TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
SİBER GÜVENLİK BAŞKANLIĞI

BİLGİ ve İLETİŞİM GÜVENLİĞİ DENETİM REHBERİ

MART 2026

BELGE ADI: Bilgi ve İletişim Güvenliği Denetim Rehberi

SÜRÜM NO: 1.1

SÜRÜM TARİHİ: 01.03.2026

GİZLİLİK DERECESİ: Tasnif Dışı

Değişiklik No	Değişiklik Tarihi	Değişiklik Nedeni
1.0	Ekim 2021	İlk Yayın
1.1	Mart 2026	Mülga olan Dijital Dönüşüm Ofisi'nin yetkilerinin Siber Güvenlik Başkanlığı'na devredilmesi nedeniyle doküman üzerinde tasarımsal ve kurumsal değişiklikler yapılmıştır.

https://www.siberguvenlik.gov.tr

Bilgi ve İletişim Güvenliği Denetim Rehberi hakkındaki
görüş ve öneriler aşağıda yer alan elektronik posta adresine iletilebilir.

Elektronik Posta: bgrehber@siberguvenlik.gov.tr

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
SİBER GÜVENLİK BAŞKANLIĞI

BİLGİ ve İLETİŞİM GÜVENLİĞİ DENETİM REHBERİ

MART 2026

İÇİNDEKİLER

Sayfa

ŞEKİLLER

TABLOLAR

TANIMLAR VE KISALTMALAR

Bilgi ve İletişim Güvenliği Rehberi'nde yer alan tanım ve kısaltmalar bu dokümanda geçerli olmakla birlikte diğer tanım ve kısaltmalara aşağıda yer verilmiştir.

Tanım / Kısaltma	Açıklama
Başdenetçi	Belgelendirme Programı kapsamında yetkilendirilen Başdenetçi
Belgelendirme Programı	TSE'nin Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Veren Personel ve Firma Belgelendirme Programı
BGYS	ISO / IEC 27001 uyumlu Bilgi Güvenliği Yönetim Sistemi
CISA	Certified Information Systems Auditor / Sertifikalı Bilgi Sistemleri Denetçisi
Denetçi	• Bu dokümanın 3.1.1. başlığının "b" maddesinde yer alan yeterlik ve yetkinliğe sahip personel • Belgelendirme Programı kapsamında yetkilendirilen Denetçi
Denetim	Bilgi ve İletişim Güvenliği Rehberi'nde yer alan süreç ve tedbirlerin tam, doğru, etkin bir şekilde gerçekleştirilip gerçekleştirilmediğinin bağımsız ve sistematik olarak incelenmesi ve raporlanması
Denetim Dosyası	Denetimin amacı, kapsamı, denetim ekibi, denetime ait tüm çalışma formları, denetim raporu ve eklerini içeren tüm bilgi ve belgelerin bir araya getirilerek birleştirilmesinden oluşan tek bir dosya
Denetim Koordinatörü	Denetim ekibi faaliyetlerinin koordinasyonundan ve denetimin yürütülmesinden sorumlu olan ekip lideri
Denetim Rehberi	Bilgi ve İletişim Güvenliği Rehberi uyum denetimlerinin bağımsız bir şekilde planlanması, yürütülmesi ve raporlanması konularında kurumlara ve denetçilere yol göstermek amacıyla hazırlanan işbu doküman
Denetim Riski	Rehber uyum çalışmalarında bir eksiklik olmasına rağmen denetçinin bunları tespit edememesi sonucunda denetim raporuna doğru görüş verememesi riskidir. Yapısal risk, kontrol riski ve tespit riski bileşenlerinden oluşur. • Yapısal risk: Herhangi bir kontrol olmadan bir faaliyetin ortaya çıkaracağı risk • Kontrol riski: Kontrol tarafından zamanında önlenemeyen veya tespit edilemeyen önemli bir eksikliğin oluşma riski • Tespit riski: Denetçinin denetlenen Kurumun bilgi sistemlerinde olabilecek bir eksikliği tespit edememesi riski

Tanım / Kısaltma	Açıklama
Eksiklik	Bilgi ve İletişim Güvenliği Rehberi'nde yer alan süreç veya tedbirlerin etkin olmamasına, hata ya da tehditlerin zamanında tespit edilememesine veya önlenememesine sebep olan durum
Firma	Belgelendirme Programı kapsamında yetkilendirilen Firma
IEC	International Electrotechnical Commission / Uluslararası Elektroteknik Komisyonu
ISO	International Organization for Standardization / Uluslararası Standardizasyon Kuruluşu
Kontrol	Bilgi ve İletişim Güvenliği Rehberi'nde yer alan tedbirlerin etkin bir şekilde yerine getirilmesi amacıyla uygulanan faaliyetler
Makul Güvence	Denetim çalışmasında gerekli teknik bilgi ve tecrübeye sahip denetçinin, denetim prosedürlerini uygulamak suretiyle elde ettiği güvenilir, uygun ve yeterli düzeyde kanıtlara dayanarak sunduğu kesin (mutlak) olmayan güvence
Örneklem	Denetlenecek ana kütlenin (popülasyon) tamamı hakkında makul bir day oluşturmak üzere sonuca varmak amacıyla ana kütle içindeki kalemlerin %100'ünden daha azına denetim prosedürlerinin uygulanması
Rehber	Bilgi ve İletişim Güvenliği Rehberi
SGB	Siber Güvenlik Başkanlığı
TSE	Türk Standardları Enstitüsü
Üst Yönetici	• 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu kapsamındaki kamu kurum ve kuruluşları için anılan Kanunun 11 inci maddesinde tanımlanan Üst Yönetici • Rehber kapsamındaki diğer kurum ve kuruluşlar için bilgi işlem biriminden sorumlu olan en üst yönetici

GİRİŞ

1. BÖLÜM

1. GİRİŞ

6 Temmuz 2019 tarihinde yayımlanarak yürülüğe giren Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi uyarınca, kamu kurumları ve kritik altyapı hizmeti veren işletmeler; karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliğin bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla belirli güvenlik tedbirlerini uygulamakla yükümlü kılınmıştır. Genelge çerçevesinde farklı güvenlik seviyelerinde tedbirler içeren Bilgi ve İletişim Güvenliği Rehberi hazırlanmış, kapsam dâhilindeki Kurumlar tarafından gerekleri yerine getirilmek üzere 27 Temmuz 2020 tarihinde yayımlanmıştır. Kurumların Rehbere uyum sağlarken yerine getirmesi gereken adımlardan biri olan denetim süreci ise bu Denetim Rehberi ile düzenlenmektedir.

1.1. Bilgi ve İletişim Güvenliği Denetim Rehberinin Amacı

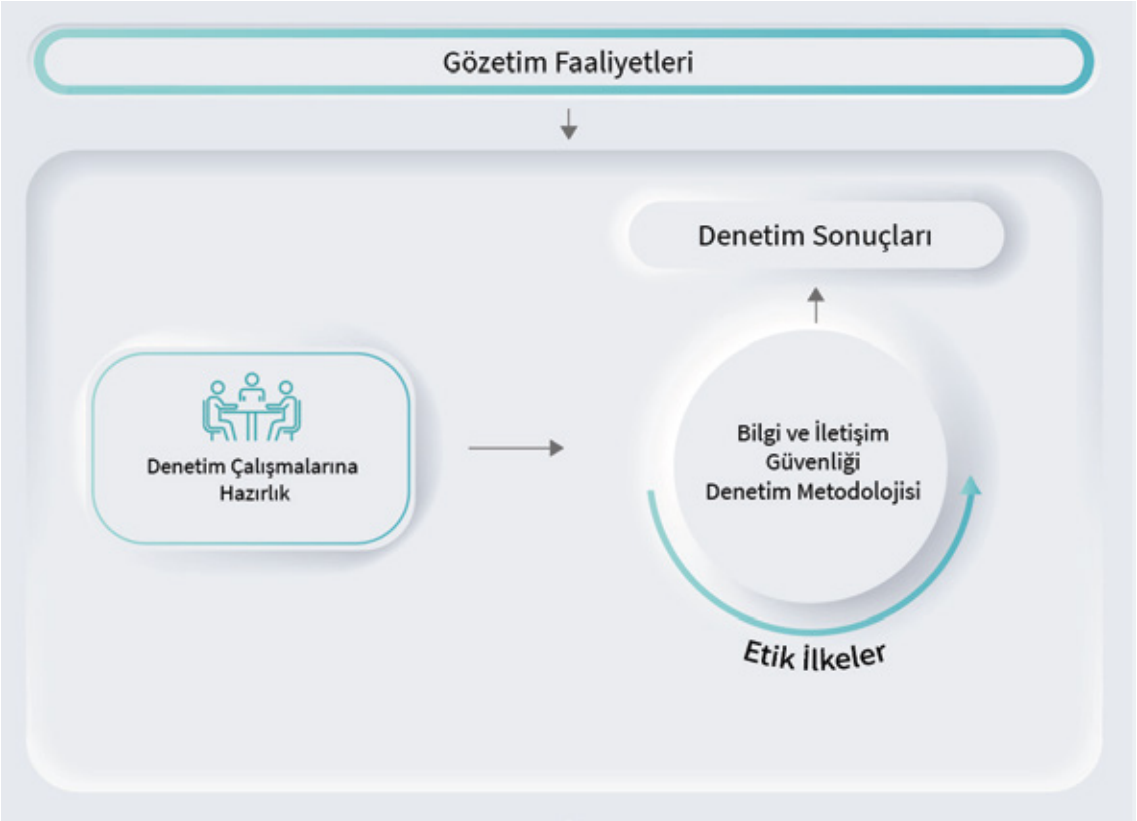
Bilgi ve İletişim Güvenliği Rehberi kapsamında yer alan Kurumların belirli çalışmaları yerine getirmeleri beklenmektedir. Bu çalışmaların; planlama, uygulama, değişiklikleri yönetme, kontrol etme ve önlem alma süreçlerini içeren bir çerçevede yürütülmesi gerekmektedir. Kontrol etme ve önlem alma sürecinin bir parçası olan denetimin yılda en az bir kez gerçekleştirilmesi amacıyla Kurumlar tarafından gerekli planlamalar yapılmalı ve işletilmelidir.

Denetim çalışmalarının belirli bir metodolojide gerçekleştirilmesi, denetimi yürütecek ekibin alanında yetkin olması ve denetime yönelik gözetim faaliyetlerinin etkinliği denetim çalışmalarının verimliliği açısından önem arz etmektedir. Denetimin bağımsız bir şekilde planlanması, yürütülmesi ve raporlanması konularında Kurumlara ve denetçilere yol göstermek amacıyla bu Denetim Rehberi hazırlanmıştır.

1.2. Bilgi ve İletişim Güvenliği Denetim Rehberinin Yapısı

Denetim Rehberi, Kurumlara ve denetçilere denetimde uyulması gereken usul ve esasları sunmaktadır. Denetim Rehberi, sırayla aşağıda yer alan bölümleri içermekte ve Şekil 1'de genel yapısına yer verilmektedir.

- Bölüm 2, Kurumun denetime yönelik yapacağı hazırlık çalışmalarına ve denetimi dış hizmet alım yoluyla gerçekleştirmesi durumunda uyması gereken yükümlülüklere yönelik bilgi vermektedir.
- Bölüm 3, denetim metodolojisinin nasıl uygulanması gerektiğine yönelik bir çerçeve çizmektedir.
- Bölüm 4, denetim sonuçlarının Kurum tarafından SGB'ye gönderilmesi ve denetim sonuçları üzerinden gerçekleştirilecek gözetim faaliyetlerine yönelik bilgi içermektedir.



Şekil 1. Bilgi ve İletişim Güvenliği Denetim Rehberi'nin Yapısı

Bilgi ve İletişim Güvenliği Rehberi'nde gerçekleştirilecek herhangi bir değişikliğin gerektirdiği durumlar dâhil olmak üzere ihtiyaçlar ve değişen şartlar göz önünde bulundurularak Denetim Rehberi güncellenecektir. Denetim Rehberi'nin güncel sürümüne https://www.siberguvenlik.gov.tr adresinden erişilebilecektir.

DENETİM ÇALIŞMALARINA HAZIRLIK

2. BÖLÜM

2. DENETİM ÇALIŞMALARINA HAZIRLIK

Kurumlara Rehberin yayım tarihi olan 27 Temmuz 2020 itibarıyla 24 aylık bir uyum süresi verilmiştir. İlk yıl denetimlerinde Kurumlar denetim faaliyetleri ile ilgili hazırlık çalışmalarına en geç 24 aylık sürenin sonunda başlamalıdır. Ancak uyum çalışmalarını 24 aydan önce tamamlayan Kurumlar denetim faaliyetleri için gerekli hazırlık çalışmalarına uyum süresinin dolmasını beklemeden başlayabilir.

Rehber kapsamındaki tüm Kurumlarda, denetim faaliyetlerinin öncelikli olarak iç denetim birimlerinde görev alan ve bilgi teknolojileri alanında denetim yapmak üzere görevlendirilen iç denetçiler tarafından gerçekleştirilmesi esastır. Kritik altyapı hizmeti veren işletmelerde, düzenleyici ve denetleyici kurumlar ilgili mevzuatları çerçevesinde bu Rehbere uygun şekilde ayrıca denetim faaliyetleri gerçekleştirebilir.

İç denetim birimlerinin bulunmadığı ya da iç denetim birimi olmasına rağmen denetimi yürütecek yeterlik ve yetkinlikte denetçiye sahip olunmadığı hallerde bu durum iç denetim birimi/iç denetçi veya bilgi işlem birimi tarafından yazılı olarak Üst Yöneticiye bildirilir. Bu durumda denetim faaliyetlerinin bağımsız bir şekilde yürütülmesini sağlamak üzere kurum içi diğer personel, diğer kamu kurum ve kuruluşlarından görevlendirilecek personel veya hizmet alımı yolu ile denetim faaliyeti gerçekleştirilebilir.

Kurumlar denetim çalışmalarına hazırlanırken aşağıda yer verilen hususları göz önünde bulundurmalıdır:

a) Kurumların bilgi işlem birimlerinde sunulan hizmetler (mevcut bilişim altyapısının kurulumu, geliştirilmesi, güncellenmesi, güvenliği gibi) bağlı olunan merkezî teşkilat tarafından gerçekleştiriliyor ve Kurum tarafından yalnızca son kullanıcı destek/bakım hizmetleri yürütülüyor ise denetim faaliyetlerinin merkezî teşkilat tarafında gerçekleştirilmesi yeterlidir.

b) Üst Yönetici tarafından denetim faaliyetlerinin etkin bir şekilde yürütülmesini teminen 3.1.1. başlığı altındaki hususlar dikkate alınarak belirlenen iç denetçi veya kurum içi diğer personel denetim faaliyetlerini yürütmek üzere görevlendirilir. Denetim ekibi, denetimin tarafsızlığını ve bağımsızlığını sağlamak amacıyla Rehber uyum faaliyetlerinde yer almayan ve denetlenen birime bağlı olmayan personelden teşkil edilmelidir.

c) Kamu kurum ve kuruluşlarında Üst Yönetici mevcut personeli ile denetim ekibini oluşturamadığı durumda öncelikli alternatif olarak diğer kamu kurum ve kuruluşlarından geçici görevlendirme ile denetim faaliyetlerini gerçekleştirmek üzere personel görevlendirebilir.

ç) Üst Yönetici, kamu kurum ve kuruluşlarında “b” ve “c” maddeleri; kritik altyapı hizmeti veren işletmelerde ise “b” maddesi çerçevesinde denetim ekibini oluşturamadığı durumda 3.1.1. başlığı altındaki denetim ekibi kriterlerini sağlayacak personeli hizmet alım yolu ile denetim faaliyetini gerçekleştirmek üzere görevlendirmelidir. Bu durumda Kurum sonraki yıl denetimlerini iç kaynakları ile yürütmek için gerekli bütçe, personel vb. gereksinimlere yönelik planlamalarını yapmalıdır.

d) Kurumun hali hazırda uymakla yükümlü olduğu mevzuat doğrultusunda ISO/IEC 27001 uyumlu BGYS kurulum, işletim ve belgelendirme yükümlülüğünün bulunması ve bu yükümlülük çerçevesinde BGYS kapsamı ile Rehber uyum kapsamının aynı olması durumunda, BGYS iç tetkik çalışmaları ile Rehber uyum denetimleri tek bir denetim altında yürütülebilir. Ancak denetim çalışmaları sonucunda SGB'ye iletilmesi gereken bilgi ve belgeler bu dokümanda tanımlı formatlara uygun olarak oluşturulmalıdır. Bu şekilde gerçekleştirilecek denetimlerde Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi (BİGDES) üzerinde yer alan tedbir eşleştirme tablolarından faydalanılabilir.

e) Kurum; ilgili olduğu sektörden sorumlu düzenleyici ve denetleyici kuruluş, ilgili bakanlık veya diğer otoriteler tarafından gerçekleştirmekle yükümlü tutulduğu bilgi ve iletişim güvenliği konulu denetimleri Rehber uyum denetimleri ile örtüştürebildiği durumlarda bu denetimleri birlikte gerçekleştirebilir. Ancak denetim çalışmaları sonucunda iletilmesi gereken bilgi ve belgeler bu dokümanda tanımlı formatlara uygun olarak oluşturulmalıdır.

Denetimin Hizmet Alımı ile Gerçekleştirilmesine İlişkin Hususlar

Kurum hizmet alım sürecinde ve buna istinaden yapılacak denetim hizmet alım sözleşmesinde taraflara ait yükümlülükleri doğru ve açık bir şekilde tanımlamalıdır. Kurum ile firma ve denetçiler için denetim hizmet alım sözleşmesinde uyulması gereken asgari yükümlülüklere aşağıda yer verilmektedir. Kurumun faaliyet alanına, iş süreçlerine, denetlenen varlık gruplarının kritiklik derecesine, denetimin kapsamına göre gerek duyulduğu takdirde ilave yükümlülükler (ör. güvenlik soruşturması, kişi güvenlik belgesi) Kurum tarafından denetim hizmet alım sözleşmesinde ele alınmalıdır.

Kurum yükümlülükleri:

a) Denetim hizmetini, Belgelendirme Programı kapsamında yetkilendirilmiş firmalardan almak.

b) Denetim hizmetini, sözleşme tarihinden önceki iki yıl içerisinde Kuruma Rehber uyum faaliyetleri konusunda danışmanlık hizmeti vermiş olan firma ve denetçilerden almamak.

c) Denetim hizmeti alınacak firmadan art arda üçten fazla denetim hizmeti almamış olmak.

ç) Sözleşmede denetimin amacı, kapsamı, sözleşmenin feshine ilişkin şartlara yer vermek.

d) Hangi uzmanlık alanlarında denetçiye ihtiyaç duyulduğunu sözleşmede açıkça yer vermek.

e) Sözleşmede denetim kapsamında hazırlanması gereken rapor, çalışma formları gibi belgelerin format ve özelliklerini belirtmek.

f) Kurumun bilgi güvenliği gereksinimlerine uygun olarak Rehberde yer alan "Tedarikçi İlişkileri Güvenliği" başlığı altındaki tedbirlere sözleşmede yer vermek.

g) Sözleşme kapsamında firma ve denetim ekibinde yer alacak tüm personelin gizlilik taahhütnamesi imzalayacağı hususunda hükümlere yer vermek.

ğ) Denetim ekibine denetim kapsamında yer alan süreç, altyapı ve uygulamalara yönelik elektronik ve fiziksel ortamda yapılan tüm çalışmalar hakkında tam ve doğru bilgi vermek; bu çalışmalar doğrultusunda kullanılan tüm dokümantasyon ve ilişkili kayıt, veri/bilgi, belge vb. kaynakları denetime uygun ve hazır hale getirmek.

h) Denetim ekibine denetim çalışmalarını yürütürken ihtiyaç duyacağı bilgisayar, harici disk vb. ekipmanları mümkün olduğu ölçüde Kurum kaynakları ile sağlamak. Sağlanan ekipmanı; hangi denetçiye, hangi ekipmanın, hangi tarihler arasında teslim edildiği/ alındığı gibi bilgileri içerecek şekilde tutanak altına almak.

ı) Denetim süresince, Kurum bünyesinde gerçekleştirilen faaliyetler ile ilgili bilgi aktarımında bulunabilecek personel kaynağını denetim kapsamına ve denetim planına uyumlu olacak şekilde tahsis etmek.

i) Denetim kapsamında yapılan değerlendirmelerin doğruluğunu olumsuz etkileyebilecek herhangi bir faaliyette bulunmamak.

Firma ve denetçi yükümlülükleri:

a) Denetim ekibinde Belgelendirme Programı kapsamında yetkilendirilen personel görevlendirmek.

b) Denetim çalışmaları kapsamında elde ettiği/ürettiği her türlü bilgi, belge ve dokümanın bütünlüğünü korumak ve gizliliğini sağlamak.

c) Denetim sürecinde elde ettiği/ürettiği elektronik ve/veya basılı formattaki belgeleri denetim yapılan Kurumun yazılı izni olmadan denetim faaliyetlerinin yürütüldüğü fiziksel ortamların dışına çıkarmamak.

ç) Denetim sürecinde; denetim kapsamına yönelik olmayan bilgi, belge veya dokümanları inceleme, denetim kapsamı dışında olan bilgi sistemlerine erişim, denetim faaliyetlerinin yürütüldüğü fiziksel ortamların haricindeki ortamlara erişim gibi denetimin amacı dışında olan taleplerde bulunmamak.

d) Denetim kapsamında elde ettiği/ürettiği herhangi bir veri/bilgiyi kişisel menfaatler için veya hukuka aykırı olarak Kurumun ya da üçüncü kişilerin menfaatine veya itibarına zarar verebilecek şekilde kullanmamak.

e) Denetim kapsamında yapılan değerlendirmelerin tarafsızlığına zarar verebilecek herhangi bir faaliyette bulunmamak.

f) Denetim faaliyeti sırasında bağımsızlığın veya tarafsızlığın ortadan kalktığı durumlarda bu hususu Kurumun ilgili birimlerine bildirmek.

g) Denetim raporunu doğru, tarafsız ve nesnel biçimde hazırlamak.

ğ) Denetim süresince oluşturulan tüm çalışma formlarını, bulgu tablosunu, denetim raporunu ve eklerini denetim dosyası haline getirmek.

h) Denetim Dosyasının bütünlüğünün bozulmasını önleyecek yöntemler kullanmak. Denetim Dosyasını ve özet (hash) bilgisini Kuruma elektronik ortamda teslim etmek.

BİLGİ ve İLETİŞİM GÜVENLİĞİ DENETİM METODOLOJİSİ

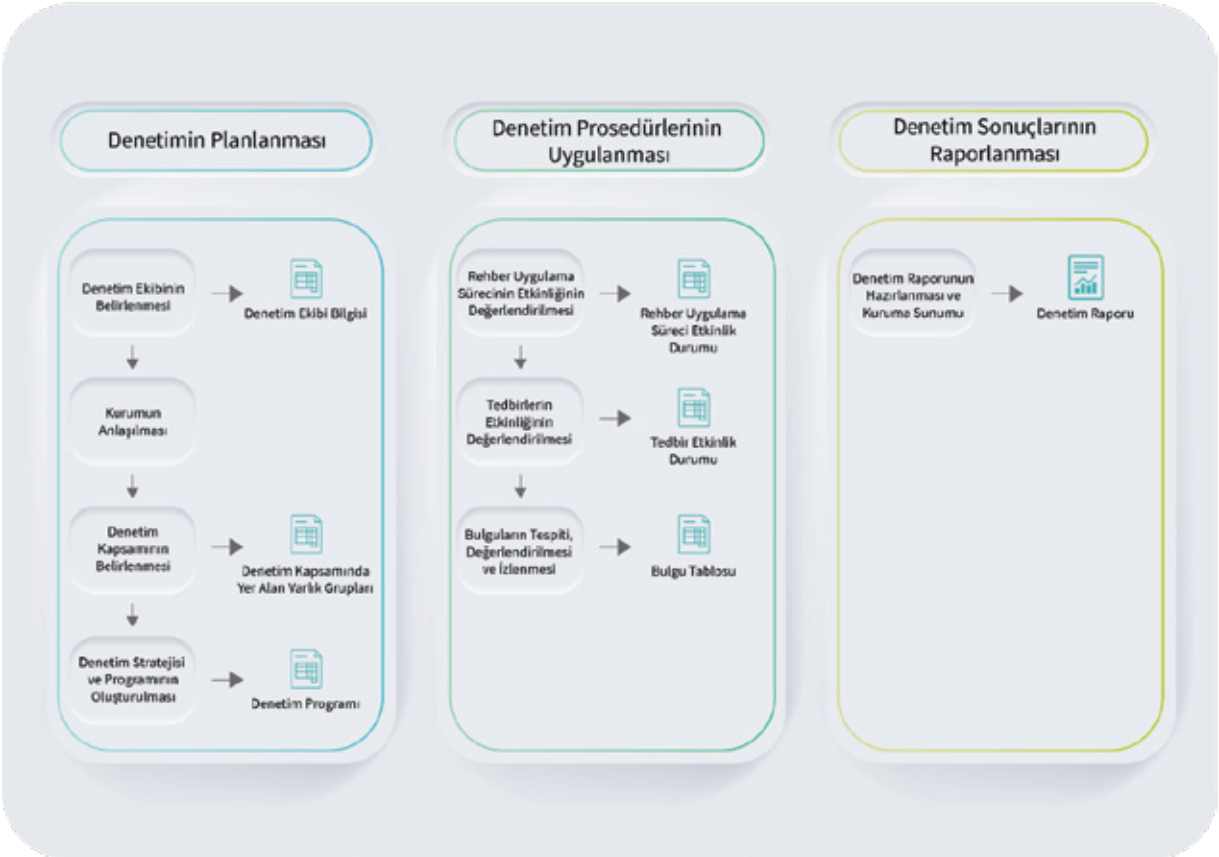
3. BÖLÜM

3. BİLGİ VE İLETİŞİM GÜVENLİĞİ DENETİM METODOLOJİSİ

Rehber uyum denetiminde uygulanacak metodoloji; denetimin planlanması, denetim prosedürlerinin uygulanması ve denetim sonuçlarının raporlanması olmak üzere üç ana süreç ekseninde (Şekil 2) ilerlemektedir. Denetimin temel hedefi aşağıda yer verilen kriterlerin ölçülmesidir.

a) Rehber uygulama sürecinin etkinliği

b) Varlık gruplarına uygulanan tedbirlerin etkinliği



Şekil 2. Denetim Ana ve Alt Süreçleri

Denetim çalışmalarına hazırlık ve Şekil 2'de yer alan süreçler kapsamında yürütülecek faaliyetler için örnek rol ve sorumluluklara Tablo 1'de yer verilmektedir. Tablo 2'de sorumluluk atama matrisindeki rollere ilişkin kısaltmaların açıklamaları yer almaktadır.

Tablo 1. Bilgi ve İletişim Güvenliği Denetimi İçin Sorumluluk Atama Matrisi

No.	Faaliyet Adı	Rol Adı								
		Üst Yönetici	İlgili Birim Yöneticileri	İlgili Birim Uzman Personeli	Kurumsal SOME Yöneticisi	Denetim Koordinatörü	Denetçi / Uzman	SGB	Bağlı/ İlgili/ İlişkili Kurum	İlgili Düzenleyici ve Denetleyici Kurum
1	Denetim Çalışmalarına Hazırlık	O	S	S	S				D	D
2	Denetimin Planlanması	B	B	B	B	O, S	S			
3	Denetim Prosedürlerinin Uygulanması	B	B	B	B	O, S	S			
4	Denetim Sonuçlarının Raporlanması	B	B	B	B	O, S	S			
5	Düzeltici ve Önleyici Faaliyetlerin Takibi	O	S	S	S			B		
6	Denetim Sonuçlarının Gönderilmesi	O, S	B	B	B	S	S	B	B	B
7	Denetim Gözetim Faaliyetleri							O, S	B	B

Tablo 2. Sorumluluk Atama Matrisi Rolleri

Kısaltma	Açıklaması
S	Sorumlu: Görevi gerçekleştiren
O	Onaylayan: Hesap veren, görevi durdurabilen, devam ettirebilen, son kararı verebilen
D	Danışılan: Görev yapılmadan önce bilgisine başvurulması gereken
B	Bilgilendirilen: Görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen

3.1. DENETİMİN PLANLANMASI

Denetimin planlanması, denetim hedeflerini gerçekleştirmek maksadıyla takip edilmesi gereken adımların belirlenmesi ve bir yol haritasının oluşturulması sürecidir. Denetimin bütüncül bir yaklaşımla ele alınmasına ve verimli bir şekilde yürütülmesine zemin hazırlayacak ilk adımdır. Bu süreçte Kurumun faaliyet alanı, iş süreçleri, organizasyon yapısı, mevzuattan kaynaklanan yükümlülükleri, iç ve dış paydaşları gibi temel konular anlaşılmalı ve bu doğrultuda denetim kapsamının belirlenmesine girdi sağlanmalıdır.

Denetimin planlanması süreci aşağıda yer alan alt süreçler işletilerek yürütülmelidir:

a) Denetim ekibinin belirlenmesi
b) Kurumun anlaşılması
c) Denetim kapsamının belirlenmesi
ç) Denetim stratejisi ve denetim programının hazırlanması

3.1.1. Denetim Ekibinin Belirlenmesi

Denetimi gerçekleştirecek ekipteki denetçi sayısı ve denetçilerin uzmanlık alanları; Kurum bilgi varlıkları, iş süreçleri, bilgi sistemlerinin karmaşıklığı dikkate alınarak belirlenmelidir. Denetim ekibi belirlenirken asgari olarak aşağıda yer alan hususlar göz önünde bulundurulmalıdır.

a) Denetim ekibi en az 2 denetçiden oluşmalıdır. Denetimin kapsamı ve denetlenen sistemlerin karmaşıklığına bağlı olarak denetim ekibindeki denetçi sayısı artırılabilir.

b) Denetim ekibi kurum iç denetçisi, kurum içi personel veya diğer kamu kurum ve kuruluşlarından görevlendirilecek personelden oluşuyor ise;

   - Personel aşağıda yer verilen yetkinliklerin en az birini sağlamalıdır.
     - ISO/IEC 27001 Başdenetçi sertifikasına sahip olmak
     - CISA sertifikasına sahip olmak
     - Belgelendirme Programı kapsamında yetkilendirilmiş denetçi veya başdenetçi olmak
   - Kamu kurum ve kuruluşlarında denetim ekibi, yukarıdaki maddede verilen yetkinliklerden en az birine sahip ya da iç tetkik veya iç denetim faaliyetlerinde bulunmuş ve bilgi sistemleri denetimi alanında eğitim almış personelden teşkil edilebilir.
   - Üst Yönetici tarafından denetim ekibi faaliyetlerinin koordinasyonu, denetimin planlanması, yürütülmesi ve raporlanmasını sağlamak üzere denetim ekibindeki denetçilerden biri Denetim Koordinatörü olarak belirlenir.

c) Denetim ekibi hizmet alım yolu ile oluşturuluyor ise;

   - Ekipte yer alan tüm denetçiler Belgelendirme Programı kapsamında yetkilendirilmiş olmalıdır. Ekipte ilgili program kapsamında yetkilendirilen en az bir denetçi ve başdenetçi yer almalıdır.
   - Ekipteki başdenetçi Denetim Koordinatörü rolünü üstlenir. Ekipte birden fazla başdenetçi olması durumunda başdenetçiler arasından biri Denetim Koordinatörü olarak belirlenir.

ç) Denetim ekibi oluşturulurken Rehber uygulama süreci ile varlık gruplarına uygulanması gereken tedbirlerin etkinliğini değerlendirebilecek denetçi dağılımının sağlanmasına özen gösterilmelidir.

d) Denetim çalışmalarında, denetim ekibindeki denetçilere ilave olarak özel uzmanlık veya ihtisas gerektiren alanlarda tecrübesinden faydalanılmak üzere uzman personel görevlendirilebilir. Denetim ekibinde uzman yer alması durumunda, uzmanın yapacağı çalışmalar denetçi refakatinde gerçekleştirilmelidir. Uzmanın; hangi varlık grupları, tedbirler ya da süreçler üzerinde çalışma yapacağı, çalışmaların denetçiye nasıl raporlanacağı denetçiler tarafından belirlenmelidir.

e) Denetim ekibinin tamamı aşağıda yer verilen etik ilkelere uyum sağlamalıdır. Denetim ekibinde yer alan denetçi ve uzmanların tamamına EK – I Gizlilik Taahhütnamesi, EK – J Tarafsızlık Taahhütnamesi imzalatılmalıdır.

Denetim ekibi nihai halini aldıktan sonra, EK – A'da yer alan Denetim Ekibi Bilgisi formu ile kayıt altına alınmalıdır.

Etik İlkeler

Denetçilik mesleğinin en temel özelliği görev alınacak işlerde kamu yararının gözetilmesi ve denetime tabi Kurumun objektif bir şekilde değerlendirmeye tabi tutulmasıdır. Bu bağlamda, denetim ekibinde yer alan denetçilerin/uzmanların aşağıda yer verilen temel etik ilkelere uyum sağlaması gerekmektedir.

a) Dürüstlük: Denetçinin mesleki faaliyetlerinde veya iş ilişkilerinde doğru ve güvenilir olmasıdır.

b) Tarafsızlık: Denetçinin mesleki muhakemesine çıkar, ön yargı gibi herhangi bir durum veya ilişkinin etki etmemesidir.

c) Mesleki yeterlik ve özen: Denetçinin mesleki konularda güncel ve yeterli bilgiye sahip olması ve yaptığı işlerde bu bilgiyi dikkatle uygulamasıdır.

ç) Sır saklama: Denetçinin mesleki faaliyetlerinde edindiği bilgilerin gizliliğini sağlamasıdır.

d) Mesleğe uygun davranış: Denetçinin mesleki itibarını zedeleyecek her türlü tutum, davranış ve eylemden kaçınmasıdır.

3.1.2. Kurumun Anlaşılması

Yapılacak denetimin verimliliğini artırmak ve denetim raporuna makul güvence sağlayacak denetim görüşünü oluşturmak amacıyla denetim ekibi Kurumu anlamaya yönelik bilgi toplama faaliyeti gerçekleştirmelidir. Ancak denetim ekibi, bilgi toplama faaliyetini denetimin amacı ile sınırlı tutmalıdır. Kurumun anlaşılması aşamasında denetim ekibi asgari olarak aşağıda yer verilen hususları yerine getirmelidir:

- Kurum Organizasyon Yapısı

  a) Kurumun teşkilat ve organizasyon yapısı hakkında bilgi edinilir.

  b) Kurum bilgi işlem biriminin genel organizasyon yapısı içerisindeki yeri, yönetimdeki temsil seviyesi ve bilgi işlem faaliyetlerinin gerçekleştirilmesine yönelik rol dağılımları hakkında bilgi edinilir.

  c) Rehber sorumluluk atama matrisinde yer alan rollerin dağılımının nasıl yapıldığı incelenir.

- Kurum İş Süreçleri

  a) Kurumun kuruluş amacına ve faaliyet alanına yönelik bilgi toplanır.

b) Kurum hizmetlerinin neler olduğu ve hangi paydaşlarla ilişkili olduğu belirlenir.

c) Kurum bilgi işlem birimi faaliyetlerinin kapsamı ve diğer birimlerle ilişkisi belirlenir.

ç) Kurumun stratejik planları, BGYS kapsamında oluşturulan süreç dokümanları ve/veya risk analizi raporları var ise incelenir. İş süreçlerini içeren dokümantasyonun olmadığı durumlarda Kurum ilgilileri ile toplantılar gerçekleştirilerek süreçler anlaşılmaya çalışılır.

- Önceki Dönem Denetim Raporları

a) Önceki dönemde gerçekleştirilen denetim varsa buna ilişkin rapor ve bulgular incelenir. Denetim faaliyetlerinin yürütülmesinde hizmet alım yolu kullanılıyor ise inceleme faaliyetleri Kurumun uygun görmesi durumunda gerçekleştirilir.

b) Rehber uyum denetimi faaliyetleri haricinde iç denetim yoluyla veya bağımsız bir denetim kuruluşu tarafından bilgi güvenliğini değerlendirmeye yönelik denetim, sızma testi veya kaynak kod analizi çalışmaları gerçekleştirilmiş ise bunlara ilişkin raporlar ve bulgular incelenir. Denetim faaliyetlerinin yürütülmesinde hizmet alım yolu kullanılıyor ise inceleme faaliyetleri Kurumun uygun görmesi durumunda gerçekleştirilir.

- Üçüncü Taraf Hizmetler

a) Kurum bilişim faaliyetlerinin sürekliliğinde üçüncü taraf hizmetlere olan bağımlılık hakkında bilgi edinilir.

b) Bilgi varlıklarına yönelik bakım ve destek çalışmalarında üçüncü tarafların rolü hakkında bilgi edinilir.

- Mevzuattan Kaynaklanan Yükümlülükler

a) Kurum bilgi sistemlerinin işletilmesi ve güvenliğinin sağlanmasına yönelik yasal düzenlemeler hakkında bilgi edinilir.

b) Kurumun diğer birimleri özelindeki yasal düzenlemelerin bilgi işlem ve bilgi güvenliği süreçlerine etkisi analiz edilir.

- Kurum Varlık Grupları

a) Rehber uygulama süreci kapsamında belirlenen varlık grupları ve kritiklik dereceleri hakkında bilgi edinilir.

b) Rehber uyarınca doldurulması gereken Mevcut Durum ve Boşluk Analizi Formu incelenir.

c) Rehber uyarınca doldurulması gereken Varlık Grubu ve Kritiklik Derecesi Tanımlama Formu, uygulama ve teknoloji alanı ile sıkılaştırma tedbirlerinden hangilerinin varlık gruplarına uygulanmak üzere seçildiğini anlamak üzere incelenir.

3.1.3. Denetim Kapsamının Belirlenmesi

Denetim ekibi, Rehber uyum faaliyetleri çerçevesinde yer alan varlık gruplarından hangilerini denetim kapsamına dâhil edeceğini belirlerken risk odaklı denetim yaklaşımı ile hareket etmeli ve önemlilik kriterini esas almalıdır. Önemlilik, eksiklikler sonucu ortaya çıkacak durumların Kurumun bilgi ve iletişim güvenliğine yansıyacak olası etkilerinin denetçi tarafından mesleki bilgi ve tecrübesine dayalı olarak değerlendirilmesidir. Önemlilik Kurumun iş süreçleri, verdiği hizmetler ve bunlarla ilişkili varlık gruplarının kritiklik seviyesi ile doğrudan ilgilidir.

Denetim ekibi, yapacağı risk değerlendirmesi çerçevesinde kapsamı belirlerken Rehber uyum çalışmalarıyla tanımlanan varlık grubu ana başlıkları ile ilişkili en az bir varlık grubunu kapsama dâhil etmelidir. Risk değerlendirme sürecinde varlık grubunun gizliliği, bütünlüğü, erişilebilirliği ile etki alanları (bağımlı varlıklar, etkilenen kişi sayısı, kurumsal ve toplumsal sonuçlar, sektörel etki) dikkate alınmalıdır. Risk değerlendirmesinde; önceki yıl denetiminden bu yana bilgi sistemleri üzerindeki önemli değişiklikler, önceki yıl denetiminde kapsama dâhil edilen varlık grupları, elde edilen bulgular ve bulgulara yönelik gerçekleştirilen düzeltici ve önleyici faaliyetler de göz önünde bulundurulmalıdır.

Denetim ekibi belirlediği denetim kapsamını EK – B'de yer alan tablo ile kayıt altına almalıdır.

3.1.4. Denetim Stratejisi ve Programının Oluşturulması

Kurumun anlaşılması ve denetim kapsamının belirlenmesi çalışmalarını müteakip denetim ekibi, etkinlik değerlendirmelerini nasıl gerçekleştireceğini ele alan denetim stratejisini belirlemelidir. Denetim stratejisi belirlenirken aşağıdaki unsurlar asgari olarak göz önünde bulundurulmalıdır:

a) Denetimin başlangıç ve bitiş tarihleri

b) Denetim ekibinde yer alacak denetçiler

c) Denetim ekibinde yer alacak uzmanlar

ç) Denetim kapsamında yer alan birimler, varlık grupları

d) Denetim süresince iletişim halinde olunacağı öngörülen Kurum personeli bilgisi ve iletişim yöntemleri

e) Denetim kapsamında ihtiyaç duyulacak sızma testi ve kaynak kod analizi raporları

f) Denetim süresince uygulanacak denetim prosedürleri

g) Denetim zaman planı taslağı (denetim prosedürlerinin uygulanmasına, bulguların incelenmesine, raporun oluşturulmasına yönelik zaman bilgileri)

Denetim stratejisi belirlendikten sonra denetimin ana hedefleri olan Rehber uygulama sürecinin ve varlık gruplarına uygulanan tedbirlerin etkinliğini değerlendirmek amacıyla gerçekleştirilecek çalışmaların belirli bir program dâhilinde yürütülmesi için denetim programı oluşturulmalıdır. Denetim programı denetim hedefi doğrultusundaki iki ana başlık üzerinden aşağıda yer alan unsurlar dikkate alınarak hazırlanmalıdır:

- Hedef 1: Rehber Uygulama Sürecinin Etkinliğinin Değerlendirilmesi

  a) Kurum varlık gruplarının, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanması

  b) Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanması

  c) Varlık grupları tanımlama çalışmalarının varsa bilgi güvenliği yönetim sistemi kapsamında oluşturulan varlık envanteri ile ilişkilendirilmesi

  ç) Varlık grupları kritiklik derecelerinin Rehbere uygun olarak belirlenmesi

  d) Varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi

  e) Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirlerinin varlık grubu ile uygun bir şekilde eşleştirilmesi

  f) Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması

  g) Telafi edici kontrollerin dokümante edilmesi

  ğ) Rehber uygulama yol haritasının oluşturulması

- Hedef 2: Varlık Gruplarına Uygulanan Tedbirlerin Etkinliğinin Değerlendirilmesi

  a) Tedbirlerin, denetim kapsamı dâhilindeki varlık gruplarına etkin bir şekilde uygulanıp uygulanmadığının değerlendirilmesi

  b) Denetim kapsamı dâhilindeki varlık grubu ile ilişkilendirilmiş tedbirler yerine uygulamaya alınan telafi edici kontrollerin uygunluğunun ve etkinliğinin değerlendirilmesi

Denetim programı, denetim ekibi tarafından Denetim Koordinatörü liderliğinde EK – C'ye uygun olarak doldurulmalıdır. Denetim programında yer alan takvim bilgileri için Kurum ile denetim öncesi mutabakat sağlanmalıdır.

3.2. DENETİM PROSEDÜRLERİNİN UYGULANMASI

Denetimin bu adımında, varlık gruplarına yönelik güvenlik tedbirlerinin etkinliğini değerlendirmek için hangi denetim yöntemlerinin kullanılması gerektiği, denetim görüşünün oluşturulmasına makul güvence sağlayacak düzeyde denetim kanıtının nasıl toplanacağı, elde edilen bulguların değerlendirilmesi ve sınıflandırma yöntemleri ele alınmaktadır.

Bu süreçte denetim ekibi, Rehberde yer alan her varlık grubu ve tedbir maddesi için tanımlı denetim yöntemi ve denetim soru önerilerinden faydalanabilir.

3.2.1. Denetim Yöntemleri

Denetçi, tedbirlerin etkinliğini değerlendirirken aşağıda yer alan denetim yöntemlerinden veya belirleyeceği farklı denetim yöntemlerinden faydalanabilir:

a) Mülakat: Denetim yapılan birim kapsamında söz konusu çalışmaların nasıl gerçekleştirildiği bilgisinin ilgili Kurum personeli ile yüz yüze görüşülerek edinilmesidir. Gerekli görülmesi durumunda dokümantasyon inceleme çalışması ile desteklenmelidir.

b) Gözden Geçirme: Denetim yapılan birim kapsamında söz konusu çalışmalara yönelik güvenlik gereksinimleri göz önünde bulundurularak detaylı ve sistematik olarak yapılan incelemedir.

c) Güvenlik Denetimi: Bilgi teknolojileri ve güvenlik sistemlerine ait kuralların, sıkılaştırma ve yapılandırma çalışmalarının teknik olarak denetlenmesidir. Gerekli görülmesi durumunda otomatik araç kullanımı ile desteklenmelidir.

ç) Sızma Testi: Bilgi teknolojileri ve güvenlik sistemleri kapsamında güvenlik açıklarının tespit edilmesini sağlayan, yetkin kişiler tarafından ve yasalara uygun olarak gerçekleştirilen güvenlik testleridir. Denetim ekibi sızma testini gerçekleştirebilecek yeterlik ve yetkinliğe sahip olduğu durumda ilgili tedbirlerin etkinliğini değerlendirmek üzere sızma testi gerçekleştirebilir, Kurumun hangi aralıklarla sızma testi yaptırıp yaptırmadığını sorgulayabilir, daha önce yapılan sızma testi raporlarında elde edilen bulguların giderildiğine yönelik doğrulama yapabilir veya ilgili raporları değerlendirebilir.

d) Kaynak Kod Analizi: Güvenli yazılım geliştirme konusunda uzman kişiler tarafından kaynak kodların incelenmesi ve güvenlik açıklarının tespit edilmesini sağlayan denetim çalışmasıdır. Denetim ekibi kaynak kod analizi gerçekleştirebilecek yeterlik ve yetkinliğe sahip olduğu durumda ilgili tedbirlerin etkinliğini değerlendirmek üzere kaynak kod analizi gerçekleştirebilir, Kurumun hangi aralıklarla kaynak kod analizi gerçekleştirdiğini sorgulayabilir veya daha önce oluşturulan kaynak kod analizi raporlarını değerlendirebilir.

Belirlenecek denetim yöntemi; tedbirin uygulanma biçimine ve tedbirin uygulandığı varlığa uygun şekilde seçilmelidir.

3.2.2. Denetim Kanıtlarının Toplanması

Denetim kanıtı, denetim raporuna ve denetçinin görüşüne dayanak sağlamak için denetim süresince elde edilen tüm bilgi, belge ve dokümanı ifade eder. Denetçi, denetim kanıtı toplarken önceki dönem denetim raporu ve bulgularından faydalanabilir. Denetim hizmet alım yolu ile gerçekleştiriliyor ise denetim raporu ve bulguların hizmeti veren taraf ile paylaşılması Kurum tasarrufundadır. Denetim riskinin makul bir düzeye düşürülmesi için yeterli, uygun ve güvenilir denetim kanıtı toplanmalıdır. Denetim kanıtında olması gereken temel unsurlara ve açıklamalara aşağıda yer verilmiştir:

a) Güvenilirlik: Denetim kanıtının elde edildiği kaynağın uygunluğu, hangi koşullar altında ve hangi zamanda elde edildiğidir.

b) Uygunluk: Denetim kanıtı ile etkinliği değerlendirilecek tedbirin amacı arasında mantıksal bir bağ olmasıdır.

c) Yeterlilik: Denetim kanıtının, denetçinin yapacağı değerlendirmeyi güçlendirecek düzeyde olmasıdır.

ç) Tekrar edilebilirlik: Denetçinin elde ettiği kanıtın aynı şartlar altında başka bir denetçi tarafından elde edilebilmesidir.

Denetim kanıtı toplanırken 3.2.1. başlığı altında yer alan denetim yöntemlerinden faydalanabilir. Denetim görüşüne makul güvence oluşturmak için denetim kanıtı toplanırken birden fazla denetim yöntemi bir arada kullanılabilir. Denetçi toplayacağı denetim kanıtının yeterliliğini bazı durumlarda otomatize edilmiş tek bir kontrol testi ile sağlayabilirken bazı durumlarda örneklem seçim yöntemlerine başvurabilir. Denetçi topladığı denetim kanıtlarını ilgili olduğu çalışma formuna referans olarak göstermelidir.

3.2.2.1. Denetim Çalışma Formu

Denetim çalışma formu; denetçinin denetim süresince yaptığı çalışmaları, uyguladığı denetim prosedürlerini, bunlara istinaden elde ettiği denetim kanıtlarını ve denetçi değerlendirmelerini içerir. Denetçi, çalışma formlarını yapılan denetimle daha önce ilgisi olmayan bir denetçinin anlayabileceği şekilde ve elektronik ortamda hazırlamalıdır. Çalışma formları; ilgili çalışmayı yürüten denetçi, çalışmaya başlanılan tarih, çalışmanın tamamlandığı tarih ve çalışmayı gözden geçiren denetçi bilgisini içerecek şekilde EK – D'ye uygun olarak oluşturulmalıdır. Denetçi elde ettiği kanıtları çalışma formuna doğrudan işleyebileceği gibi sözleşme, politika, prosedür, toplantı tutanağı gibi kanıtları çalışma formuna ek olarak tutabilir. Bir çalışma formuna, oluşturulan başka bir çalışma formu çapraz referans olarak verilebilir. Denetim raporu yazılıp, tüm çalışma formları bir denetim dosyasında birleştirildikten sonra denetim ekibi çalışma formları üzerinde herhangi bir değişiklik yapmamalıdır. Denetim ekibi, Kuruma teslim edeceği denetim dosyasında çalışma formlarının bütünlüğünü sağlamaya yönelik kontroller uygulamalıdır.

3.2.3. Rehber Uygulama Sürecinin ve Tedbirlerin Etkinliğinin Değerlendirilmesi

Hedef 1: Rehber Uygulama Sürecinin Etkinliği

Denetçi, Rehber uygulama sürecinin doğru bir şekilde gerçekleştirilip gerçekleştirilmediğini değerlendirmek için EK – E'de yer alan denetim soruları çerçevesinde çalışmalarını yürütmelidir. Kurumun anlaşılması sürecinde elde edilen bilgiler, ilgili Kurum personeli ile yapılan mülakatlar ve sorulara cevap olarak sunulan bilgi, belge ve dokümantasyonların gözden geçirilmesi denetçinin uygulama sürecinin etkin olup olmadığını belirlemesinde yardımcı olacaktır.

Hedef 2: Varlık Gruplarına Uygulanan Tedbirlerin Etkinliği

Denetçi, denetim kapsamındaki varlık gruplarına uygulanması gereken tedbirlerin etkinliğini değerlendirirken asgari olarak aşağıda yer verilen faaliyetleri gerçekleştirir:

a) Önceki dönem denetim çalışmalarından elde edilen bulgu ve kanıtlardan yararlanarak, iki denetim dönemi arasındaki sürede kontrolün etkinliğini etkileyecek bir değişikliğin gerçekleşip gerçekleşmediğini sorgular. Denetim faaliyetlerinin yürütülmesinde hizmet alım yolu kullanılıyor ise bulgu ve kanıtlara yönelik bilgiler Kurumun uygun görmesi durumunda denetim ekibi ile paylaşılır.

b) Tedbirlerin gerçekleştirilmesi amacıyla tesis edilecek kontrollerin manuel ya da otomatik olup olmadığını sorgular.

c) Kontrollerin etkin olma durumunun başka kontrollere bağlı olup olmadığını değerlendirir. Değerlendirme sonucunda bağlı kontrollerin etkinliğini ölçecek çalışmaların yapılıp yapılmayacağına karar verir.

ç) Kontrollerin tesis edilmesinde hangi birim/personelin görev aldığına yönelik bilgi edinir.

Rehberde yer alan denetim yöntemi önerileri ve soru örnekleri denetçinin etkinlik değerlendirme çalışmalarına yardımcı olmak için genel bir çerçeve sunmaktadır. Denetçi mesleki tecrübesine ve muhakemesine dayanarak kullanacağı yöntem ve soruları genişletebilir. Etkinlik değerlendirme sürecinde gerçekleştirilen faaliyetler ve elde edilen kanıtlar çalışma formlarına işlenmelidir.

Denetçi tedbirin etkin olduğuna karar verirken, kontrollerin tasarım ve işletim etkinliğini test etmelidir. Kontrolün tasarım olarak etkin olması; kontrolün hedeflenen duruma ulaşmak için tam ve doğru bir şekilde tasarlanmasıdır. Tasarım etkinliğinin değerlendirilmesinde denetçi genellikle üzerinden geçme, politika, prosedür, süreç, talimat gibi dokümanların incelenmesi ve gözden geçirilmesi çalışmalarını yürütür. Kontrolün işletim olarak etkin olması; tasarımı etkin olan kontrolün tasarlandığı şekilde işletilmesini ifade etmektedir. Denetçi işletim etkinliğinin değerlendirilmesinde güvenlik denetimi, sızma testi ve kaynak kod analizi gibi bilgisayar destekli denetim yöntemlerinden faydalanabilir.

Bazı kontrollerde tasarım ve işletim etkinliğinin ayrı ayrı değerlendirilmesi kontrolün doğası gereği mümkün olmamaktadır. Bu gibi durumlarda çoğunlukla kontrolün tasarım olarak etkin olması kontrolün işletiminin de etkin olduğu şeklinde değerlendirilir.

Denetçi varlık gruplarına uygulanan tedbirlerin etkinliğini belirlemeye yönelik yaptığı denetim çalışmalarını EK – F'de yer alan tabloda kayıt altına almalıdır. Denetçi tedbirlerin etkin olup olmadığına karar verirken genellikle örneklem seçimi yöntemlerinden faydalanmalıdır.

3.2.3.1. Etkinlik Değerlendirmede Örneklem Seçimi

Örneklem seçimi, denetim raporuna görüş oluşturmak amacıyla denetimin yeterli sayıda varlık, süreç, kayıt ve işlem üzerinde yürütülmesini ifade eder.

Örneklem seçiminin amacı, denetçiye örneklemin seçildiği ana kütle hakkında sonuçlara varmak için makul bir dayanak oluşturmaktır. Bu nedenle, denetçinin tarafsız ve objektif bir şekilde ana kütlenin tipik özelliklerini taşıyan ögelerden oluşan örneklem seçmesi önemlidir.

Denetçi örneklem seçim yöntemini:

a) Varlık grubu içindeki varlıkları belirlemek

b) Belirlenmiş varlıkla ilişkili tedbire ait kontrol testi sayısını belirlemek

için kullanabilir.

Denetçi örneklem büyüklüğünü belirlerken örneklem alacağı varlık grubunun kritiklik derecesi, ana kütlenin büyüklüğü, kontrol riski gibi faktörleri dikkate almalı ve mesleki muhakemesini kullanmalıdır.

Denetçi örneklem seçiminde istatistiki ya da istatistiki olmayan yöntemler kullanabilir. İstatistiki örnekleme yönteminde her bir örnek, bilinen bir seçilme olasılığına sahiptir. İstatistiki olmayan örnekleme yönteminde ise örnekleme birimlerinin seçiminde denetçinin mesleki muhakemesi önemlidir. Örneklem büyüklüğü istatistiki ve istatistiki olmayan yaklaşımlar arasında ayrım yapmak için geçerli bir kriter değildir. Denetçi istatistiksel olmayan yöntemlerle kontrol testi sayısını belirlerken Tablo 3'ten faydalanabilir.

Tablo 3. Kontrolün Sıklığına Bağlı Örneklem Büyüklüğü

Kontrol Sıklığı	Örneklem Büyüklüğü	
	Risk Düzeyi	
	Düşük	Yüksek
Yıllık	1	1
Aylık	2	3
Haftalık	5	8
Günlük	15	25
İşlem bazında	25	40

Bazı kontrollerin yapısı gereği tek bir sürecin incelenmesi ya da tek bir yapılandırma ayarının test edilmesi kontrolün birden çok varlık ya da varlık grubu için etkin olduğu konusunda belirleyici olabilir. Ancak bilgi güvenliği farkındalığını sağlamaya yönelik eğitimlerin tüm personele verilmesi ya da tedarik süreçlerinde olması gereken güvenlik gereksinimlerinin tüm hizmet alım sözleşmelerinde uygulanması gibi kontrollerin etkinliği değerlendirilirken denetçi örneklem seçiminden faydalanabilir.

Denetçi kontrollerin etkinliğine yönelik makul güvence sağlayabilecek kanıt elde edememesi durumunda belirlediği örneklem büyüklüğünü artırmalıdır. Denetçinin kabul edebileceği denetim risk seviyesi ile örneklem büyüklüğü arasında genellikle ters bir orantı vardır. Kabul edilebilir denetim riski azaldıkça, tedbirin etkinliğini belirlemek amacıyla denetçinin seçtiği örneklem büyüklüğü artar. Denetçi örneklem büyüklüğünü genişleterek kanıtlarının yeterlilik ve güvenilirlik seviyesini artırır.

3.2.4. Bulguların Tespiti, Değerlendirilmesi ve İzlenmesi

Bulguların Tespiti

Bulgu, denetçinin denetim süreci boyunca kontrollerin tasarımı veya işletimine dair tespit ettiği eksikliklerin Kurumun bilgi güvenliğinde yaratacağı riske göre değerlendirmesi sonucunda belirlenir. Yapılan değerlendirmede eksikliklerin tek başına ya da birlikte oluşturacağı risk kapsamında bulgu olarak nitelendirilebileceği göz önünde bulundurulmalıdır. Denetçi, Rehber uygulama sürecindeki herhangi bir eksikliği de ortaya çıkaracağı riske göre bulgu olarak değerlendirebilir.

Yapılacak değerlendirmede, EK – E Rehber Uygulama Süreci Etkinlik Durumu tablosu ile EK – F Tedbir Etkinlik Durumu tablosunda kayıt altına alınan veriler göz önünde bulundurulmalıdır. Denetçi elde ettiği bulguları mesleki muhakemesini de kullanarak aşağıda yer alan kritiklik derecelerine göre sınıflandırmalıdır. Bulgunun kritiklik derecesi belirlenirken Kurumda ortaya çıkaracağı güvenlik riskinin bilgi güvenliğine olan etkisi ve gerçekleşme olasılığı göz önünde bulundurulmalıdır. Denetçi bulguların sınıflandırılmasında Tablo 4'ten yararlanabilir.

Tablo 4. Bulgu Kritiklik Seviyesi

Bulgu Kritiklik Seviyesi	Açıklama
Çok Yüksek	Kurumu ciddi anlamda zarara uğratabilecek ve gerçekleşme ihtimali çok yüksek olan bulgular bu grupta değerlendirilir. Bu gruptaki bulguların etkisi değerlendirildiğinde: • Kurum, misyonunu yerine getirmek için sürdürmesi gereken temel hizmetlerinden birçoğunu veremez hale gelebilir. • Kurumun sunduğu hizmetlerde kritik olduğu değerlendirilen varlıkların kaybına, işletilmez hale gelmesine neden olabilir. • Kişilerin ölümüne veya ölümcül yaralanmalara sebep olabilir. • Telafisi zor itibar kaybına neden olabilir.
Yüksek	Kurumu zarara uğratabilecek ve gerçekleşme ihtimali yüksek olan bulgular bu grupta değerlendirilir. Bu gruptaki bulguların etkisi değerlendirildiğinde: • Kurumun misyonunu yerine getirmesi için sunması gereken temel hizmetler kesintiye uğrayabilir. • Kurumun sunduğu hizmetlerde kullanılan varlıkların zarar görmesine neden olabilir. • Kişilerin yaralanmalarına sebep olabilir. • Kurumun itibarı zedelenebilir.
Orta	Kurumun misyonunu yerine getirmek için sürdürmesi gereken temel hizmetlerin etkin ve verimli sunulamamasına neden olan bulgulardır.
Düşük	Kurum misyonunu yerine getirmek için sürdürmesi gereken temel hizmetlerini vermeye devam eder. Kurumun daha iyi bir hizmet sunmasını sağlamaya yönelik bulgulardır.

Elde edilen bulgular, EK – G Bulgu Tablosunda tanımlanmalıdır. Tabloda bulguya neden olan eksiklik veya zayıflığın ilgili olduğu tedbir maddeleri ve yaratabileceği riskin açık bir şekilde tanımlı olması gerekmektedir. Denetimlerde tespit edilen bulguların standart bir şekilde kodlanması bulguların takibini kolaylaştıracaktır. Bu doğrultuda, eklenecek her bir bulgu için aşağıda yer alan etiketleme yöntemi kullanılmalıdır.

- Denetim Yılı: Bulgunun tespit edildiği cari yıl bilgisidir.
- Denetim Dönemi: Denetim yılında yapılan kaçıncı denetim olduğu bilgisidir.
- Bulgu Sıra No: Bulgunun denetim dönemi içinde kaçıncı bulgu olduğunu ifade eden ve 1'den başlayarak artan sıra bilgisidir.
- Denetim Unsuru: Denetim hedefine bağlı olarak "Rehber Uygulama Sürecinin Etkinliği" ise "U" şeklinde, "Varlık Gruplarına Uygulanan Tedbirlerin Etkinliği" ise "T" şeklinde ifade edilmelidir.

"Rehber Uygulama Sürecinin Etkinliği" denetim hedefi için Tablo 5'te yer alan denetim unsurlarından biri bulgu tablosuna işlenecek kısaltma olarak kullanılmalıdır.

Tablo 5. Rehber Uygulama Süreci ile İlişkili Denetim Unsurları

Denetim Unsuru	Bulgu Tablosuna İşlenecek Kısaltması
Kurum varlık gruplarının, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanması	U01
Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanması	U02
Varlık grupları tanımlama çalışmalarının varsa bilgi güvenliği yönetim sistemi kapsamında oluşturulan varlık envanteri ile ilişkilendirilmesi	U03
Varlık grupları kritiklik derecelerinin Rehbere uygun olarak belirlenmesi	U04
Varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi	U05
Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirlerinin varlık grubu ile uygun bir şekilde eşleştirilmesi	U06
Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması	U07
Telafi edici kontrollerin dokümante edilmesi	U08
Rehber uygulama yol haritasının oluşturulması	U09

Denetim hedefi "Varlık Gruplarına Uygulanan Tedbirlerin Etkinliği" ise Tablo 6'da yer alan denetim unsurlarından biri bulgu tablosuna işlenecek kısaltma olarak kullanılmalıdır.

Tablo 6. Varlık Gruplarına Uygulanan Tedbirlerin Etkinliği ile İlişkili Denetim Unsurları

Denetim Unsuru	Bulgu Tablosuna İşlenecek Kısaltması
Ağ ve Sistem Güvenliği	T01
Uygulama ve Veri Güvenliği	T02
Taşınabilir Cihaz ve Ortam Güvenliği	T03
Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği	T04
Personel Güvenliği	T05
Fiziksel Mekânların Güvenliği	T06
Kişisel Verilerin Güvenliği	T07
Anlık Mesajlaşma Güvenliği	T08
Bulut Bilişim Güvenliği	T09
Kripto Uygulamaları Güvenliği	T10
Kritik Altyapılar Güvenliği	T11
Yeni Geliştirmeler ve Tedarik	T12
İşletim Sistemi Sıkılaştırma Tedbirleri	T13
Veri Tabanı Sıkılaştırma Tedbirleri	T14
Sunucu Sıkılaştırma Tedbirleri	T15

Kritiklik Seviyesi: Bulguya verilen kritiklik derecesidir. Kritiklik derecesi Çok Yüksek olarak belirlenen bulgular "Ç", Yüksek olarak belirlenen bulgular "Y", Orta olarak belirlenen bulgular "O", Düşük olarak belirlenen bulgular için "D" kısaltmaları kullanılır.

Tablo 7'de, bulgu listesine eklenecek bulguların yukarıda belirtilen etiketleme yöntemi kullanılarak ifade edilmesine yönelik örnekler yer almaktadır.

Tablo 7. Bulgu Etiketleme Örneği

Bulgunun Kodu	Denetim Yılı	Denetim Dönemi	Bulgu Sıra No	Denetim Unsuru	Kritiklik Seviyesi
2021.1.2.U04.Y	2021	1	2	Varlık grupları kritiklik derecelerinin Rehbere uygun olarak belirlenmesi (U04)	Yüksek
2022.2.3.T04.O	2022	2	3	Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği (T04)	Orta

Tespit Edilen Bulguların Değerlendirilmesi ve İzlenmesi

Denetim çalışmaları kapsamında elde edilen bulguların;

- Kurum tarafından herhangi bir bilgi, belge, dokümanın tam olarak veya zamanında bildirilmemesi
- Denetçinin dikkatinden kaçan herhangi bir husus sebebiyle yanlış değerlendirme yapması

gibi durumlardan kaynaklanmadığını garanti altına almak amacıyla, denetim ekibi ve denetim kapsamında yer alan birim sorumluları ve/veya yöneticileri arasında tespit edilen bulguların gözden geçirilmesine ilişkin toplantı gerçekleştirilir. Yapılan toplantı, bir toplantı tutanağı ile kayıt altına alınarak denetim dosyasına eklenir.

Denetim faaliyetini yürüten denetim ekibinin kurum içi personelden oluştuğu durumlarda denetim ekibi aracılığıyla; diğer kamu kurum ve kuruluşlarından geçici görevlendirme veya hizmet alım yolu ile oluştuğu durumlarda ise Kurum tarafından görevlendirilecek birim/personel aracılığıyla bulguların takibine yönelik izleme sistemi tanımlanmalı ve işletilmelidir. İzleme sistemi; elde edilen bulguların kök neden analizinin yapılması, kritiklik derecesi yüksek olan bulgular öncelikli olmak üzere bunları ortadan kaldırmaya veya kritiklik derecesini düşürmeye yönelik düzeltici veya önleyici faaliyetlerin belirlenmesi, aksiyon planlarının hazırlanması ve bunları gerçekleştirecek sorumlu birim/personelin belirlenmesine yönelik temel süreç ve faaliyetleri içermelidir.

3.3. DENETİM SONUÇLARININ RAPORLANMASI

3.3.1. Denetim Raporunun Hazırlanması ve Kuruma Sunumu

Denetim ekibinin Rehber uyum faaliyetlerinin etkinliği ile ilgili kanaatini objektif, açık, öz ve anlaşılır bir dille beyan ettiği belge denetim raporunu ifade eder. Denetim ekibi, denetim görüşünü oluşturacak yeterli bilgi, belge ve dokümanın Kurum tarafından sağlanmadığı durumlarda veya denetimin bağımsızlığını ya da tarafsızlığını zedeleyecek herhangi bir durumun varlığında Kurumun ilgili birimlerine bunu yazılı olarak bildirir.

Denetim ekibi, denetim görüşünü oluşturmaya yönelik herhangi bir kısıt veya engel ile karşılaşmadığı durumda denetim raporunu aşağıdaki başlıkları içerecek şekilde hazırlamalıdır.

a) Rapor Kapağı: Kurum adı, denetim tarihi ve raporu hazırlayan denetçi bilgilerini içerir.

b) Yönetici Özeti: Denetimin yapılma amacını, kapsamını, kapsam dışı bırakılan hususlar var ise bu hususların kapsam dışı bırakılma nedenlerini, denetim gerçekleştirilirken uygulanan metodolojiyi, Kurumun Rehbere uyum durumunu, elde ettiği bulguların Kurum bilgi güvenliğinde yaratacağı risklerin kısa bir özetini içerir.

c) İçindekiler: Rapor içeriğine ilişkin dizin bilgisini içerir.

ç) Tanımlar ve Kısaltmalar: Denetim raporunda yer alan ve tanımlanmasının raporun anlaşılması açısından faydalı olacağı değerlendirilen kavramlar ile raporda yer alan kısaltmaların açık haline yönelik bilgiyi içerir.

d) Giriş: Kurumun bilgi güvenliği kapsamında uyum sağlaması gereken yasal düzenlemeler, bilgi güvenliğine yönelik organizasyon yapısı, bilişim sistemleri kapsamında iç ve dış paydaşlara hizmet veren sistem, uygulama ve altyapısı hakkında genel bilgiyi içerir.

e) Denetim Kapsamına İlişkin Bilgi: Kurum bilişim sistemlerinde yer alan varlık gruplarından hangilerinin denetim kapsamına dâhil edilip edilmediğine yönelik bilgiyi içerir.

f) Denetim Görüşü: EK – H'de yer alan şablonun, denetim görüşünü yansıtacak şekilde denetim ekibi tarafından doldurularak ekipte yer alan tüm denetçiler ve Kurum Üst Yöneticisi tarafından imzalanması sonucu oluşturulan dokümandır.

g) Ekler: Denetim kapsamındaki varlık grupları, denetim ekibi bilgisi, bulgu tablosu, denetim görüşü ile denetçinin rapor içeriğinde bahsettiği ve ek olarak sunmak istediği diğer bilgi, belge ve dokümanı içerir.

Denetim raporunu oluşturan belgelerin her sayfası ekler dâhil denetim ekibinde yer alan denetçiler tarafından 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile imzalanarak rapor nihai haline getirilir.

Denetim raporu gizlilik dereceli bilgi niteliği taşımakta olup Kurum bilgi güvenliği gereksinimleri doğrultusunda gizlilik derecesi belirlenir. Rapor herhangi bir ortamda denetim ekibi veya Kurum tarafından yayımlanmamalıdır. Denetim raporu denetim dosyası içine dâhil edilerek Kuruma teslim edilmelidir.

Denetim ekibi yalnızca; denetim kapsamını, Kuruma teslim edilen denetim dosyasının boyutunu, dosyanın özet (hash) bilgisini ve teslim edilme tarihini içeren bilgileri taraflarca tutanak altına alarak elektronik ortamda saklamalıdır. Denetim ekibi bunların dışında herhangi bir belge, doküman veya sair bilgiyi Kurum dışına çıkarmamalıdır.

Denetim ekibi, denetim çalışmalarını yürütürken Kurum kaynakları dışında herhangi bir uygulama, cihaz vb. araç kullandığı durumda, denetim çalışmalarını tamamladıktan sonra bu araçlar üzerindeki Kuruma ait her tür bilgiyi Kurum gözetiminde geri döndürülemeyecek şekilde silmeli veya mümkünse imha işlemini gerçekleştirerek yapılan işlemleri tutanak altına almalıdır.

DENETİM SONUÇLARININ GÖNDERİLMESİ

4. BÖLÜM

4. DENETİM SONUÇLARININ GÖNDERİLMESİ

2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi uyarınca Rehber kapsamındaki kurum ve kuruluşların, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturması ve yılda en az bir defa uygulamayı denetlemesi, denetim sonuçları ile yapılan düzeltici ve önleyici faaliyetleri, Rehberde belirtilen usul ve esaslara göre bir rapor halinde iletmeleri gerekmektedir. Bu kapsamda denetim raporunun aşağıda yer verilen bölümleri denetim raporunun oluşturulma tarihinden itibaren en geç iki aylık süre içinde Bilgi ve İletişim Güvenliği Uyum ve Denetim İzleme Sistemi'ne (BİGDES) 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile Üst Yönetici veya Üst Yöneticinin yetkilendirdiği personel tarafından imzalanarak iletilir.

a) EK – A'da yer alan Denetim Ekibi Bilgisi

b) EK – B'de yer alan Varlık Grupları ve Denetim Kapsamı

c) EK – E'de yer alan Rehber Uygulama Süreci Etkinlik Durumu

ç) EK – F'de yer alan Tedbir Etkinlik Durumu

d) EK – H'de yer alan Denetim Görüşü

Denetim çalışmalarının gerçekleştirilememesi durumunda, bu durum Kurum Üst Yöneticisi tarafından gerekçesi ile bildirilmelidir. Siber Güvenlik Başkanlığı, denetim sonuçları üzerinden ilgili mevzuat çerçevesinde gözetim faaliyetleri yürütür.

EKLER

EK – A: DENETİM EKİBİ BİLGİSİ

Kurum Adı				
Denetleyen	**Kurum Personeli**	☐		
	Kurum Dışı Geçici Görevlendirme	☐	**Kurum Adı**	
	Firma	☐	**Firma Adı**	
Sıra No	**Denetim Rolü** (Denetçi – D Başdenetçi – BD Uzman – U Denetim Koordinatörü – DK)	**Adı ve Soyadı**	**Görevlendirilme Türü** (Kurum Personeli – KP Geçici Görevlendirme – GG Hizmet Alımı – HA)	**Sertifika / Uzmanlık Alanı** (ISO/IEC 27001 Başdenetçi Sertifikası CISA Sertifikası TSE Tarafından Yetkilendirilen Denetçi Veri Tabanı Uzmanı Ağ ve Sistem Uzmanı vb.)
1				
2				
3				
4				
5				
6				
7				
8				

EK – B: VARLIK GRUPLARI VE DENETİM KAPSAMI

Denetim ekibi tarafından denetim kapsamına alınan varlıklar aşağıdaki tabloda kayıt altına alınmalıdır.

Varlık Grubu Ana Başlığı	Varlık Grubu No	Varlık Sayısı	Varlık Grubu Adı	Kritiklik Derecesi 1 / 2 / 3	Denetim Kapsamında mı? Evet – E Hayır – H
Ağ ve Sistemler					
Uygulamalar					
Taşınabilir Cihaz ve Ortamlar					
Nesnelerin İnterneti (IoT) Cihazları					
Fiziksel Mekânlar					
Personel					

EK – C: DENETİM PROGRAMI

Hedef 1: Rehber Uygulama Sürecinin Etkinliğinin Değerlendirilmesi				
Denetlenecek Süreç	**Denetçi(ler) / Uzman(lar)**	**Bilgi Alınacak Birim / Personel**	**Hazırlanması Gereken Bilgi, Belge, Doküman**	**Öngörülen Denetim Zamanı**
Kurum varlık gruplarının, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanması				
Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanması				
Varlık grupları tanımlama çalışmalarının varsa bilgi güvenliği yönetim sistemi kapsamında yönetilen varlık envanteri ile ilişkilendirilmesi				
Varlık grupları kritiklik derecelerinin Rehbere uygun olarak belirlenmesi				
Varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi				

Hedef 1: Rehber Uygulama Sürecinin Etkinliğinin Değerlendirilmesi				
Denetlenecek Süreç	**Denetçi(ler) / Uzman(lar)**	**Bilgi Alınacak Birim / Personel**	**Hazırlanması Gereken Bilgi, Belge, Doküman**	**Öngörülen Denetim Zamanı**
Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirlerinin varlık grubu ile uygun bir şekilde eşleştirilmesi				
Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması				
Telafi edici kontrollerin dokümante edilmesi				
Rehber uygulama yol haritasının oluşturulması				

Hedef 2: Varlık Gruplarına Uygulanan Tedbirlerin Etkinliğinin Değerlendirilmesi				
Denetlenecek Süreç	**Denetçi(ler) / Uzman(lar)**	**Bilgi Alınacak Birim / Personel**	**Hazırlanması Gereken Bilgi, Belge, Doküman**	**Öngörülen Denetim Zamanı**
Ağ ve sistem güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Uygulama ve veri güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Taşınabilir cihaz ve ortam güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Nesnelerin interneti (IoT) cihazlarının güvenliği tedbirlerinin değerlendirilmesi				
Personel güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Fiziksel mekânların güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Kişisel verilerin güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				

Anlık mesajlaşma güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Bulut bilişim güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Kripto uygulamaları güvenliği tedbirlerinin etkinliğinin değerlendirilmesi				
Kritik altyapıların güvenliğine yönelik tedbirlerin etkinliğinin değerlendirilmesi				
Yeni geliştirmeler ve tedarike yönelik güvenlik tedbirlerin etkinliğinin değerlendirilmesi				
İşletim sistemi sıkılaştırma tedbirlerinin etkinliğinin değerlendirilmesi				
Veri tabanı sıkılaştırma tedbirlerinin etkinliğinin değerlendirilmesi				
Sunucu sıkılaştırma tedbirlerinin etkinliğinin değerlendirilmesi				

EK – D: ÇALIŞMA FORMU

Denetçi çalışma formundaki "Örneklem Seçimi Hakkında Bilgi" alanını örneklem seçimi ile ilgili hangi yöntemleri uyguladığını, örneklemdeki ana kütle ve örneklem büyüklüğü hakkında bilgi verecek şekilde doldurmalıdır.

Kurum Adı							
Çalışma Formu No							
Oluşturan Denetçi		**Tarih**		**Gözden Geçiren Denetçi**		**Tarih**	
İlgili Varlık Grupları							
Denetlenen Süreç(ler) / Tedbir(ler)							
Başlangıç – Bitiş Tarihi							
Örneklem Seçimi Hakkında Bilgi							
Referans Çalışma Formları • •							
Kanıtlar • •							
Değerlendirmeler • •							

EK – E: REHBER UYGULAMA SÜRECİ ETKİNLİK DURUMU

Denetim yöntemleri alanında yer alan “Diğer” denetçinin aşağıdaki tabloda yer verilen denetim yöntemleri dışında kullandığı denetim yöntemini ifade etmektedir.

Kurum Adı							
Rehber Sürümü				**Tarih**			
Denetçi / Uzman Bilgisi							
	1	2	3	4	5	6	7
Denetim Rolü							
Ad - Soyad							
Bilgi Alınan Kurum Personeli							
	1	2	3	4	5	6	7
Unvan							
Ad - Soyad							

Soru No	**Denetim Sorusu**	**Denetim Yöntem(ler)i** (Mülakat – M Gözden Geçirme – G Diğer – D)	**Çalışma Formu No**	**Etkinlik Durumu** (Etkin – E Kısmen Etkin – K Etkin Değil – ED)
1	Kurum varlık grupları, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanmış mıdır?			
2	Kurum bilgi varlıkları en az bir varlık grubu altında tanımlanmış mıdır?			

Soru No	Denetim Sorusu	Denetim Yöntem(ler)i (Mülakat – M Gözden Geçirme – G Diğer – D)	Çalışma Formu No	Etkinlik Durumu (Etkin – E Kısmen Etkin – K Etkin Değil – ED)
3	Varlık grupları tanımlama çalışmaları, varsa bilgi güvenliği yönetim sistemi kapsamında oluşturulan varlık envanteri ile ilişkilendirilmiş midir?			
4	Varlık grupları kritiklik dereceleri Rehbere uygun olarak belirlenmiş midir?			
5	Varlık gruplarına uygulanacak tedbirler kritiklik derecesine uygun olarak belirlenmiş midir?			
6	Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirleri varlık grubu ile uygun bir şekilde eşleştirilmiş midir?			
7	Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmaları yapılmış mıdır?			
8	Telafi edici kontroller dokümante edilmiş midir?			
9	Rehber uygulama yol haritası oluşturulmuş mudur?			

EK – F: TEDBİR ETKİNLİK DURUMU

Denetçi, denetim kapsamına aldığı varlık grubu ana başlıkları ile ilgili tedbirlerin etkinlik durumuna ilişkin bilgiyi içerecek şekilde aşağıdaki tabloyu doldurmalıdır.

Kurum Adı							
Rehber Sürümü				**Tarih**			
Denetçi / Uzman Bilgisi							
	1	2	3	4	5	6	7
Denetim Rolü							
Ad - Soyad							
Bilgi Alınan Kurum Personeli							
	1	2	3	4	5	6	7
Unvan							
Ad - Soyad							

Varlık Grubu Ana Başlığı No (3.1., 3.2., 3.3., 3.4., 3.5., 3.6.)	**Varlık Grubu No**	**Tedbir No**	**Tedbirin Uygulanma Durumu** (Uygulandı – U, Kısmen Uygulandı – K, Çoğunlukla Uygulandı – Ç, Telafi Edici Kontrol Uygulandı – T, Uygulanmadı – Y, Uygulanabilir Değil – UD)	**Telafi Edici Kontrol No** (Varsa)	**Tedbirin Etkinlik Durumu** (Etkin – E, Kısmen Etkin – K, Etkin Değil – ED)	**Denetim Yöntem(ler)i** (Mülakat – M Gözden Geçirme – G Güvenlik Denetimi – GD Sızma Testi – S Kaynak Kod Analizi – K Diğer – D)	**Çalışma Formu No**

EK – G: BULGU TABLOSU

Sıra No	Bulgu Kodu	İlgili Olduğu Tedbir Maddeleri
1		
2		
3		
4		
5		
6		
7		

EK – H: DENETİM GÖRÜŞÜ

..... Bakanlığına / Kurumuna / Anonim Şirketine /……. :

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

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

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

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

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

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

Bilgi ve İletişim Güvenliği Rehberi uygulama sürecinde:

a) Kurum varlık gruplarının, Rehberde yer alan varlık grubu ana başlıkları ile uyumlu olacak şekilde tanımlanma durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."

b) Kurum bilgi varlıklarının mutlaka bir varlık grubu altında tanımlanma durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."

c) Varlık grupları tanımlama çalışmalarının varsa bilgi güvenliği yönetim sistemi kapsamında oluşturulan varlık envanteri ile ilişkilendirilme durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."

ç) Varlık grupları kritiklik derecelerinin Rehbere uygun olarak belirlenme durumu "kısmen gerçekleştirilmiştir", "tamamen gerçekleştirilmiştir", "hiç gerçekleştirilmemiştir."

d) Varlık gruplarının kritiklik derecesine uygun tedbirlerin belirlenmesi “kısmen gerçekleştirilmiştir”, “tamamen gerçekleştirilmiştir”, “hiç gerçekleştirilmemiştir.”

e) Uygulama ve teknoloji alanına yönelik tedbirler ve sıkılaştırma tedbirlerinin varlık grubu ile uygun bir şekilde eşleştirilmesi “kısmen gerçekleştirilmiştir”, “tamamen gerçekleştirilmiştir”, “hiç gerçekleştirilmemiştir.”

f) Her bir varlık grubu için mevcut durum ve boşluk analizi çalışmalarının yapılması “kısmen gerçekleştirilmiştir”, “tamamen gerçekleştirilmiştir”, “hiç gerçekleştirilmemiştir.”

g) Telafi edici kontrollerin dokümante edilmesi “kısmen gerçekleştirilmiştir”, “tamamen gerçekleştirilmiştir”, “hiç gerçekleştirilmemiştir.”

ğ) Rehber uygulama yol haritasının oluşturulma durumu “kısmen gerçekleştirilmiştir”, “tamamen gerçekleştirilmiştir”, “hiç gerçekleştirilmemiştir.”

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

Varlık Grubu Ana Başlığı No	**Varlık Grubu No**	**Uygulanması Gereken Toplam Tedbir Sayısı**	**Tedbirlerin Etkinlik Durumu**		
(3.1., 3.2., 3.3., 3.4., 3.5., 3.6.)			**Etkin Olan Tedbir Sayısı**	**Etkin Olmayan Tedbir Sayısı**	**Kısmen Etkin Tedbir Sayısı**

Düzenlenme Yeri ve
Tarihi:

Denetim Koordinatörü:

İmza:

Denetçi (ler)

İmza:

EK – I: GİZLİLİK TAAHHÜTNAMESİ ÖRNEĞİ

<İşbu Gizlilik Taahhütnamesi (Taahhütname), Kurumun denetim ekibinde görev alan kişilere imzalatacağı gizlilik taahhütnamesinin hazırlanma sürecinde örnek alınmak üzere oluşturulmuştur. Kurum, bilgi güvenliği gereksinimlerine uygun olarak Gizlilik Taahhütnamesini özelleştirilebilir.>

Bu Taahhütname, Bilgi ve İletişim Güvenliği Rehberi uyum denetimi kapsamında denetim ekibinde yer alan Denetçilerin / Uzmanların denetim çalışmaları süresince elde ettiği veya ürettiği bilgiler ile kullandıkları bilgi varlıklarının kullanma esaslarının belirtilmesi, sorumluluklarının tanımlanması ve ilgili kişiye sorumluluklarının bildirilmesi amacıyla oluşturulmuştur.

Tanımlar ve Kısaltmalar

Tanım	Açıklama
Denetçi	Denetim faaliyetini gerçekleştirmek üzere denetim ekibinde görev alan kişi / kişilerdir.
Denetim	Bilgi ve İletişim Güvenliği Rehberi'nde yer alan süreç ve tedbirlerin tam, doğru, etkin bir şekilde gerçekleştirilip gerçekleştirilmediğinin bağımsız ve sistematik olarak incelenmesi ve raporlanmasıdır.
Gizli Bilgi	• Bilmesi gereken kişiler dışındakilere açıklanması veya verilmesi, millî güvenlik ve ülke menfaatleri bakımından sakıncalı görülen ve haiz olduğu önem derecelerine göre "ÇOK GİZLİ", "GİZLİ", "ÖZEL" veya "HİZMETE ÖZEL" şeklinde sınıflandırılan bilgi/veriler, • Kuruma ait özel sırlar, mali bilgiler, personel bilgileri, sistem bilgileri, materyaller, programlar, dokümanlar, bilişim sistemleri içerisinde tutulan veriler, donanım/yazılım ve tüm diğer uygulamalar, • 24/03/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında tanımlanan ve Kurum tarafından işlenen kişisel veriler ile özel nitelikli kişisel veriler, • Açıklanması halinde kişi ve kurumlara maddi veya manevi zarar verme ya da herhangi bir kişi veya kuruma haksız fayda sağlama ihtimali bulunan her türlü bilgi ve belgedir.
Kurum	[Denetlenen Kurum veya Kuruluşun Adı]'dır.
Uzman	Denetim ekibindeki Denetçi'lere ilave olarak özel uzmanlık veya ihtisas gerektiren alanlarda denetim çalışmalarında tecrübesinden faydalanılmak üzere görevlendirilen kişi/kişilerdir.

Esaslar

a) Bu Taahhütname denetim ekibindeki tüm Denetçi/Uzman'lar tarafından imzalanır.

b) Denetçi/Uzman bu Taahhütname hükümlerinin hepsini kabul eder.

c) Denetçi/Uzman bu Taahhütname'nin tamamını dikkatle okumakla yükümlüdür.

ç) Taahhütname, Denetçi/Uzmanın işbu belgeyi imzalaması ile yürürlüğe girer.

d) Taahhütname iki kopya olarak hazırlanır. Bir kopyası Denetçi/Uzmanda, diğer kopyası ise Kurumda kalır.

Yükümlülükler

Kuruma ait Gizli Bilgilerin korunması ve bilgi varlıklarının kullanım esasları hususunda;

a) Kurum tarafından şahsıma teslim edilmiş veya erişim yetkisi verilmiş olan Gizli Bilgileri; sadece denetim görevi ile ilgili işler için kullanacağımı, koruyacağımı, işleyeceğimi, aktaracağımı; Gizli Bilgileri bilmesi gereken yetkili kişiler haricinde hiç kimse ile paylaşmayacağımı, edindiğim her türlü Gizli Bilgiyi sır olarak saklayacağımı ve tüm bu yükümlülükleri denetim çalışmalarının sona ermesi halinde de süresiz olarak yerine getireceğimi,

b) Görevim kapsamında erişim hakkımın bulunduğu bilgileri, yetkim dâhilinde ya da yetkimi aşarak şahsım dâhil hiçbir kişi, grup, kurum veya kuruluşun menfaati için kullanmayacağımı,

c) Yetkisi olmadığı halde, bulunduğu görev ve makamı kullanarak tarafımdan bilgi talep eden kişileri, Kuruma veya süreci yöneten amire/ilgililere bildireceğimi,

ç) Bilgi sistemlerinde kullanılan/yer alan programları, verileri veya diğer unsurları hukuka aykırı olarak ele geçirme, işleme, değiştirme, silme girişiminde veya eyleminde bulunmayacağımı ve bunları iletip çoğaltmayacağımı,

d) Kurum tarafından şahsıma denetim çalışmaları kapsamında emanet edilen cihazları sadece görevime yönelik faaliyetler için kullanacağımı ve bu cihazlarda Kurumun bilgisi dışında hiçbir mekanik ya da yazılım değişikliği yapmayacağımı/yaptırmayacağımı,

e) Kurum tarafından şahsıma tahsis edilen kaynakları kullanarak gerçekleştirdiğim görevim ile ilgili her türlü faaliyetten, Kurum bilişim kaynaklarını kullanarak oluşturduğum ve/veya şahsıma tahsis edilen Kurum bilişim kaynağı üzerinde bulundurduğum her türlü içerikten (belge, doküman, yazılım gibi) sorumlu olacağımı,

f) Denetim ile ilgili görevimi tamamladığım durumda; Kurum bilgisayarında ve/veya diğer veri depolama ortamlarında elde ettiğim/ürettiğim tüm verileri, bilgileri, belgeleri, eksiksiz olarak ilgilisine teslim edeceğimi ve bunların hiçbir kopyasını almayacağımı,

g) 6698 sayılı Kişisel Verilerin Korunması Kanunu'na uygun hareket edeceğimi,

ğ) İşbu Taahhütname hükümlerine uygun davranmaktan, ihlali halinde ise Kuruma ve üçüncü kişilere vereceğim her türlü zarardan sorumlu olacağımı,

h) İşbu Taahhütnamenin ihlal edilmesi sonucu doğacak tüm hukuki ve idari sorumlukları peşinen kabul ettiğimi, bu taahhütlerimi yerine getirmemem veya ihlal etmem hâlinde her türlü hukuki sorumluluğun şahsıma ait olduğunu

kabul, beyan ve taahhüt ederim.

Tarih

İmza

Taahhüt edenin

Adı Soyadı :

T.C. Kimlik No :

Telefon Numarası :

E-Posta Adresi :

Adresi :

EK – J: TARAFSIZLIK TAAHHÜTNAMESİ ÖRNEĞİ

<İşbu Tarafsızlık Taahhütnamesi örneği, Kurumun denetim ekibinde görev alan kişilere imzalatacağı tarafsızlık taahhütnamesi hazırlanma sürecinde örnek alınmak üzere oluşturulmuştur. Kurum, gereksinimlerine uygun olarak Tarafsızlık Taahhütnamesini özelleştirilebilir.>

Denetlenen Kurum	
Denetim Başlangıç ve Bitiş Tarihi	
Denetim Kapsamındaki Birimler	• • •

a) Bilgi ve İletişim Güvenliği Rehberi uyum çalışmalarını yürüten bilgi işlem biriminde görev almadığımı,

b) Denetim kapsamında yer alan birimlerde birinci, ikinci ve üçüncü derece kan ve sıhri hısımım olan veya maddi/manevi menfaat ilişkimin bulunduğu herhangi bir kişinin bulunmadığını,

c) Denetim başlangıç / denetim işi hizmet alım sözleşmesi tarihinden önceki iki yıl içerisinde Kuruma Bilgi ve İletişim Güvenliği Rehberi uyum faaliyetleri konusunda danışmanlık hizmeti vermediğimi,

ç) Denetim kapsamındaki birim personeline ya da yöneticilerine yönelik olarak herhangi bir önyargımın bulunmadığını,

d) Denetim çalışmaları süresince tarafsızlığımı bozacak ya da tarafsızlığımın bozulduğu intibaı uyandıracak herhangi bir durum ile karşılaşmam halinde, en kısa sürede Kurum ilgililerine bu durumu bildireceğimi

kabul, beyan ve taahhüt ederim.

Tarih

İmza

<u>Taahhüt edenin</u>

Adı Soyadı :

T.C. Kimlik No :

Telefon Numarası :

E-Posta Adresi :

Adresi :

BİLGİ ve İLETİŞİM GÜVENLİĞİ DENETİM REHBERİ