

Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ



Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi
25/03/2022 25 Mart 2022 Tarihli Resmi Gazete Sayı:
31789 Bankacılık Düzenleme ve Denetleme Kurumund...

Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ

Tarih: 25 Mart 2022

Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi 25/03/2022

25 Mart 2022 Tarihli Resmi Gazete

Sayı: 31789

Bankacılık Düzenleme ve Denetleme Kurumundan:

BİRİNCİ BÖLÜM

Başlangıç Hükümleri

Amaç ve kapsam

MADDE 1- (1) Bu Tebliğin amacı, 31/12/2021 tarihli ve 31706 altıncı mükerrer sayılı Resmî Gazete'de yayımlanan [Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmelik](#) kapsamında hazırlanacak olan bağımsız denetim raporunun içerik ve şekline ilişkin usul ve esasları

belirlemektir.

Dayanak

MADDE 2- (1) Bu Tebliğ; Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimi Hakkında Yönetmeliğin 38 inci maddesinin ikinci fıkrası uyarınca düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3- (1) Bu Tebliğde geçen;

a) Bilgi sistemleri bağımsız denetimi: Yönetmeliğin 24 üncü maddesinde yer alan denetimi,

b) BT: Bilgi Teknolojilerini,

c) Denetçi: Yönetmeliğin 4 üncü maddesinin birinci fıkrasında tanımlanan denetçiyi,

ç) Denetim alanı: Ek-1'de verilen denetim başlıklarını,

d) Denetlenen: Yönetmeliğin 4 üncü maddesinin birinci fıkrasında tanımlanan denetleneni,

e) İş süreçleri bağımsız denetimi: Yönetmeliğin 25 inci maddesinde yer alan denetimi,

f) Kayda değer kontrol eksikliği: Yönetmeliğin 6 ncı maddesinin birinci fıkrasında tanımlanan kayda değer kontrol eksikliğini,

g) Kontrol: Yönetmeliğin 4 üncü maddesinin birinci fıkrasında tanımlanan kontrolü,

ğ) Kontrol hedefi: Yönetmeliğin 4 üncü maddesinin birinci fıkrasında tanımlanan kontrol hedefini,

h) Kontrol zayıflığı: Yönetmeliğin 6 ncı maddesinin birinci fıkrasında tanımlanan kontrol zayıflığını,

ı) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

- i) Kurum: Bankacılık D zenleme ve Denetleme Kurumunu,
- j)  nemli kontrol eksikliđi: Y netmeliđin 6 ncı maddesinin birinci fıkrasında tanımlanan  nemli kontrol eksikliđini,
- k) Y netmelik: Bilgi Sistemleri ve İř S reçleri Bađımsız Denetimi Hakkında Y netmeliđi,
- ifade eder.

İKİNCİ BÖLÜM

Genel Kavramlar

Rapor hazırlanırken uyulması gereken ilkeler

MADDE 4- (1) Denetçi, raporun tam, dođru, objektif, inandırıcı ve konunun m saade ettiđi  lç de aık ve  z olmasına ařađıdaki hususları dikkate alarak  zen g sterir:

a) Denetçi, raporun tam olmasını raporda denetim amalarının tamamını karřılayan bilgilere yer vererek; raporlanmış hususları, bu hususların yeterli ve dođru bir Őekilde anlaşılmasını sađlayacak biimde sunarak ve raporun ieriđine iliřkin bu Tebliđde ifade edilen gereksinimleri sađlayarak temin eder.

b) Denetçi, raporun dođru olmasını; sunulan bulguların gerekten var olmasıyla ve bu bulguların dođru bir Őekilde sunulmasıyla temin eder. Raporun dođruluđu ve g venilirliđi, raporda sunulan b t n bulguların dođru bir Őekilde aktarılmasıyla sađlanır. Raporda sadece denetçinin alıřma kađıtlarında konuyla alakalı yeterli delille desteklenen bilgi, bulgu ve yargılara yer verilir. Denetim aısından  nemli g r len verilerden bazılarının denetlenmemesi veya denetlenememesi durumunda denetçi bunu raporunda aıka belirtir, varsa verinin kısıtlamalarını rapora ekler ve bu konuya iliřkin raporda herhangi bir yargıda bulunmaz.

c) Denetçi, raporun objektif olmasını, raporun ieriđinde yer

alan unsurları dengeli bir şekilde sunarak ve sunum yaklaşımında tarafsız bir duruş sergileyerek sağlar. Raporun inandırıcılığı açısından rapordaki delillerin tarafsız bir şekilde sunulması gereklidir. Denetçi, raporun tarafsız olmasını ve yanıltıcı olmamasını sağlamakla yükümlüdür. Rapor, raporda yer alan bulgulara dayanılarak hareket edilebilecek bir yaklaşımla sunulur. Denetçi raporunda savunmaya ya da suçlamaya yönelik bir dil kullanmamaya özen gösterir.

ç) Denetçi, raporunun inandırıcı olmasını; denetim sonuçlarının denetim amaçlarını karşılama, bulguların ikna edici bir şekilde sunulması ve raporda yer verdiği yargıların denetim kanıtları tarafından iyi bir şekilde desteklenmesi ile sağlar. Denetçi, raporunda bulgularının geçerliliği ve yargıların makullüğü hakkında yeterli ve ikna edici bilgilere yer verir.

d) Denetçi, raporunun açık olmasını, akıcı ve anlaşılır ifadeler kullanarak temin eder. Raporda herhangi bir şeyi saklamayan, açık, yalın ve mümkün olduğunca teknik olmayan bir dil kullanılır. Teknik terimlerin veya kısaltmaların kullanıldığı durumlarda, bu terimler ayrıca açıklanır ve kullanılan kısaltmalara ilişkin bilgilere raporda ayrı bir bölümde yer verilir. Raporda kısa ve etken fiilli cümleler kullanılmasına özen gösterilir. Denetçi raporda gerekli gördüğü yerlerde konunun daha iyi anlaşılmasını sağlamak amacıyla grafik, tablo ve resim gibi görsel araçlardan faydalanır.

e) Denetçi raporunda ifade etmek istediklerini mümkün olduğunca kısa ve öz bir şekilde ifade eder, vermek istediği mesajı gölgeleyebilecek gereksiz detaylardan ve tekrarlardan kaçınır.

Bulgular

MADDE 5- (1) Denetçi, yeterli ve uygun denetim kanıtlarıyla desteklenecek şekilde kayda değer kontrol eksikliklerini ve

önemli kontrol eksikliklerini sınıflandırır ve Ek-2'de belirlenen esaslara göre kodlayarak raporunda yer verir.

(2) Denetçi, bulguları ifade ederken, denetim amaçlarının gerektirdiği kadarıyla, bu bulguların kriter ve durumlarına ilişkin bilgilere aşağıda tanımlandığı şekliyle yer verir:

a) Kriter: Bulgunun ilişkili olduğu alanla/faaliyetle ilgili olarak bu alanın/faaliyetin olması gerektiği durumu veya bu alandan/faaliyetten ne beklendiğini ifade eder.

b) Durum: Bulgunun ilişkili olduğu alanın/faaliyetin mevcut uygulanma şekli veya durumu ile kriter ve bu durum arasındaki farkların temel sebeplerini ifade eder.

(3) Kriterde mevzuat aykırılığı varsa denetçi bu durumu ilgili mevzuat hükmüne açıkça referans vererek ve aykırılığı oluşturan durum ile mevzuat hükmü bağlantısını net ifadelerle açıklayarak rapora konu eder.

(4) Kontrol zayıflığı olarak tanımlanan bulgular, denetçi tarafından denetlenenin yetkililerine yazılı olarak iletilir. Denetçi, böyle bir yazının denetlenenin yetkililerine iletildiğine dair ifadeye ve Ek-1'de yer alan denetim alanlarında tespit ettiği kontrol zayıflıklarının sayısına raporunda yer verir.

(5) Denetçi, geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş olan tüm bulguları değerlendirir, bu bulguların son durumlarına, devam edip etmediklerine ve denetlenen tarafından taahhüt edilen aksiyon planına uyumuna ilişkin açıklamalarına raporunda yer verir. Bu süreçte raporda bulgunun güncel durumuna ve ilgili kriterlerine yer verilir.

(6) Denetçi, topladığı denetim kanıtlarına dayanarak sahtecilik, kanun dışı uygulamalar, suistimal, çift kayıt sistemi veya mükerrer bilgi sistemleri gibi hallerden bir veya birkaçının bulunduğu kanaatine varırsa, raporun tamamlanmasını

beklemeden söz konusu bulgulara ilişkin olarak ivedilikle Kuruma bilgi verir.

(7) Denetçi, raporunda yer verdiği tüm bulguları usul ve esasları Kurumca belirlenecek şekilde elektronik ortamda Kuruma iletir. Kuruma yapılan bildirimlerin güncel durumu yansıtması gerekmektedir. Kuruma bildirilen bilgilerle raporda yer alan bilgilerin uyumluluğu esastır.

Denetlenenin görüşleri

MADDE 6- (1) Denetçi bulgular, sonuçlar ve varsa planlanan düzeltme çalışmaları hakkında denetlenenin görüşlerini raporlar.

(2) Denetçi, geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş bulgulara ilişkin denetlenenin görüşlerine ve denetlenenin bulgunun giderilmesine ilişkin yaptığı çalışmalara raporunda yer verir.

(3) Denetçi, denetlenenin görüş bildiremediği veya görüş bildirmeyi reddettiği durumlara, nedenleriyle birlikte raporunda yer verir.

Bulgularla ilgili sonuç değerlendirmesi

MADDE 7- (1) Denetçi, raporda denetim amaçları, denetim bulguları ve varsa denetlenenin görüşlerini yorumlayarak kendi çıkarımları ve görüşleri doğrultusunda değerlendirmelerle ihtiyaç varsa açıklamalarına yer verir.

(2) Denetçi, denetlenenin görüşlerine katılmadığı veya planlanan düzeltme çalışmalarının uygun olmadığını düşündüğü takdirde buna sonuç değerlendirmesinde ayrıca yer verir. Denetçi, denetlenenin görüşlerini haklı bulması halinde, raporda ilgili düzeltmeleri yapar.

(3) Herhangi bir bulgunun düzeltildiğine dair bir beyanın rapor tarihinden önce denetlenen tarafından denetçiye ulaşması durumunda, tespit edilen her bir bulgu için birer defaya

mahsus olmak koşuluyla, denetçi denetlenenin beyanını doğrulamak için bu bulgunun son durumunu tahlil eder, bulgunun ortadan kalktığı kanaatine ulaşırsa bulgunun düzeltildiğine dair yargısına raporun bulguya ilişkin sonuç değerlendirmesi bölümünde yer verir.

(4) Denetçi, bulgulara ait sonuç değerlendirmesi bölümünde bulgunun devam durumunu; "devam etmektedir", "kısmen düzeltilmiştir" veya "düzeltilmiştir" şeklinde raporunda ifade eder.

(5) Denetçi, geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş olan bulgulara ait sonuç değerlendirmesi bölümünde bulgunun aksiyon planının yeterliliği ve uyumluluğuna da yer verir.

(6) Denetçi, raporda düzeltildiğini beyan ettiği bulgularda, mümkün olan hallerde riskin gerçekleşmesi durumunu kontrol ederek sonuç değerlendirmesinde bu bilgiye yer verir.

ÜÇÜNCÜ BÖLÜM

Rapor İçeriği

İçerik

MADDE 8- (1) Denetçinin hazırlayacağı rapor aşağıdaki unsurları içerecek şekilde düzenlenir:

- a) Başlık.
- b) Raporun sunulduğu merci.
- c) Yönetmeliğin 32 nci maddesi kapsamında oluşturulan denetim mektubu.
- ç) Yönetici özeti.
- d) İçindekiler.
- e) Denetim çalışmasına ilişkin bilgi.

- f) Denetlenenin bilgi sistemleri hakkında genel bilgi.
- g) Denetlenenin iç kontrol ve iç denetim yapısına ilişkin değerlendirme.
- ğ) İş süreçleri bağımsız denetimi bölümü.
- h) Bilgi sistemleri bağımsız denetimi bölümü.
- ı) Kısaltmalar.
- i) Sözlük.

Yönetici özeti

MADDE 9- (1) Yönetici özeti aşağıda belirtilen şekilde hazırlanır:

a) Denetçi, bu bölümde denetimin amaçlarını tanımlar ve bu denetim amaçlarına erişmek için uyguladığı denetimin kapsam ve metodolojisini özet olarak açıklar.

1) Denetçi, neden bu görevi üstlendiğini ve bu raporun hazırlanış amacını içerecek şekilde, denetim amaçlarını açık ve net olarak ifade eder.

2) Denetçi, denetim çalışmasının önemlilik kavramı çerçevesinde belirlenen kapsamını açık ve net bir şekilde ifade eder. Denetim kapsamını sınırlayan herhangi bir durum var ise, bu sınırlamalar da açık bir şekilde denetim kapsamında ifade edilir.

b) Yapılan denetim çalışmasına ilişkin olarak genel bir değerlendirmeye yer verilir.

c) Cari ve geçmiş dönemlerde tespit edilen bulguların özetlendiği bir tablo Ek-4'de tanımlanan örneğe uygun olarak doldurulur.

ç) Denetçinin tespit ettiği bulgular arasından öne çıkanlar ve bu bulguların taşıdıkları iş risklerine yer verilir.

d) İş süreçleri bağımsız denetimi ve yapıldıysa bilgi sistemleri bağımsız denetimi sonucunda ortaya çıkan bulgular da dikkate alınarak, denetlenenin durumu hakkında genel bir değerlendirmeye yer verilir.

Denetim çalışmasına ilişkin bilgi

MADDE 10- (1) Denetçi, denetim amaçlarını gerçekleştirmek için yapılan denetim çalışmasına ilişkin olarak;

a) Denetim çalışması yürütülürken dikkate alınan önemli varsayımlara,

b) Denetimi gerçekleştirdiği denetlenen birimlere veya şubelere,

c) Denetim kapsamındaki süreçlerle ilgili sorumlularının unvan ve erişim bilgilerine,

ç) Kuruma raporlanan denetçi listesiyle aynı olacak şekilde, ayrılan denetçiler dâhil denetime katılan tüm denetçilerin yer aldığı denetim ekibi ve denetimin başlama/bitiş tarihlerine,

rapordaki denetim çalışmasına ilişkin bilgi bölümünde yer verir.

Denetlenenin bilgi sistemleri hakkında genel bilgi

MADDE 11- (1) Bilgi sistemlerinin değerlendirilmesi kısmı aşağıdaki hususları içerir:

a) BT bölümü çalışan profili hakkında bilgi.

b) Denetlenenin denetim alanlarından sorumlu yöneticilerine ait doğrudan iletişim sağlanabilecek iletişim bilgileri.

c) BT bölümünün organizasyon yapısına dair bilgi.

ç) Denetlenenin faaliyetlerini yürütmesinde kullanılan uygulamalar/sistemler/araçlar hakkında genel bilgi.

- d) Denetlenenin bilgi sistemi mimarisi hakkında özet bilgi.
- e) Denetlenenin ağ altyapısının anlatılması ve ağ topolojisi.
- f) Denetlenenin faaliyetleri ile ilgili yazılımların ve araçların bilgi sistemleri mimarisi üzerinde gösterimi.
- g) Bilgi sistemleri denetimi yapılmışsa, değişiklik yönetimi, güvenlik yönetimi gibi kritik kontrol hedeflerini destekleyen araçlar hakkında özet bilgi.

Denetlenenin iç kontrol ve iç denetim yapısına ilişkin değerlendirme

MADDE 12- (1) Denetçi, raporun bu bölümünde aşağıdaki hususlara yer verir:

- a) İç denetim biriminin, finansal raporlama sistemlerine ilişkin iç kontrollerinin denetimi kapsamında yapmış olduğu planlamaların, faaliyetlerin ve denetim sonuçlarının takibinin değerlendirilmesi.
- b) Yönetimin finansal raporlama sistemlerine ilişkin iç kontrollerin tesis edilmesi ve sağlıklı bir şekilde işletilmesine verdiği önem, söz konusu kontrollerin yeterliğini ve etkinliğini ölçmedeki performansının değerlendirilmesi.
- c) Yöneticilerin finansal raporlama sistemlerine ilişkin iç kontrollerle ilgili risk değerlendirme sürecinin değerlendirilmesi.

(2) Denetçi, BT denetim ekibiyle ilgili olarak;

- a) Ekibin profilini,
- b) Faaliyetlerini,
- c) Yapmış oldukları denetim çalışmalarını,
- ç) Organizasyon içerisindeki yerlerini,

raporunda belirtir.

(3) Denetçi, bu bölümün sonunda bu bölüm kapsamında tespit ettiği her bir bulgu için Ek-3'te yer alan tabloyu doldurur. Geçmiş dönemlerde tespit edilmiş ve bir önceki dönem raporunda halen giderilmediği ifade edilmiş olan bulgular da aynı tablo formatında sunulur.

İş süreçleri bağımsız denetimi

MADDE 13- (1) Denetçi, iş süreçleri üzerindeki kontrollerinin etkinlik, yeterlilik ve uyumluluğuna ilişkin yaptığı denetim sırasında kullandığı önemlilik değerlendirmesini ve bu değerlendirme sonucunda hangi süreçleri seçtiğini, seçim nedenlerini ve seçmediği süreçleri neden seçmediğini açık ve net bir şekilde ifade eder.

(2) Denetçi, denetlenenin faaliyetlerine ilişkin süreçlere dair denetlenen tarafından kendisine sunulan iş akış diyagramlarını ve bu diyagramlarda yer verilen süreçler üzerindeki kontrollerine ilişkin kendi çalışmasını özetleyen tabloyu Ek-5'te belirtildiği şekliyle doldurarak raporuna ekler.

(3) Denetçi, denetim esnasında tespit ettiği veya geçmiş dönemden gelen her bir iş süreci bulgusu için Ek-3'te yer alan tabloyu doldurur; bulgulara iş süreçleri bağımsız denetimi bölümü altındaki ilgili oldukları başlık altında yer verir.

(4) Denetçi, süreç üzerindeki kontrollerin, kendilerinden beklenen işlevleri layıkıyla yerine getirme durumlarına ve sürecin bütününe etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmelerine sürece ilişkin bölümün sonunda yer verir.

Bilgi sistemleri bağımsız denetimi

MADDE 14- (1) Denetçi, denetlenenin tabii olduğu mevzuat çerçevesinde yürüttüğü bilgi sistemleri bağımsız denetiminde kullandığı önemlilik değerlendirmesini açık ve net bir şekilde

raporunda ifade eder.

(2) Denetçi, denetlenen her bir denetim alanı ayrı bir başlık altında olacak şekilde mevzuat gereksinimlerinin nasıl gerçekleştirildiğine ilişkin detaylara ve denetim alanı sorumlularına raporda yer verir.

(3) Denetçi, denetim esnasında tespit ettiği veya geçmiş dönemden gelen her bir bilgi sistemleri bulgusu için Ek-3'te yer alan tabloyu doldurur; bulgulara bilgi sistemleri bağımsız denetimi bölümü altındaki ilgili oldukları başlık altında yer verir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Konsolide denetim raporu

MADDE 15- (1) Yönetmeliğin 2 nci maddesi ve 4 üncü maddesinin birinci fıkrasının (j) bendi uyarınca bağımsız denetim kuruluşlarınca gerçekleştirilen banka bilgi sistemleri ve iş süreçlerinin denetimi kapsamına giren bankaların konsolidasyon kapsamındaki ortaklıklarına ilişkin konsolide denetim raporu aşağıdaki bölümleri içerir:

a) Yönetmeliğin 32 nci maddesi kapsamında oluşturulan denetim mektubu.

b) Yönetici özeti.

c) İçindekiler.

ç) Banka iştirakleri ile ilgili Ek-6'da tanımlandığı şekliyle hazırlanan tablo.

d) Denetim çalışmasına ilişkin bilgi.

e) Banka ve ortaklıkların konsolide finansal tabloya etkileri açısından değerlendirilmeleri.

(2) Yönetici özeti bölümünde, 9 uncu maddenin birinci fıkrasının (a) ve (b) bentlerinde belirtilen bilgiler, banka ve ortaklıklarında konsolide finansal tabloya etkileri bakımından öne çıkan bulgular ve bu bulguların konsolide finansal tablo açısından değerlendirmeleri sunulur. Konsolide edilecek finansal bilgiyi üreten bilgi sistemi ve/veya süreç ile banka ve ortaklıklar arasında finansal bilgi akışı hakkında genel bir değerlendirme yapılır.

(3) Banka ve ortaklıkların konsolide finansal tabloya etkileri açısından değerlendirilmeleri bölümünde aşağıdaki hususlar dikkate alınır:

a) Bankada tespit edilen bulgular, konsolide finansal tablo açısından değerlendirilerek sınıflandırılır. Kayda değer kontrol eksikliği ve önemli kontrol eksikliği olarak sınıflandırılan bulgular Ek-3'te yer alan tablolardan uygun olanı ile doldurularak sunulur.

b) Bilgi sistemleri bağımsız denetimine dâhil edilen her ortaklık için aşağıdaki bilgiler sunulur:

1) Ortaklığın adı, ortaklık yapısı (iştirak, bağlı ortaklık ya da birlikte kontrol edilen ortaklık olma durumu), faaliyetleri ve konsolide denetime dahil edilme sebepleri hakkında bilgi,

2) Ortaklıkta, bilgi sistemleri ve iş süreçleri denetimlerinden hangilerinin gerçekleştirildiği, hangi süreçlerin/denetim alanlarının denetlendiği ve bu süreçlerin/denetim alanlarının seçilmesinde kullanılan önemlilik değerlendirmesi sunularak denetim kapsamı,

3) Gerçekleştirilen denetim sonucunda, konsolide finansal bilgilerinin tanımlanması, üretilmesi, kullanılması, doğruluk, bütünlük ve güvenilirliğinin sağlanması konularında, denetime tabi tutulan ortaklığın etkisine ilişkin genel bir değerlendirme,

4) Konsolide finansal tablo açısından değerlendirilerek kayda

deęer ve önemli kontrol eksiklięi olarak sınıflandırılan ve Ek-3'te yer alan tablo doldurularak hazırlanan ortaklıklarda tespit edilen bulgular.

Yürürlükten kaldırılan teblię

MADDE 16- (1) 13/1/2010 tarihli ve 27461 sayılı Resmî Gazete'de yayımlanan Baęımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimine İlişkin Rapor Hakkında Teblię yürürlükten kaldırılmıştır.

Yürürlük

MADDE 17- (1) Bu Teblię yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 18- (1) Bu Teblię hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

[Ekleri için tıklayınız](#)