerçevesinde itiraz ve başvuru haklarını kullanma haklarına sahiptir.

(3) Denetlenen taraf denetim sonucunda tespit edilen hususların giderilmesine yönelik gerekli işlemleri yerine getirmek ve Başkanlık tarafından talep edilen düzeltici faaliyetleri gerçekleştirmekle ve Başkanlığa bildirmekle yükümlüdür.

(4) Kanunlarla özel olarak korunması öngörülen bilgi ve belgelerin paylaşımında ilgili kanun hükümleri saklıdır.

Kurum ve kuruluşların denetim ve gözetim yükümlülükleri

MADDE 11- (1) Bu Yönetmelik kapsamındaki kurum ve kuruluşlar;

a) Başkanlığın ilgili mevzuatına uyumu sağlamak ve denetlemek üzere sorumlu birim veya birimleri görevlendirir.

b) Sorumlu birimlerin yürüteceği görevleri yerine getirebilmesi amacı ile ihtiyaç duyulan personeli ve gerekli görülen diğer kaynakları tahsis eder.

c) Başkanlığın ilgili mevzuatına uyum çalışmalarını yürütür, denetim ve gözetim yükümlülüklerini yerine getirir.

ç) Gözetim platformunda yetkilendirilecek temsilcileri belirler, Başkanlıkça talep edilen bilgilerin istenilen formatta ve periyotta paylaşılmasını sağlar.

(2) Kurum ve kuruluşlara uygulanacak denetim ve gözetim yöntemleri, raporlama, bildirim, denetim ve gözetim yükümlülükleri Başkanlıkça belirlenir.

(3) Sektörel SOME konumundaki kurum ve kuruluşlar denetim ve gözetim yükümlülüklerini Başkanlığın ilgili mevzuatına göre yürütür.

ÜÇÜNCÜ BÖLÜM
Denetim ve Gözetime İlişkin Uygulama Esasları

Denetim ve gözetim yaklaşımı

MADDE 12- (1) Denetim ve gözetim faaliyetleri katmanlı bir yapı içerisinde;

a) Kurum ve kuruluşların gözetim platformu üzerinden Başkanlığın ilgili mevzuatındaki yükümlülüklerine ilişkin uyum durumlarını öz değerlendirme usulüyle beyan etmesi ve Başkanlığın bu veriler üzerinden gözetim faaliyetlerini yürütmesi,

b) Kurum ve kuruluşların iç denetim birimleri veya ilgili kurum bünyesindeki ilgili yetkin birimlerince öz denetimini gerçekleştirmesi, denetim sonuçlarını Başkanlığa bildirmesi ve Başkanlığın bu sonuçlar ile kendisine sunulan diğer bilgi ve veriler üzerinden gözetim faaliyetlerini yürütmesi,

c) Başkanlıkça belirlenecek usul ve esaslara göre bağımsız denetim kuruluşları ve bağımsız denetçilerin kullanılması,

ç) Başkanlığın kendi öz kaynakları ile denetim, inceleme ve gözetim faaliyetlerini gerçekleştirmesi,

şeklinde uygulanır.

(2) Denetim ve gözetim faaliyetleri sonucunda elde edilen bilgi, bulgu ve değerlendirmeler, kurum ve kuruluşların Başkanlıkça belirlenen yükümlülüklere uyum seviyesinin belirlenmesi amacıyla kullanılır.

(3) Başkanlık kurum ve kuruluşların risk ve kritiklik düzeyleri, geçmiş denetim ve gözetim kayıtlarını dikkate alarak ilave doğrulama, gözetim, inceleme veya denetim faaliyetleri gerçekleştirilebilir.

(4) Başkanlık birinci fıkrada sayılan denetim ve gözetim yöntemlerini risk odaklılık ve orantılılık ilkeleri çerçevesinde ayrı ayrı, karma veya kademeli olarak uygulayabilir.

Denetimin temel ilkeleri

MADDE 13- (1) Denetim faaliyetleri hukuka uygunluk, tarafsızlık ve bağımsızlık, risk odaklılık, objektiflik, ölçülülük, şeffaflık, eşitlik ve hesap verebilirlik temel ilkeleri çerçevesinde yürütülür.

(2) Denetimler, denetlenen tarafın sunduğu hizmetlerin sürekliliği gözetilerek yürütülür; hizmetlerin kesintiye uğramaması esastır.

(3) Denetim sırasında elde edilen bilgi, belge, veri ve diğer kayıtlar ilgili mevzuat hükümleri saklı kalmak kaydıyla gizli tutulur.

(2) Denetim

MADDE 14– (1) Denetim, Kanun kapsamına giren her türlü fiil ve işlemin belirlenmiş bir ölçüte uyumlu olup olmadığı hususunda makul güvence sağlayacak bir görüş oluşturulması amacı ile yapılır.

(2) Başkanlık, denetimin etkinliğinin, sürekliliğinin, yeterliliğinin ve denetim kaynaklarının etkin kullanımının sağlanması amacı ile risk odaklı bakış açısına sahip dinamik bir yaklaşımla denetim yapar.

(3) Denetim; denetimin konusu hakkında, mesleki etik ilkelere bağlı kalmak ve mesleki şüphecilik içinde bulunmak suretiyle, yeterli ve uygun denetim kanıtı toplanmasını, bu kanıtlara dayandırılarak bir görüş oluşturulmasını ve görüşün raporlanmasını kapsar.

(4) Denetimin unsurlarını; denetimin konusu, tarafları, ölçütü, kanıtları ve denetim raporu oluşturur.

(5) Denetim sonucunda tespit edilen bulgular risk dereceleri esas alınarak mevzuata aykırılık, güvenlik zafiyeti, kontrol eksikliği ve iyileştirmeye açık hususlar şeklinde sınıflandırılabilir.

(6) Denetim sırasında yapılan tüm işlemler, denetçiler tarafından düzenlenecek tutanağa bağlanır. Tutanakta; denetimin tarihi, konusu, dayanağı, denetçiler ve denetlenenin yasal temsilcileri, denetime katılanlar, incelenen belge, veri ve sistemler, yürütülen testler ve erişim kayıtları, alınan kopya veya örnekler ile varsa itiraz ve beyanlar yer alır. Düzenlenen tutanak, denetim ekibi ile denetlenen kurum veya kuruluşun imza yetkisine sahip temsilcisi tarafından imzalanır. Denetlenen tarafın tutanağı imzalamaktan imtina etmesi hâlinde bu durum tutanağa şerh düşülerek imza altına alınır.

(7) Denetlenen tarafın sistemlerine uzaktan erişim sağlanmasının gerekli olduğu hallerde; erişimler denetimin amacı ve kapsamı için gerekli asgari yetki seviyesiyle, denetlenen tarafın yetkili personelinin gözetiminde ve tüm oturum hareketleri kayıt altına alınarak gerçekleştirilir. Elektronik ortamda sunulan bilgi, belge ve doğrulama verileri denetim kanıtı olarak kabul edilir ve denetim kanıtı başlıklı madde hükümlerine göre muhafaza edilir.

(8) Denetim sonucunda gerekli görülmesi hâlinde takip denetimi yapılabilir veya diğer idari süreçler başlatılabilir.

(9) Denetim sonucunda tespit edilen bulgular, Başkanlık tarafından denetlenen tarafa bildirilir; gerekli görülen hâllerde düzeltici tedbirlerin alınması istenebilir. Bu durumda denetlenen taraf bulgulara ilişkin düzeltici faaliyet planını ve takvimini Başkanlığa göndermekle yükümlüdür.

(10) Denetim faaliyetlerinin kapsamı, yöntemi, süresi, bulguların sınıflandırılması, raporlanması, düzeltici faaliyetlerin izlenmesi ile ilgili usul ve esaslar Başkanlıkça belirlenir.

(11) Denetim uzaktan veya yerinde icra edilebilir.

(12) Uzaktan denetim faaliyeti yürütülmekte olan denetim faaliyetlerinin; denetlenen taraf yetkilileri ile toplantıların gerçekleştirilmesi, denetime konu bilgi, belge ve verilerin alınması ve denetlenen tarafa ait sanal veya fiziki ortamların denetlenmesi dâhil diğer tüm denetim

aşamalarının tamamının veya bir kısmının denetçi tarafından teknolojik araçlar ve bilgi teknolojileri vasıtasıyla uzaktan gerçekleştirilmesi şeklinde yürütülür.

Denetim türleri

MADDE 15- (1) Başkanlık denetim faaliyetlerini re'sen, yıllık denetim programı kapsamında ve program dışı olarak yürütebilir.

(2) Denetim programı, Başkanlık tarafından belirlenen risk değerlendirme ölçütleri ve önceliklendirme esasları çerçevesinde hazırlanır.

(3) Denetim programı Başkan tarafından onaylanır; gerekli görülmesi hâlinde yıl içinde değişiklik yapılabilir.

(4) Program dışı denetimler; Başkanlıkça gerekli görülen hallerde Başkanın onayıyla re'sen yapılır.

(5) Başkanlık; yıllık denetim programı kapsamında veya program dışı olarak, belirli bir konuya, sektöre, teknolojik altyapıya veya risk alanına yönelik özel kapsamlı denetimler planlayabilir ve yürütebilir.

Denetim ekibinin oluşturulması

MADDE 16- (1) Denetimler, Başkan tarafından görevlendirilen denetim ekibi tarafından yürütülür.

(2) Denetim ekibi, denetlenecek konu ve kurumların özellikleri ile uzmanlık ihtiyacı dikkate alınarak oluşturulur.

(3) Denetim ekibi, bir denetim sorumlusu ile yeterli sayıda denetçiden oluşur.

(4) Denetimin kapsamı ve niteliği dikkate alınarak teknik, idari veya hukuki uzmanlık gerektiren hallerde Başkanlığın ilgili birimlerinden personel ile Başkanlıkça uzman veya bilirkişi denetim ekibinde görevlendirilebilir.

(5) Denetimin tarafsızlığını etkileyebilecek hâlleri bulunan kişiler ilgili denetimde görevlendirilemez.

Denetim ölçütü

MADDE 17– (1) Denetimlerde, uygunluğun değerlendirilmesine esas teşkil eden önceden belirlenmiş denetim ölçütleri kullanılır.

(2) Denetim ölçütleri;

a) Başkanlıkça yayımlanan ilgili mevzuatta düzenlenen yükümlülükler ve teknik uygulama usul ve esasları ile bu konudaki rehber ve teknik düzenlemeler,

b) Kuruluşun faaliyet alanı, bilgi varlıklarının ve bilgi ve iletişim teknolojileri altyapısının kritiklik düzeyi, riskleri ve maruz kaldığı tehditler,

c) Başkanlıkça gözetilecek diğer hususlar,

esas alınarak Başkanlıkça belirlenir.

(3) Denetim ölçütlerinin uygulanabilirliği ile denetlenen tarafın aldığı tedbirlerin yeterliliği değerlendirilirken, riskin niteliği, muhtemel etkisi, faaliyetlerinin kritiklik düzeyi ve tabi olduğu sektörel düzenlemeler göz önünde bulundurulur.

(4) Denetim ölçütlerinde; uygulanacak kontrol ve test yöntemleri, değerlendirme kriterleri, kanıt gereklilikleri, bulgu sınıflandırması, risk değerlendirmesi, olgunluk seviyeleri ve raporlama esasları düzenlenebilir.

(5) Teknolojik gelişmeler, tehdit ortamındaki değişimler ve ulusal siber güvenlik ihtiyaçları dikkate alınarak, ilgili mevzuatla belirlenen yükümlülükler saklı kalmak kaydıyla, denetimlerde kullanılacak teknik ve uygulamaya ilişkin ölçütler Başkanlıkça güncellenebilir.

Denetim kanıtı

MADDE 18– (1) Denetim kanıtı, denetim ölçütlerine göre uyumun değerlendirilmesi ve makul güvence oluşturulması amacıyla denetim kapsamında elde edilen yeterli ve uygun bilgi, belge ve beyanlardır. Denetim kanıtları, mesleki şüphecilik ilkesi gözetilerek elde edilir.

(2) Denetim bulguları yeterli, ilgili, güvenilir ve doğrulanabilir kanıtlara dayanır. Kanıtların elde edilmesi ve değerlendirilmesine ilişkin usul ve esaslar Başkanlıkça belirlenir.

(3) Denetim kapsamında elde edilen kanıtların bütünlüğü ve izlenebilirliği korunur.

(4) Kanıtların elde edilmesi, taşınması, saklanması ve kullanılması sırasında gizlilik ile kişisel verilerin korunmasına ilişkin mevzuat hükümlerine uyulur.

Denetim raporu

MADDE 19– (1) Denetim raporu, denetim kapsamında elde edilen denetim kanıtlarının değerlendirilmesi sonucunda ulaşılan bulgu, tespit ve sonuçların yer aldığı; denetim konusunun denetim ölçütlerine uygunluğu hakkındaki denetçi görüşünü içeren Başkanlık düzenlemelerine uygun olarak hazırlanan ve imzalanan yazılı belgedir.

(2) Denetim sonucunda taslak denetim raporu hazırlanır.

(3) Taslak raporda tespit edilen bulgular ile bunlara ilişkin değerlendirmelere yer verilir.

(4) Denetim ekibi tarafından hazırlanan taslak denetim raporları kalite güvence sürecine tabi tutulur.

(5) Taslak rapordaki bulgular denetlenen tarafa yazılı olarak bildirilir. Denetlenen taraf bulgulara ilişkin yazılı savunmasını bildirimin alındığı tarihten itibaren otuz gün içinde Başkanlığa iletir.

(6) Denetlenen tarafın yazılı savunması denetim ekibince değerlendirilir.

(7) Denetim ekibi, yeni bilgi ve belgeler sunulması halinde veya itiraz ve eleştirileri yerinde bulduğu durumlarda denetim raporunu güncelleyebilir.

(8) Denetim, nihai denetim raporunun tamamlanmasıyla sona erer.

(9) Nihai denetim raporu, denetim sonucunda elde edilen bulguların teknik, idari ve hukuki boyutlarıyla ele alınması ve uygulanacak yaptırımların değerlendirilmesi amacıyla Denetim ve Yaptırım Değerlendirme Komisyonuna sunulur.

(10) Denetimin raporlanması aşamasına ilişkin diğer hususlar Başkanlık tarafından belirlenir.

Kalite güvence sistemi

MADDE 20- (1) Başkanlık denetim faaliyetlerinin belirlenen usul, esas ve standartlara uygun, etkin ve tutarlı şekilde yürütülmesini sağlamak amacıyla kalite güvence sistemini kurar ve işletir.

(2) Kalite güvence sistemi kapsamında; denetim faaliyetlerinin planlanması, yürütülmesi, sonuçlandırılması ve raporlanması aşamalarının kalite yönünden izlenmesi ve değerlendirilmesi, denetim dosyalarının ve raporlarının incelenmesi, uygulama birliğinin değerlendirilmesi, dönemsel gözden geçirmelerin yapılması, tespit edilen eksiklik ve geliştirme alanlarına yönelik gerekli iyileştirme faaliyetlerinin yürütülmesi sağlanır.

(3) Sektörel SOME' ler, denetim hizmet sağlayıcıları, bağımsız denetim kuruluşları ve bağımsız denetçiler, denetim ve gözetim faaliyetlerini gerçekleştirirken belirlenen kalite standartlarını esas alır.

(4) Sektörel SOME' lerin, denetim hizmet sağlayıcıların, bağımsız denetim kuruluşları ve bağımsız denetçilerin denetim ve gözetim faaliyetleri, kalite güvence sistemi kapsamında izlenir ve değerlendirilir.

(5) Kalite güvence sistemi ile kalite standartlarının uygulanmasına ilişkin usul ve esaslar Başkanlıkça belirlenir.

İnceleme

MADDE 21– (1) Başkanlık, Kurum ve kuruluşların ilgili Başkanlık mevzuatına ve standartlara uygunluğu hakkında sınırlı güvence sağlayan ve geliştirme önerileri içeren inceleme faaliyeti yürütebilir.

(2) İnceleme faaliyetinde ağırlıklı olarak beyan yöntemi, mülakatlar, analitik değerlendirmeler, otomatik tarama araçları ve sınırlı örnekleme teknikleri kullanılarak değerlendirme gerçekleştirilebilir.

(3) Başkanlık, resen ya da ihbar veya şikâyet üzerine inceleme başlatılmasına karar verebilir.

(4) İnceleme faaliyetlerinde denetçi görevlendirilmesinde 16 ncı madde hükümleri uygulanır.

(5) Yapılan inceleme neticesinde denetçi inceleme raporunu hazırlar.

(6) İnceleme raporunun değerlendirilmesi sonucunda denetim süreçleri başlatılabilir.

(7) Başkanlık denetim süreçlerinde mahallinde inceleme yapabilir veya yaptırabilir. Mahallinde inceleme faaliyeti yerinde denetim şeklinde işletilir. Mahallinde incelemeye tabi tutulanların yükümlülükleri ile mahallinde inceleme ile görevlendirilen personelin yetki ve yükümlülüklerinde 8 inci, 9 uncu ve 10 uncu madde hükümleri uygulanır.

Acil durumlar

MADDE 22– (1) Denetim ve inceleme faaliyetleri sırasında millî güvenliği, kamu düzenini, kamu sağlığını, kritik altyapıların işleyişini etkileyen veya ulusal siber güvenlik açısından tehlike veya ciddi risk oluşturduğu değerlendirilen bir durumun tespit edilmesi hâlinde, Başkanlık riskin niteliğini ve muhtemel etkilerini değerlendirerek bu maddenin ikinci ila beşinci fıkralarında belirtilen tedbirleri uygulayabilir.

(2) Başkanlık, riskin niteliğini değerlendirerek tehlikenin bertaraf edilmesi veya etkilerinin azaltılması amacıyla beklemeksizin müdahalede bulunabilir.

(3) Başkanlık gerekli siber güvenlik tedbirlerinin derhal ve öncelikle alınmasını ilgili kurum veya kuruluşa bildirir. İlgili kurum, bildirilen tedbirleri gecikmeksizin uygulamakla yükümlüdür.

(4) İlgili kurum tarafından gerekli tedbirlerin alınmaması veya gecikilmesi hâlinde, ya da bu tedbirlerin alınması halinde dahi sonuç alınamayacağının veya Başkanlığın müdahalesinin elzem olduğunun belirlenmesi durumunda doğabilecek zararların önlenmesi amacıyla Başkanlıkça ilgili mevzuat çerçevesinde geçici idari ve teknik kısıtlama tedbirleri uygulanabilir veya uygulanması sağlanır.

(5) Tespit edilen durumun sektörel veya ulusal ölçekte siber krize dönüşme riski taşıdığının değerlendirilmesi hâlinde, Başkanlığın ilgili siber olay ve kriz yönetimi mekanizmaları derhal devreye alınır. Bu durumda denetim faaliyetinin devamına, kapsamının değiştirilmesine veya geçici olarak durdurulmasına Başkanlıkça karar verilir.

Denetimin engellenmesi

MADDE 23- (1) Aşağıdaki fiil ve davranışlar denetimin engellenmesi olarak kabul edilir:

a) Denetim ekibinin binalara, veri merkezlerine, sistem odalarına veya inceleme sahalarına girişinin engellenmesi veya geciktirilmesi,

b) Denetim kapsamında talep edilen bilgi, belge, sistem kaydı (log), trafik verisi, konfigürasyon dökümü veya numunelerin verilmemesi, geç verilmesi, tahrif edilmesi veya gerçeğe aykırı sunulması,

c) Denetim için gerekli kullanıcı erişim haklarının, ağ erişimlerinin veya teknik inceleme imkanlarının tanınmaması veya kısıtlanması,

ç) Denetim ekibine karşı fiziki, psikolojik baskı uygulanması veya görevlerini yapmalarının fiilen zorlaştırılması.

d) Herhangi bir suretle denetim faaliyetinin yerine getirilmesinin engellenmesi.

(2) Denetim esnasında engelleme, fiziki veya teknik mukavemet, cebir veya tehdit ile karşılaşılması ya da delillerin karartılması riskinin bulunması hâlinde; durum denetim ekibince engellemenin niteliğini, zamanını ve sorumlularını içeren tutanak tanzim edilerek derhal işlem yapılır. Kanunun 16' ncı maddesi uyarınca gerekli idari ve/veya adli işlemlerin tesis edilmesi amacıyla tutanak ve ilgili belgelerle Başkanlığa bildirilir. Gerekli görülmesi hâlinde denetimin icrası için kolluk kuvveti refakati talep edilir.

Takip denetimi

MADDE 24– (1) Başkanlık düzeltici faaliyetlerin yerine getirilip getirilmediğinin tespiti amacıyla denetim raporuna istinaden gerek gördüğünde takip denetimi yapabilir veya bağımsız denetim kuruluşları ile bağımsız denetçilere yaptırabilir.

(2) Takip denetimi yalnızca bulgularla sınırlı olarak gerçekleştirilebileceği gibi gerekli görülmesi hâlinde denetimin tamamını da kapsayabilir.

(3) Takip denetiminde önceki denetim sonuçları esas alınır.

(4) Takip denetimi sonucunda; düzeltici faaliyetlerin süresi içinde yerine getirilmediğinin veya bulguların giderilmediğinin tespiti hâlinde haklı ve kabul edilebilir bir gerekçe sunulması halinde ek süre verilebilir.

(5) Takip denetimi sonucunda; haklı ve kabul edilebilir bir gerekçe olmaksızın düzeltici faaliyetlerin süresi içinde yerine getirilmediğinin veya bulguların giderilmediğinin tespiti hâlinde, Kanunun ilgili hükümleri uyarınca idari yaptırımlar tatbik edilir.

Öz değerlendirme

MADDE 25- (1) Kurum ve kuruluşların Başkanlığın ilgili mevzuatında belirlenen yükümlülüklerine uyum durumunu belirlemek, eksiklikleri tespit etmek ve düzeltici faaliyetleri planlamak amacıyla öz değerlendirme yöntemi kullanılabilir.

(2) Öz değerlendirme Başkanlıkça belirlenen usul, esas ve ölçütler çerçevesinde gerçekleştirilir.

(3) Öz değerlendirme sonuçları, gerekli kanıt ve kayıtlarla birlikte Başkanlığa belirlenen usul ve esaslar çerçevesinde bildirilir veya erişilebilir hale getirilir.

(4) Öz değerlendirme sonuçları, kurum ve kuruluşların mevzuata uyumuna ilişkin bağımsız ve tarafsız güvence sağladığı şeklinde değerlendirilemez.

(5) Öz değerlendirme kapsamında tespit edilen eksikliklerin giderilmesinden kurum ve kuruluşlar sorumludur.

Öz denetim

MADDE 26– (1) Kurum ve kuruluşlar; usul, esas ve periyotları Başkanlıkça belirlenen öz denetimlerin yapılmasını, bu denetimlerin etkin bir şekilde yürütülmesi için gerekli her türlü teknik, idari ve lojistik desteğin sağlanmasını ve denetim sonuçlarının Başkanlığa raporlanmasını sağlamakla yükümlüdür.

(2) Öz denetimler iç tetkik veya iç denetim usulü ile yapılabilir.

(3) Kurum ve kuruluşlar öz denetimi iç kaynakları ile yürütmek için gerekli bütçe, personel, eğitim vb. gereksinimlere yönelik planlamalarını yapmalıdır.

(4) Kurum ve kuruluşlar, öz denetim ekibini en az iki denetçi ve ihtiyaç duyulan sayıda uzman personelden teşkil eder.

(5) Öz denetim ekibinde görevlendirilecek personelin; iç tetkik, iç denetim veya bilgi sistemleri denetimi alanlarından en az birinde deneyim sahibi olması, denetim yapacağı ilgili faaliyet alanında bilgi ve deneyime sahip olması ve Başkanlıkça belirlenen yetkinlik kriterlerini

sağlaması zorunludur. Denetim ekibi, denetlenecek sistemlerin teknolojik yapısına uygun teknik uzmanlığı kapsayacak şekilde oluşturulur.

(6) Öz denetimler için oluşturulacak denetim ekibi, denetimin tarafsızlığını ve bağımsızlığını sağlamak amacıyla uyum faaliyetlerinde yer almayan personelden teşkil edilmelidir.

(7) Kritik altyapıya sahip kurum ve kuruluşlarda öz denetim faaliyetlerinin öncelikli olarak iç denetim birimlerinde görev alan ve bilgi teknolojileri alanında denetim yapmak üzere görevlendirilen iç denetçiler tarafından gerçekleştirilmesi esastır.

(8) İç denetim birimlerinin bulunmadığı ya da iç denetim birimi olmasına rağmen öz denetimi yürütecek yeterlik ve yetkinlikte kurum denetçisine sahip olunmadığı hallerde denetim faaliyetlerinin bağımsız bir şekilde yürütülmesini sağlamak üzere kurum içi diğer personel, kamu kurumları için diğer kamu kurumlarından görevlendirilen personel kullanılarak öz denetim faaliyeti gerçekleştirilebilir.

(9) Kurum ve kuruluşlar öz denetime ilişkin sonuçları denetimin tamamlandığı tarihten itibaren iki ay içerisinde, öz denetimini takvim yılı sonuna kadar tamamlamadığı takdirde mevcut durumunu takip eden yılın ikinci ayı sonuna kadar Başkanlıkça belirlenen usul ve esaslara göre Başkanlığa bildirir.

Denetimlerde hizmet alım usulünün kullanılması

MADDE 27– (1) Bu Yönetmeliğin 26 ncı maddesinin yedinci ve sekizinci fıkralarında belirtilen şekilde öz denetimin gerçekleştirilememesi hâlinde veya ek güvence gereksinimi nedeniyle, kurum ve kuruluşlar öz denetim faaliyetlerini hizmet alımı yoluyla, Başkanlıkça yetkilendirilmiş denetim hizmet sağlayıcılara yaptırabilir. Bu kapsamda gerçekleştirilen faaliyetler öz denetim olarak değerlendirilir.

(2) Sektörel SOME'ler ilgili mevzuata binaen denetim yükümlülüklerini iç kaynakları ile gerçekleştirememesi hâlinde veya ek güvence gereksinimi nedeniyle, Başkanlıkça yetkilendirilmiş denetim hizmet sağlayıcılarını denetim faaliyetlerinde kullanabilir. Bu kapsamda gerçekleştirilen faaliyetler sektörel denetim olarak değerlendirilir.

(3) Hizmet alım usulünün kullanılması durumu Başkanlığa bildirilir ve aşağıdaki usul ve esaslara uyulur:

a) Denetim, denetlenecek konuya ilişkin olarak denetim tarihinden önceki iki yıl içinde ilgili kurum veya kuruluşa danışmanlık veya uyum hizmeti sunmuş olan hizmet sağlayıcıya yaptırılamaz.

b) Aynı hizmet sağlayıcı ile birbirini izleyen ikiden fazla denetim dönemi için sözleşme imzalanamaz.

c) Hizmet alımına ilişkin sözleşmelerde asgari olarak denetimin amacı, kapsamı, sözleşmenin feshine ilişkin şartlar, tedarikçi güvenliği hususları, gizlilik hükümleri ve hizmet sağlayıcının sorumlulukları, denetim kapsamında üretilecek belgeler, bunların biçim ve içerikleri, denetçilerin sahip olması gereken uzmanlık alanlarına yer verilir.

ç) Denetim faaliyetlerinde öncelikle denetlenen kurum veya kuruluşa ait kurumsal cihaz, yazılım, donanım ve diğer teknik imkânların kullanılması ve denetlenen kurum veya kuruluşun bilgi sistemlerinin güvenliği, gizliliği ve sürekliliği üzerinde olumsuz etki oluşturulmaması esastır.

d) Denetim faaliyetlerinin bağımsızlığını, tarafsızlığını veya sonuçların güvenilirliğini olumsuz etkileyebilecek faaliyetlerde bulunulamaz.

e) Denetim hizmet sağlayıcıları hazırladığı raporları hizmet sözleşmesi imzaladığı taraflara sunar.

(4) Hizmet alım usulünün kullanılması durumunda kurum ve kuruluşlar sonraki denetim döneminde 26 ncı maddenin üçüncü fıkrası uyarınca gerekli çalışmaları planlar ve uygular.

(5) Denetim hizmet sağlayıcıların taşıması gereken asgari nitelikler, yetkilendirme ve belgelendirme esasları Başkanlık tarafından belirlenir.

Bağımsız denetim kuruluşları ve bağımsız denetçilerin kullanılması

MADDE 28- (1) Başkanlık yürüttüğü denetim faaliyetlerinde bağımsız denetim kuruluşları ve bağımsız denetçileri görevlendirilebilir. Bu durumda bağımsız denetim kuruluşları ve bağımsız denetçiler Başkanlığın denetim yetkisini kullanır. Hazırladıkları denetim raporlarını Başkanlığa iletir.

(2) Bağımsız denetim kuruluşu, aynı denetim döneminde denetlenen taraf nezdinde de aktif görev almışsa, bu durum çıkar çatışması sayılır ve söz konusu denetim kuruluşu bu durumda görevlendirilemez.

(3) Bağımsız denetim kuruluşu ve denetçiler, kurum ve kuruluşun denetim konusu sistemleri tasarımı, kurulumu, işletimi faaliyetlerinde doğrudan ya da dolaylı olarak son beş yıl içerisinde görev almamış olmalıdır.

(4) Bağımsız denetçi, tarafsızlığını ve bağımsızlığını yazılı bir "Bağımsızlık Beyanı" ile taahhüt etmek zorundadır.

(5) Bağımsız denetçi ve bağımsız denetim kuruluşlarının taşıması gereken nitelikler, başvuru usulü, yetkilendirme ve belgelendirme esasları Başkanlık tarafından belirlenir.

(6) Başkanlık bağımsız denetim kuruluşlarının denetim faaliyetlerini denetim ve gözetime tabi tutar, denetim kuruluşundan denetçilerin yetkinliğine ilişkin rapor isteyebilir, performans değerlendirmesi gerçekleştirebilir.

(7) Başkanlık, denetim kuruluşları ve denetçilere ilişkin gözetim sonuçları, kalite değerlendirmeleri, uygunsuzluklar, düzeltici faaliyetler ve diğer gözetim kayıtlarını elektronik ortamda tutabilir.

(8) Başkanlık, bağımsız denetçi ve denetim kuruluşlarının yetkisini, mevzuata aykırılık, görevin kötüye kullanılması veya yeterlilik kaybı hâllerinde süreli veya süresiz olarak iptal edebilir.

(9) Bu madde kapsamında gerçekleştirilen denetimlerde ve 27 nci madde kapsamındaki denetimlerde aşağıdaki ortak hükümler uygulanır.

a) Denetimi yürüten kuruluş veya denetçi ile denetlenen kurum veya kuruluş arasında denetimin bağımsızlığını, tarafsızlığını veya sonuçlarının güvenilirliğini etkileyebilecek ticari, mali veya mesleki ilişkiler bulunamaz. Bu nitelikte bir durumun denetim sürecinde ortaya çıkması hâlinde ilgili kuruluş veya denetçi durumu gecikmeksizin ilgili kuruma veya Başkanlığa bildirir ve denetimin bağımsızlığını korumaya yönelik gerekli tedbirleri alır.

b) Denetimi yürüten kuruluş veya denetçi, denetlenen kurum veya kuruluşun denetim konusu sistemlerinin tasarımı, kurulumu, işletimi faaliyetlerinde veya söz konusu yapıda çalışan ürünlerin tedarik sürecinde üstlendiği görevler nedeniyle kendi faaliyetlerini denetler duruma düşemez.

c) Denetimi yürüten kuruluş veya denetçi, denetim öncesinde bağımsızlığını ve tarafsızlığını etkileyebilecek durumları değerlendirir ve bağımsızlık beyanında bulunur.

d) Denetim faaliyetleri, Başkanlıkça belirlenen denetim kriterleri, usul ve esaslar, metodolojiler, raporlama ilkeleri ve formatları ile ilgili kalite güvence hükümlerine uygun olarak yürütülür.

e) Denetim kapsamında görevlendirilen kişilerin denetlenen konuya uygun bilgi, deneyim ve teknik yetkinliğe sahip olması zorunludur.

f) Denetim faaliyetleri sırasında denetlenen kurum veya kuruluşun bilgi sistemlerinin güvenliği, gizliliği ve sürekliliği korunur. Denetim faaliyetleri, denetlenen kurum veya kuruluşun faaliyetlerini gereksiz yere aksatmayacak şekilde yürütülür.

Gözetim

MADDE 29– (1) Başkanlık, tarafların ilgili mevzuata uyumunun izlenmesi, olgunluk seviyesinin ölçülmesi, risklerin belirlenmesi ve denetim faaliyetlerinin planlanmasına esas teşkil etmek üzere sürekli veya dönemsel gözetim faaliyetleri yürütebilir.

(2) Gözetim faaliyetlerinden elde edilen sonuçlar, gerektiğinde risk değerlendirmesinde ve denetim sürecinde kullanılabilir, denetim başlatılmasına dayanak oluşturabilir.

(3) Başkanlık denetim sonucunda alınan tedbirlerin etkinliğini sürekli gözetim faaliyetleri kapsamında izleyebilir.

(4) Başkanlık, gözetim faaliyetleri kapsamında;

a) Kurum ve kuruluşların ilgili mevzuat çerçevesinde yürüttükleri faaliyetlerin izlenmesi,

b) Gözetim platformundaki verilerin incelenmesi sonucu eksik ya da hatalı olan verinin kurum ve kuruluşlar tarafından düzeltilmesine yönelik bildirimlerin yapılması,

c) İletilen verilerle analizlerin gerçekleştirilmesi ve raporların hazırlanması,

ç) Tespit edilen eksikliklerin veya ilgili mevzuata aykırılık teşkil eden hususların ilgili kurum ve kuruluşlara bildirilmesi ve gerekli koordinasyonun sağlanması,

d) Gerçekleştirilen analizlerin sonuçlarını içeren periyodik değerlendirme raporlarının ilgili taraflarla paylaşılması

görevlerini yürütür.

(5) Gözetim yükümlülüğü bulunan Sektörel SOME'ler, kurum ve kuruluşlar, bağımsız denetim kuruluşları ve bağımsız denetçiler Başkanlıkça belirlenen usul ve esaslar doğrultusunda gözetim platformuna veri girmek üzere yetkilendirilebilir.

a) Gözetim platformunda yetkilendirilecek temsilcilerin nitelikleri Başkanlıkça belirlenir.

b) Gözetim platformunda yetkilendirilen temsilciler platformun güvenli kullanımına ilişkin Başkanlık tarafından belirlenen usullere uymakla yükümlüdür.

DÖRDÜNCÜ BÖLÜM
Bildirim ve Yaptırım Esasları

Adli ve idari makamlara bildirim ve başvuru

MADDE 30– (1) Başkanlık, yürüttüğü denetim, inceleme ve gözetim faaliyetleri kapsamında mevzuata aykırılık, idari yaptırım gerektiren fiil veya suç teşkil edebileceği değerlendirilen hususların tespiti halinde gerekli idari, hukuki ve adli süreçler başlatılabilir veya ilgili merciler nezdinde başlatılması sağlanabilir.

(2) Bu kapsamda Başkanlık, ilgili idari mercilere bildirimde bulunabilir, adli mercilere intikal işlemlerini gerçekleştirebilir ve gerekli takip süreçlerini yürütebilir.

Uygunsuzlukların değerlendirilmesi ve yaptırım süreçleri

MADDE 31– (1) Denetim, inceleme ve gözetim faaliyetleri sonucunda uygunsuzluk tespit edilmesi halinde, ilgili mevzuat ve Başkanlıkça belirlenen usul ve esaslar çerçevesinde gerekli idari, teknik ve hukuki süreçler işletilir.

(2) Birinci fıkra kapsamında tespit edilen hususlar, Komisyon tarafından uygunsuzluğun niteliği, etkisi, kritiklik düzeyi ve tekrar durumu dikkate alınarak değerlendirilir.

(3) Komisyon tarafından yapılan değerlendirme sonucunda;

a) Düzeltici faaliyetlerin uygulanması,

b) Teknik tedbirlerin alınması,

c) Yetkilendirme veya görevlendirme süreçlerine ilişkin askıya alma, durdurma veya iptal işlemlerinin başlatılması,

ç) İlgili mevzuat çerçevesinde idari yaptırım uygulanmasına yönelik işlem tesis edilmesi,

d) Suç şüphesi bulunması halinde ilgili adli mercilere bildirimde bulunulması,

e) Gerekli görülmesi halinde ilgili kurum ve kuruluşlar nezdinde ilave idari ve hukuki süreçlerin başlatılması,

hususlarında ilgili işlem süreçleri başlatılması değerlendirilerek Başkana sunulur.

(4) Tespit edilen uygunsuzluklar için öncelikle uyarı yapılır ve uygunsuzluğun giderilmesi amacıyla süre verilir.

(5) Verilen süre içerisinde uygunsuzlukların giderilmemesi veya aynı uygunsuzluğun tekrarı hâlinde, yaptırımlar uygulanabilir.

(6) Uygunsuzluğun, bilgi güvenliği ihlali, hizmet kesintisi veya ulusal güvenliği etkileyebilecek nitelikte olması hâlinde, ivedi tedbirler uygulanabilir ve süre verilmeden yaptırım tesis edilebilir.

(7) Bu Yönetmelik kapsamında uygulanacak idari yaptırımlar, ilgili mevzuatta öngörülen idari ve cezai sorumlulukların uygulanmasına engel teşkil etmez.

(8) Denetim raporu, ilgili mevzuat uyarınca yürütülecek idari süreçlerde dikkate alınabilir.

(9) Denetim ile idari yaptırım süreci birbirinden bağımsız olarak yürütülür; denetim sonucunda idari yaptırım uygulanmasını gerektirdiği değerlendirilen hususlar, ilgili mevzuat hükümleri çerçevesinde işlem tesis edilmek üzere Başkanlığa bildirilir.

(10) Denetim ve gözetim faaliyetleri sonucunda tespit edilen uygunsuzlukların giderilmesine yönelik düzeltici faaliyetlerin gerçekleştirilmesi, ilgili yükümlünün yaptırım sorumluluğunu ortadan kaldırmaz.

Savunma hakkı ve itiraz

MADDE 32– (1) Hakkında idari yaptırım uygulanması teklif edilen tarafa yaptırıma esas teşkil eden hususları içeren yazılı bildirim yapılır. İlgili, tebliğ tarihinden itibaren otuz (30) gün içinde yazılı savunmasını Başkanlığa sunar. Süresi içinde savunma verilmemesi hâlinde savunma hakkından feragat edilmiş sayılır.

(2) Bu Yönetmelik uyarınca verilen idari yaptırım kararlarına ve idari işlemlere karşı, 2577 sayılı İdari Yargılama Usulü Kanunu ve ilgili kanun hükümleri uyarınca idari yargı yoluna başvurulabilir. Dava açılmış olması, kararın uygulanmasını kendiliğinden durdurmaz. Ancak yetkili yargı mercii tarafından yürütmenin durdurulmasına karar verilmesi hâlinde kararın uygulanması durdurulur.

BEŞİNCİ BÖLÜM
Çeşitli ve Son Hükümler

Denetim ve gözetim verisinin işlenmesi

MADDE 33– (1) Başkanlık, denetim ve gözetim faaliyetlerinden elde edilen sonuçları mevzuatın geliştirilmesi, standart ve rehberlerin güncellenmesi, risk değerlendirme yöntemlerinin iyileştirilmesi, siber güvenlik olgunluk seviyesinin belirlenmesi ve siber güvenlik kapasitesinin artırılması amacıyla kullanabilir.

(2) Denetim ve gözetim sonuçlarından elde edilen istatistikler ve eğilimler anonimleştirilerek kamuoyu ile paylaşılabilir.

(3) Denetim ve gözetim faaliyetleri kapsamında elde edilen kişisel veriler; hukuka ve dürüstlük kurallarına uygun, doğru ve gerektiğinde güncel, belirli, açık ve meşru amaçlarla, işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmak ve işlendiği amaç için gerekli olan süre kadar muhafaza edilmek kaydıyla işlenir.

Düzenleme yetkisi

MADDE 34– (1) Başkanlık bu Yönetmeliğin uygulanmasına yönelik, yönerge, rehber, teknik kriter, metodoloji, standart form ve benzeri düzenleyici dokümanlar yayımlayabilir, ilke ve standartları belirleyebilir.

(2) Denetim, gözetim, inceleme, raporlama, değerlendirme ve diğer operasyonel süreçler Başkanlıkça belirlenen usul ve esaslar çerçevesinde yürütülür.

(3) Kurum ve kuruluşlardan beklenen iyi uygulamaları göstermek ve Başkanlık tarafından yapılan denetimde dikkate alınacak değerlendirme ölçütleri hakkında kurum ve kuruluşları bilgilendirmek amacıyla teknik uygulama rehberleri yayımlanabilir.

(4) Teknik uygulama rehberlerindeki ilkeler, kurum ve kuruluşların siber güvenlik yükümlülüklerini uygulamalarının etkinliğinin ve yeterliliğinin değerlendirilmesinde ölçüt olarak kullanılır ve denetim sırasında veya sonrasında denetim bulgularına ilişkin olarak Başkanlık tarafından yapılan değerlendirmelere ve alınan kararlara temel teşkil eder.

(5) Teknik uygulama rehberlerindeki ilkeler ölçülülük ilkesi çerçevesinde uygulanır.

Geçiş süreci

GEÇİCİ MADDE 1- (1) Bu Yönetmelik kapsamında uygulama esasının belirlenmesine ihtiyaç duyulan yükümlülükler, ilgili esasın yayımlanmasını müteakip uygulanır.

(2) İlgili uygulama esasının yayımlanmasına kadar, ilgili yükümlülüklerin uygulanmasında mevcut usul ve esaslar ile mevcut uygulamalara devam edilir.

(3) Başkanlığın ilgili mevzuatı çerçevesinde gözetim yükümlülüğü bulunan kurum ve kuruluşlar, gözetim platformu için yetkilendirilecek temsilci bilgilerini, gözetim platformunun devreye alındığı tarihten itibaren en geç üç ay içerisinde Başkanlığa bildirir.

(4) Türk Standardları Enstitüsü (TSE) tarafından Belgelendirme Programı kapsamında yetkilendirilmiş olan Bilgi ve İletişim Güvenliği Rehberi denetçileri ile denetim firmaları, siber güvenlik alanında faaliyet gösteren denetim hizmet sağlayıcıları; Başkanlıkça yetkilendirme usul ve esasları yayımlanıp yürürlüğe girene kadar, mevcut yetki ve görevleri çerçevesinde denetim faaliyetlerini yürütmeye devam ederler.

(5) Başkanlıkça yeni usul ve esasların yayımlanmasını müteakip, söz konusu denetçi ve firmaların yetkilendirme süreçleri yeni mevzuat hükümlerine göre yeniden değerlendirilir.

(6) Başkanlıkça yeni denetim ölçütleri, gözetim platformuna uyum ve denetim sonuç verisinin gönderilmesi, denetim metodolojisi ve uyum denetimi esasları yayımlanıp yürürlüğe girene kadar; yürütülecek her türlü uyum, denetim ve gözetim faaliyetlerinde mevcut Bilgi ve İletişim Güvenliği Rehberi ile Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınır.

(7) Yeni usul ve esasların yayımlanmasını müteakip, başlamış olan denetim süreçleri eski hükümlere göre tamamlanır; yeni denetim başvuruları ve gözetim faaliyetleri ise yeni ölçütlere göre yürütülür.

Yürürlük

MADDE 35– (1) Bu Yönetmeliğin;

a) Uygulama esaslarının yayımlanması öngörülen hükümleri, ilgili uygulama esasının yayımlandığı tarihten itibaren,

b) Diğer hükümleri, yayımlandığı tarihte,

yürürlüğe girer.

Yürütme

MADDE 36– (1) Bu Yönetmelik hükümlerini Siber Güvenlik Başkanı yürütür.