Bilgi ve İletişim Güvenliği Denetimi Rehberleri ve İç Denetim

Bilgi ve İletişim Güvenliği Rehberinin denetiminde iç denetçiler kurum içi paydaş olarak; dış denetçiler ise dış paydaş olarak sorumlu tutulmuşlardır.

Uğur KARAGÖZ / Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Uzman

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ

6 Temmuz 2019 tarihli ve 30823 sayılı Resmi Gazete'de yayınlanan Bilgi ve İletişim Güvenliği Tedbirleri konulu 2019/12 sayılı Cumhurbaşkanlığı Genelge'sinde kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren Bilgi ve İletişim Güvenliği Rehberi'nin hazırlanması hükme bağlanmıştır.

Genelge gereği milli güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir. Denetim sonuçlan ile yapılan düzeltici ve önleyici faaliyetler, Rehberde belirtilen usul ve esaslara göre bir rapor halinde Cumhurbaşkanlığı Dijital Dönüşüm Ofisine (CBDDO) iletilecektir.

Bu genelge kapsamında, CBDDO tarafından hazırlanan Bilgi ve İletişim Güvenliği Rehberi 24.07.2020 tarihinde onaylanarak yürürlüğe girmiştir.

Rehberin temel amacı; bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanması olarak belirlenmiştir.

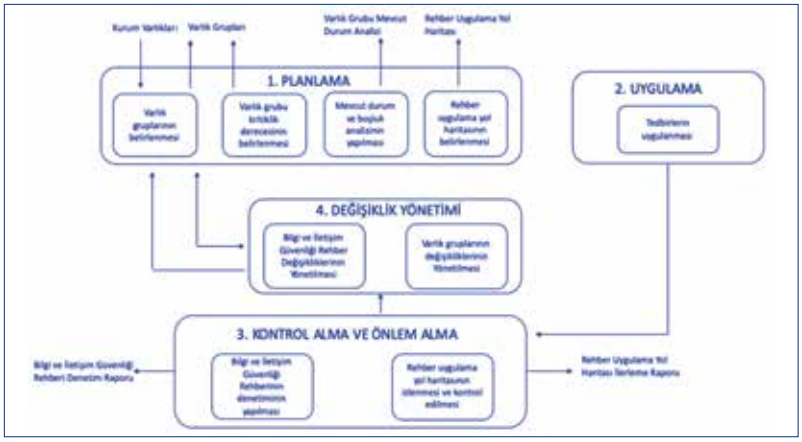
Bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşlar ile kritik altyapı hizmeti veren işletmeler Rehber kapsamına dahil edilmiştir.

Rehber içeriği itibarıyla; ulusal ve uluslararası standart ve rehberler, iyi uygulama örnekleri ve güncel mevzuat dikkate alınarak hazırlanmıştır. Rehberin uygulanabilmesi için kurumlara aşama aşama 24 aylık bir uyum süreci 27 Temmuz 2022 tarihi itibarıyla sona ermiştir. Kurumlar gerek Rehber Uygulama Yol Haritası'nın planlanması gerekse uygulanması aşamalarındaki tüm çalışmalarda aşağıda belirtilen 8 temel prensibi dikkate alacaklardır:

- Yetkin personel
- Mükerrer çalışma ve yatırımların önlenmesi
- En zayıf halkanın tespiti
- Asgari yetki tanımlama
- Saldırı yüzeyinin azaltılması
- Bilmesi gereken prensibi
- Güvenlik temelli tasarım
- Mahremiyet temelli tasarım
- Derinlemesine savunma
- Güvenlik hedeflerinin iş hedefleriyle uyumu
- Yerli ve milli ürünlerin tercih edilmesi

Yukarıda yer alan temel prensipler doğrultusunda Kurumlar uygulama sürecine ilişkin olarak 4 eksenden oluşan süreci yürüteceklerdir. Planlama ile başlayan bu süreç değişiklik yönetimi ile son bulmaktadır. Süreçteki önemli nokta; her bir adımın birbiri ile ilişkili olması ve bir aşamadaki çıktı niteliğindeki hususun diğer aşama veya aşamaların girdisi haline gelebilmesidir.

Rehberin uygulanmasına ilişkin denetimler, gerekli mekanizmalar oluşturularak, yılda en az bir kez olmak üzere iç denetim yolu ile gerçekleştirilir.



Bilgi ve İletişim Güvenliği Rehberinin denetiminde iç denetçiler kurum içi paydaş olarak; dış denetçiler ise dış paydaş olarak sorumlu tutulmuşlardır. Bu kapsamda, iç denetim birimlerinin Bilgi ve İletişim Güvenliği Rehberine dayanarak Bilgi Teknolojisi (BT) denetimini yılda en az bir kere yaparak, denetim raporlarının bir örneğini de CBDDO'ya göndermeleri gerekmektedir. Dolayısıyla yapılan bu yasal düzenleme ile kamu iç denetçilerinin yılda en az bir kere BT denetimi yapmaları zorunlu olmuştur. Bilgi ve iletişim güvenliği rehberinde alınan tedbirler ve bu tedbirlere yönelik denetim maddeleri, denetim yöntem önerileri ile denetim soru örnekleri detaylı bir şekilde ele alınmıştır. Söz konusu rehberde BT denetiminde kullanılabilecek denetim yöntemleri aşağıdaki gibi belirtilmiştir.

- Mülakat
- Gözden geçirme
- Güvenlik denetimi
- Sızma testi
- Kaynak kod analizi

Rehberin uygulanmasına ilişkin denetimler, gerekli mekanizmalar oluşturularak, yılda en az bir kez olmak üzere **iç denetim yolu** ile gerçekleştirilir. Denetim faaliyetleri Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan ve https://www.cbddo.gov.tr adresinde yayımlanan Bilgi ve İletişim Güvenliği Denetim Rehberi esas alınarak yürütülür.

BİLGİ VE İLETİŞİM GÜVENLİĞİ REHBERİ UYGULAMA SÜRECİ İÇİN SORUMLULUK ATAMA MATRİSİ

Matrise göre iç denetçilerin rolleri şunlardır:

- Varlık gruplarının belirlenmesinde

  Bilgilendirilen (görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel)

- Mevcut durum ve boşluk analizi yapılması

  Bilgilendirilen (görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel)

- Bilgi ve iletişim güvenliği denetiminin yapılması

  sorumlu (görevi gerçekleştiren personel)

- Bilgi ve iletişim güvenliği rehber değişikliklerinin yönetilmesi

  bilgilendirilen (görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel)

- Varlık gruplarının değişikliklerinin yönetilmesi

  Bilgilendirilen (görev yapıldıktan sonra görevin bittiği konusunda bilgilendirilen personel)

BİLGİ VE İLETİŞİM GÜVENLİĞİ DENETİM REHBERİ

Bilgi ve İletişim Güvenliği Rehberine uyum sağlarken yerine getirilmesi gereken adımlardan biri olan ve her yıl periyodik olarak yapılacak denetim faaliyetlerinin yürütülmesi konusunda CBDDO tarafından Bilgi ve İletişim Güvenliği Denetim Rehberi de hazırlanarak 27 Ekim 2021 tarihinde yayımlanmıştır.

Rehberde denetimi yapmakla görevli personel şu şekilde belirtilmiştir.

> *"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 veya iç denetim birimi olmasına rağmen denetimi yürütecek yeterlik ve yetkinlikte denetçiye sahip olunmadığı durumlarda iç denetim birimi/iç denetçi veya bilgi işlem birimi tarafından yazılı olarak üst yöneticiye bildirilmesi suretiyle denetimin kurum içi diğer personelin veya diğer kamu kurum ve kuruluşlarından görevlendirilecek personelle veya hizmet alımı yolu ile yapılmasına olanak sağlanmıştır.

Rehbere göre denetim ekibinin belirlenmesinde, gerçekleştirecek ekipteki denetçi sayısı ve denetçilerin uzmanlık alanları; Kurum bilgi varlıkları, iş süreçleri, bilgi sistemlerinin karmaşıklığı dikkate alınmalıdır. 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 Rehber'de yer alan 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.

Yayımlanan 2 Rehbere ek olarak Bilgi ve İletişim Güvenliği Rehberi uyum denetimlerini gerçekleştirecek firma ve personelinin yeterlilik ve yetkinliklerini belirlemek amacıyla CBDDO tarafından "Bilgi ve İletişim Güvenliği Rehberi Uyum Denetimi Hizmeti Sağlayan Personel ve Firma Belgelendirme Programı" da hazırlanmıştır.

Belgelendirme programında uyum denetimlerini gerçekleştirecek denetçi ve başdenetçi profilleri tanımlanmakta; bu doğrultuda başvuruların alınması, eğitim ve sınav faaliyetlerinin gerçekleştirilmesi, denetçi ve başdenetçilerin sertifikalandırılması, firmaların belgelendirilmesi, sertifika ve belgelerin yenilenme süreci yer almaktadır. Program kapsamında düzenlenecek eğitim, sınav ve belgelendirme faaliyetleri CBDDO koordinasyonunda Türk Standartları Enstitüsü (TSE) ve TÜBİTAK Bilgem işbirliği ile yürütülmektedir.

Rehber kapsamına giren kurum ve kuruluşlar için belirlenen denetim metodolojisi 3 aşamadan oluşmaktadır.

1. Denetimin Planlanması
   a. Denetim ekibinin belirlenmesi
   b. Kurumun anlaşılması
   c. Denetim kapsamının belirlenmesi
   d. Denetim strateji ve programının oluşturulması
2. Denetim prosedürlerinin uygulanması
   a. Rehber uygulama sürecinin etkinliğinin değerlendirilmesi
   b. Tedbirlerin etkinliğinin değerlendirilmesi
   c. Bulguların tespiti, değerlendirilmesi ve izlenmesi
3. Denetim sonuçlarının raporlanması
   a. Denetim raporunun hazırlanması ve kuruma sunulması

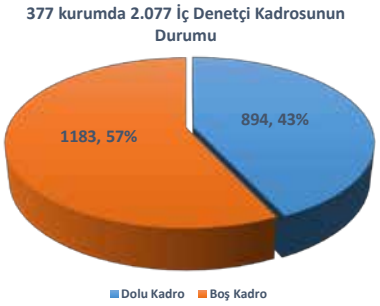
SONUÇ

CBDDO tarafından yayımlanan rehberlerin güncel olması ve iç denetçilere doğrudan BT denetimi yetkisi vermesi kurum içi denetim mekanizmasının güçlendirilmesi açısından son derece önemlidir. İç Denetim Koordinasyon Kurulu tarafından yayımlanan Kamu Bilgi Teknolojileri Denetim Rehberi'nin Ocak 2014 tarihli olmasına rağmen bu Rehberde de BT denetimine ilişkin yol gösterici pek çok husus bulunmaktadır. Özellikle Rehber'de bahsedilen 3 seviye denetim yetkinliğine bakacak olursak;

- 1. Seviye (Başlangıç seviyesi): Kamu idarelerinde iç denetim faaliyetlerinde bulunmuş ve Temel BT Denetimi Eğitimi'ne katılmış iç denetçinin bulunduğu seviyedir.
- 2. Seviye (Gelişmekte olan seviye): Kamu idarelerinde iç denetim faaliyetlerinde bulunmuş ve Temel BT Denetimi ve İleri BT Denetimi Eğitimlerine katılmış ve kamu kurumlarında en az 1-2 yıl BT denetimi çalışmalarında bulunmuş iç denetçinin bulunduğu seviyedir.
- 3. Seviye (Uzman seviyesi): CISA sertifikasına sahip ya da sınavı almaya hazır seviyede gerekli eğitimlerini tamamlamış, BT denetimi alanında en az 2-3 yıl tecrübeye sahip iç denetçinin bulunduğu seviyedir.

Rehber'de 3. seviye bir denetimi sadece Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association-ISACA) tarafından verilen Uluslararası Sertifikalı Bilgi Sistemleri Denetçisi (Certified Information Systems Auditor CISA) tarafından yapılabileceği belirtilmiştir.

Gerek Rehber hükümleri gerekse dijital dönüşümün başta siber güvenlik olmak üzere güvenlik ve kalite unsurlarının giderek önem kazanması BT Denetimini her zamankinden daha önemli bir noktaya taşımıştır. BT denetiminin sadece teknik veya idari açıdan bir bakış açısı ile etkili şekilde yapılamayacağı aşikârdır. Bu söz konusu denetimlerin niteliği itibarı ile daha spesifik, teknik, kritik ve sürekli güncel içeriğe sahip bileşenlerden oluşmasından dolayı kurumların BT alanında iç denetimin yapılmasına yönelik kurum içi farkındalığın artırılması, eğitim ve sertifikalandırma süreçlerine ağırlık verilmesi ve iç denetçilerin bu alanda daha etkili denetim yapmalarına ilişkin gerekli tedbir ve düzenlemelerin yapılmasının önemli olduğu görülmektedir.



Boş iç denetçi kadrolarına bir an önce atama yapılmasının sadece BT denetimini güçlendirmek açısından değil kurumların optimizasyonu sağlamak açısından da gerekli olduğunu söylemek mümkündür. İç Denetim Koordinasyon Kurulu tarafından 24.08.2022 tarihli kamu idarelerindeki iç denetçi kadrolarına ilişkin tablo incelendiğinde 377 kamu idaresinde 2.077 iç denetçi kadrosunun %57'sinin boş olduğu anlaşılmaktadır.

Bakanlık düzeyine bakıldığında 17 bakanlık ortalamasının iç denetçi kadroları açısından yaklaşık %50'sinin boş olduğu görülmektedir. Boş kadro yüzdesi açısından ilk 5'teki bakanlıklara bakıldığında %87 ile Milli Savunma Bakanlığı ilk sırada yer alırken, %72 ile İçişleri Bakanlığı 5. Sırada yer almaktadır. Çalıştırılan iç denetçi sayısı açısından 41 dolu kadronun 33 ünü dolduran Tarım ve Orman Bakanlığı ilk sıradadır. Kadro doluluk oranı açısından ise ilk sıradaki bakanlık Çalışma ve Sosyal Güvenlik Bakanlığı olmuştur.

KURUM	Boş Kadro Yüzdesi
Milli Savunma Bakanlığı	87,1
Dışişleri Bakanlığı	86,7
Milli Eğitim Bakanlığı	77,5
Hazine ve Maliye Bakanlığı	74,5
İçişleri Bakanlığı	72
Çevre, Şehircilik ve İklim Değişikliği Bakanlığı	60
Ticaret Bakanlığı	58,5
Ulaştırma ve Altyapı Bakanlığı	55
Gençlik ve Spor Bakanlığı	50
Sağlık Bakanlığı	49,1
Sanayi ve Teknoloji Bakanlığı	40
Enerji ve Tabii Kaynaklar Bakanlığı	33,3
Adalet Bakanlığı	25
Aile ve Sosyal Hizmetler Bakanlığı	25
Kültür ve Turizm Bakanlığı	25
Tarım ve Orman Bakanlığı	19,5
Çalışma ve Sosyal Güvenlik Bakanlığı	6,7

Dijital Türkiye yolunda BT güvenliğinin sağlanması için denetim kilit rol oynamaktadır. İlerleyen süreçte bu alandaki ihtiyacın artarak ortaya çıkacağı öngörülmektedir. Bu nedenle düzenleyici belge ve dokümanlar genel standart ve çerçeveyi belirlerken kurumlar BT denetimini öncelikleri arasına alarak söz konusu belge ve standartlara uyumu sağlamalı, kurum içi politika ve stratejilerini hayata geçirmelidirler.