

## YÖNETMELİK

Bankacılık Düzenleme ve Denetleme Kurumundan:

### BANKALARDA BAĞIMSIZ DENETİM KURULUŞLARINCA GERÇEKLEŞTİRİLECEK BİLGİ SİSTEMLERİ DENETİMİ HAKKINDA YÖNETMELİK

#### BİRİNCİ BÖLÜM Genel Hükümler

##### Amaç

**MADDE 1 – (1)** Bu Yönetmeliğin amacı, bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesiyle ilgili usul ve esasları düzenlemektir.

##### Kapsam

**MADDE 2 – (1)** Bankalar ile bilgi sistemi denetimi raporu oluşturulması amacıyla sınırlı olmak üzere konsolidasyon kapsamındaki ortaklıkları, bankalara bilgi sistemleri hizmeti veren destek hizmeti kuruluşları, bilgi sistemleri denetimi yapmaya yetkili kuruluşlar, bağımsız denetim kuruluşları ve dış hizmet sağlayıcı kuruluşlar 1 inci maddede belirtilen amaçla sınırlı olarak bu Yönetmelik hükümlerine tabidir.

##### Dayanak

**MADDE 3 – (1)** Bu Yönetmelik, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 15 inci maddesi ve 93 üncü maddesinin dördüncü fıkrası hükümlerine dayanılarak hazırlanmıştır.

##### Tanımlar ve kısaltmalar

**MADDE 4 – (1)** Bu Yönetmelikte geçen;

- a) Bağımsız denetim: BDİY'nin 5 inci maddesinin birinci fıkrasında yer alan tanımı,
- b) Bağımsız denetim kuruluşu: BDKYY'nin 7 nci maddesine göre bankalarda denetim yapma yetkisi verilen kuruluşu,
- c) Banka: Kanunun 3 üncü maddesinde geçen banka tanımını,
- ç) BDİY: 31/1/2002 tarihli ve 24657 mükerrer sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim İlkelerine İlişkin Yönetmeliği,
- d) BDKYY: 31/1/2002 tarihli ve 24657 mükerrer sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Yapacak Kuruluşların Yetkilendirilmesi ve Yetkilerinin Geçici veya Sürekli Olarak Kaldırılması Hakkında Yönetmeliği,
- e) Bilgi sistemleri denetimi: Denetlenenlerin faaliyetlerini gerçekleştirmekte kullandıkları yazılım ve donanım gibi tüm bilgi sistemi unsurlarının, bilgi sistemi süreçlerinin, finansal veri üretiminde kullanılan bilgi sistemi ve süreçlerinin ve bunlarla ilgili olarak tesis edilen iç kontrollerin nitelik, işleyiş, yeterlilik, bütünlük, güvenlik ve güvenilirliklerinin değerlendirilmesi ve rapora bağlanması aşamalarından oluşan, esas ve usulleri sözleşme ile belirlenen süreci,
- f) Denetçi: Bilgi sistemleri denetimi yapmak üzere yetkili kuruluş tarafından görevlendirilmiş yetkili meslek personelinin,
- g) Denetlenen: Bankalar ile bilgi sistemi denetimi raporu oluşturulması amacıyla sınırlı olmak üzere konsolidasyon kapsamındaki ortaklıklarını,
- ğ) Kanun: 5411 sayılı Bankacılık Kanununu,
- h) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,
- ı) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,
- i) Yetkili kuruluş: Bilgi sistemleri denetimi yapma yetkisi verilen bağımsız denetim kuruluşunu,

j) Yönetici: Denetlenenin yönetim kurulu, denetim komitesi ve kredi komitesi başkan ve üyeleri ile genel müdür, genel müdür yardımcıları ve imzaları ile denetleneni ilzam eden personeli,  
ifade eder.

## İKİNCİ BÖLÜM

### Yetkilendirme ve Meslek Mensupları

#### Yetkilendirilecek kuruluşlar ile ortaklarında aranan şartlar

**MADDE 5 –** (1) Bankalarda bilgi sistemi denetimi yapma isteyen yetkili kuruluşların;

a) Bankalarda bağımsız denetim yapma yetkisini haiz olması,  
b) Bu Yönetmelik kapsamındaki faaliyetleri yürütecek yeterli sayı ve nitelikte denetçi istihdam etmesi,

şarttır.

(2) Yetkili kuruluş ortaklarının, BDİY ve BDKYY’de yer alan şartlara ilave olarak; denetlenende veya 28/7/1981 tarihli ve 2499 sayılı Sermaye Piyasası Kanununa tabi şirketlerde denetim yapma yetkisi iptal edilmiş olan bağımsız denetim kuruluşlarında ortak veya yetki iptaline neden olan denetim faaliyetinde bağımsız denetçi veya denetçi sıfatıyla yer almamış olması şarttır.

#### Yetki başvurusu sırasında gerekli olan bilgi ve belgeler

**MADDE 6 –** (1) Bilgi sistemleri denetimi faaliyetinde bulunmak isteyen bağımsız denetim kuruluşu tarafından Kuruma verilecek başvuru dilekçesine;

a) Denetçilerin varsa Bilgi Sistemleri Denetçisi Sertifikalarının (CISA), bu Yönetmelik kapsamına ilişkin konularda aldığı veya verdiği eğitimlere ilişkin belgelerin noterce tasdik edilmiş kopyaları,

b) Denetçilerin mesleki tecrübelerini içeren ayrıntılı özgeçmişleri,

c) Denetçilerinin adli sicil belgeleri,

ç) Denetçilerinin birden fazla bağımsız denetim kuruluşunda ortaklığının bulunmadığına ve denetlenenlerde veya 2499 sayılı Sermaye Piyasası Kanununa tabi şirketlerde denetim yapma yetkisi iptal edilmiş olan bağımsız denetim kuruluşlarında ortak veya yetki iptaline neden olan denetim faaliyetinde bağımsız denetçi veya denetçi sıfatı ile yer almadığına dair beyanları,

d) Denetçilerinin mesleki faaliyetler dışında çalışmadıklarına dair beyanları, eklenir.

#### Bilgi sistemi denetimi yapma yetkisinin verilmesi

**MADDE 7 –** (1) Bilgi sistemi denetimi yapma yetkisi almak üzere başvuruda bulunan bağımsız denetim kuruluşlarının ortak ve denetçilerinin bu Yönetmeliğin 6 ncı maddesinde belirtilen bilgi ve belgeler çerçevesinde değerlendirilerek mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından yerinde incelemede bulunulması neticesinde, faaliyet konularını yürütebilecek yeterliliğe sahip oldukları kanaatine varılması halinde, söz konusu yetkili kuruluşlara Kurul kararıyla bankalarda bilgi sistemi denetimi yapma yetkisi verilir.

(2) Bağımsız denetim kuruluşlarının yetkilendirilmeleri sürecinde dikkate alınan hususlar, Kurum tarafından yeniden gözden geçirilebilir.

(3) Bilgi sistemleri denetimi yapma yetkisinin alınmasını sağlayan unsurların sürekliliği esastır. Kurum gerekli gördüğü durumlarda bu unsurların varlığını kontrol edebilir.

(4) Bilgi sistemleri denetimi yapma yetkisi alan bağımsız denetim kuruluşlarının unvanları Kurum internet sitesinde duyurulur.

#### Bilgi sistemi denetimi yapma yetkisinin kaldırılması

**MADDE 8 –** (1) Bu Yönetmelik hükümlerine aykırı hareket ettikleri tespit edilen yetkili kuruluşların, aşağıdaki durumların bir veya birkaçının varlığının tespiti halinde,

aykırılıkların mahiyetine bağılı olarak, Kurum tarafından yapılan deęerlendirme üzerine Kurul, bilgi sistemleri denetimi yapma yetkisinin geici veya srekli olarak kaldırılmasına karar verebilir.

a) Bilgi sistemine iliřkin olarak denetlenenin gerek durumunu yansıtmayan, eksik, yanlış veya yanıltıcı rapor dzenlenmesi,

b) Yapılan bilgi sistemi denetimlerinde, bilgi sistemi denetimi szleřmesinde yer alan unsurların gerekleřtirilmemesi veya eksik gerekleřtirilmesi,

c) Denetilerin, denetlenenler ile Kuruma nceden bilgi verilmeden deęiřtirilmesi,

) Kesintisiz olarak beř hesap dnemi itibarıyla denetlenenlerde bilgi sistemleri denetimi faaliyetinde bulunulmaması,

d) Bu Ynetmelik hkmlerine uygun bilgi sistemleri denetimi yapılmaması,

e) Kurumca yapılan uyarılara uyulmaması veya uyarı konusu yapılan hususların tekrar edilmesi,

f) Yetkili kuruluřun ve ortaklarının bu Ynetmelięin 5 inci maddesinde belirtilen řartları kaybetmesi,

g) Bu Ynetmelięin 6 ncı maddesi uyarınca verilmesi gereken belgelerin gereęe aykırı olması,

ę) Bu Ynetmelięin 11 inci maddesinde belirtilen ykmllklerin yerine getirilmemesi,

h) Bu Ynetmelięin yetkili kuruluř ve denetinin ykml olduęu dięer maddelerinde belirtilen hususlara aykırı iřlemlerin tespit edilmesi,

i) Denetim planı ile alıřma kaęıtlarının yapılan bilgi sistemleri denetimi alıřmalarını ve bulgularını kanıtlayamaması,

i) Yeterli denetim kanıtı elde edilememesi,

j) Bilgi sistemleri ve finansal veri retim srelerinin gvenilirlięini nemli lde etkileyecek hususların tespiti halinde, yetkili kuruluř tarafından bu Ynetmelikte tanımlanan esas ve usullere tam olarak uyulduęunun kanıtlanamaması,

k) Kurumca istenilen bilgi ve belgelerin verilmemesi.

(2) Yetkinin geici veya srekli olarak kaldırılmasından nce ilgili yetkili kuruluřun savunması alınır. Savunma istendięine iliřkin yazının teblię tarihinden itibaren bir ay iinde savunma verilmemesi halinde savunma hakkından feragat edildięi kabul edilir.

(3) Dzenlemelere aykırılıkların giderilmesi veya bildirim ykmllklerinin yerine getirilmesi iin Kurumca verilen sre iinde, yetkili kuruluřların bilgi sistemleri denetimi yapma yetkisi geici olarak Kurulca kaldırılabilir.

(4) Bu madde kapsamında yetkili kuruluřun bilgi sistemleri denetimi yetkisinin kaldırılması baęımsız denetim yetkisinin de kaldırılması anlamına gelmez. Yetkili kuruluřun baęımsız denetim yetkisini kaybetmesi, bilgi sistemleri denetimi yetkisinin kaldırılmasını gerektirir.

(5) Yetkili kuruluřun, bilgi sistemleri denetimini bu Ynetmelięin 27 nci maddesi erevesinde dıř hizmet alımı ile gerekleřtirmiř olması durumunda da bu madde hkmleri geerlidir.

(6) Bilgi sistemleri denetimi yapma yetkisi kaldırılan baęımsız denetim kuruluřlarının unvanları Kurum internet sitesinde duyurulur.

#### **Meslek mensubu unvanları**

**MADDE 9 –** (1) Denetiler kıdem sırasına gre; sorumlu bilgi sistemleri bařdenetisi, bilgi sistemleri bařdenetisi, kıdemli bilgi sistemleri denetisi, bilgi sistemleri denetisi ve bilgi sistemleri deneti yardımcısı unvanlarını alırlar.

(2) Sorumlu bilgi sistemleri bařdenetisi, yetkili kuruluřta bilgi sistemleri bařdenetisi unvanını haiz ve bilgi sistemleri denetim alıřmasını, yetkili kuruluř adına kendi kiřisel

sorumluluğu ile yürüten ve yetkili kuruluş adına bilgi sistemleri denetimi raporlarını imzalamaya yetkili kişiyi ifade eder.

(3) Bilgi sistemleri başdenetçisi unvanının kazanılması için fiilen en az 10 yıl, kıdemli bilgi sistemleri denetçisi unvanının kazanılması için fiilen en az 6 yıl, bilgi sistemleri denetçisi unvanının kazanılması için fiilen en az 3 yıl bilgi sistemi denetimi, profesyonel bilgi sistemleri kontrolü veya güvenliği tecrübesi şarttır. Bilgi Sistemleri Denetçisi Sertifikası (CISA) sahibi olan ve finansal alanda görev yapan denetim elemanlarının mesleklerindeki tecrübeleri de bu kapsamda değerlendirilebilir. Meslek unvanı için gereken tecrübe, bilgi sistemi denetimi, profesyonel bilgi sistemi kontrolü veya güvenliği konularının herhangi birinde veya birkaçında geçen sürelerin toplamından oluşur. Bilgi Sistemleri Denetçisi Sertifikası (CISA), yukarıda sayılan sürelerle ilave olarak, 1 yıl bilgi sistemleri denetimi tecrübesi yerine sayılır. Bilgi, yetenek ve liyakatları bir üst kademeye gerektirdiği nitelikte olmayanlar sürelerini doldursalar dahi bağımsız denetim kuruluşunun yetkili organlarıncaya bir üst unvana terfi ettirilemezler.

(4) Bu Yönetmelik kapsamındaki yetkili kuruluşların bilgi sistemi denetimiyle görevlendirilmiş meslek mensuplarının tümü, yılda en az yirmi saat, üç yılda en az yüz yirmi saat bilgi sistemi denetimi alanında sürekli eğitim programları kapsamında eğitim aldığı veya verdiğini belgelemelidir. Söz konusu belgeler yetkili kuruluşlar tarafından muhafaza edilir.

## **ÜÇÜNCÜ BÖLÜM**

### **Tarafların Yükümlülükleri**

#### **Denetlenenin yükümlülükleri**

**MADDE 10 –** (1) Denetlenen, bilgi sistemlerinden, bunlara ait dokümantasyondan, finansal bilgi üretim süreçlerine ait dokümantasyon ile her türlü kayıt, bilgi, belge, yapı ve uygulamadan, bilgi sistemleri kapsamındaki her türlü genel ve uygulama kontrolleri ile iç kontrol sisteminin tesis edilmesinden, yeterliliğinden, verimli ve etkin çalışmasından sorumludur.

(2) Denetlenen, öncelikle bilgi sistemi dokümantasyonunu, finansal bilgi üretim süreçlerine ait dokümantasyonu ve bu dokümantasyonla ilgili her türlü kayıt, bilgi, belge, yapı ve sistemlerini bilgi sistemleri denetimine uygun ve hazır hale getirmek zorundadır.

(3) Denetlenen, denetçinin bilgi sistemleri denetimine yönelik talep ettiği her türlü bilgi ve belgeyi vermekle yükümlüdür.

(4) Denetlenen, denetçilere faaliyetlerinde kullandıkları tüm sistem ve uygulamaları ve kullanım amaçlarını kapsayan uygulama listesini bildirmekle yükümlüdür. Uygulama kontrolleri, denetlenen tarafından, finansal veri üretim süreçlerini ve içerdikleri verileri oluşturan, destekleyen, kullanan ve saklayan tüm sistemler ve uygulamalar için belirlenir, değerlendirilir ve raporlanır. Bu kontrollerin değerlendirilmesinde, sistemlerin yazılı dokümantasyonlara uyumu, yazılı kontrollerin yeterliliği ve uygulanması, içerdikleri verilerin güvenliği, bütünlüğü ve sürekliliği gözden geçirilir.

(5) Denetlenen, bu Yönetmeliğin 14, 15, 16 ve 17 nci maddelerinde yer alan genel kontrol konusu her bir sürece ilişkin olarak aşağıda sayılan hususlara uygun bir ortam tesis eder:

a) Süreç sahibi: Her genel kontrol konusu süreç için sorumluluğu açıkça tanımlanmış bir süreç sahibi atanır.

b) Tekrarlanabilirlik: Genel kontrol konusu süreçler tekrarlanabilir biçimde tanımlanır.

c) Hedefler ve amaçlar: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açıkça tanımlanmış hedefler ve amaçlar oluşturulur.

ç) Roller ve sorumluluklar: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açık bir şekilde roller, faaliyetler ve sorumluluklar tanımlanır.

d) Süreç performansı: Belirlenen hedeflere göre her genel kontrol sürecinin performansı ölçülür.

e) Politikalar, planlar ve prosedürler: Her bir genel kontrol süreciyle ilgili politikalar, planlar ve prosedürler yazılı hale getirilir, belli aralıklarla gözden geçirilir, güncellenir, onaylanır ve tüm ilgili birimlere duyurulur.

### **Yetkili kuruluşların ve denetçilerin yükümlülükleri**

**MADDE 11** – (1) Denetçi, ortaya çıkan hata ve suiistimaller hakkında denetlenenin yöneticilerine her aşamada bilgi vermek zorundadır.

(2) Bu Yönetmeliğin 6 ncı maddesinde belirtilen belge ve beyanlardaki değişikliklerin beş iş günü içinde Kuruma bildirilmesi zorunludur. Ana sözleşme, yönetim ve organizasyon yapılarındaki değişiklikler ile bilgi sistemleri denetim kadrosunda meydana gelen her türlü değişikliğin gerekçeleri ile bildirilmesi gereklidir.

(3) Yetkili kuruluşlar, istihdam ettikleri bilgi sistemleri denetçilerinin süreklilik arz edecek şekilde eğitim programlarına katılmalarını sağlamakla yükümlüdür.

(4) Yetkili kuruluş, sözleşme süresi içinde bilgi sistemleri denetiminden çekilmesi ya da sözleşmenin feshedilmesi hallerinde, durumu gerekçesiyle birlikte beş iş günü içerisinde Kuruma bildirmek zorundadır.

(5) Bilgi sistemleri denetçisi; mesleğin zorunlu kıldığı mesleki ilkelere ve bu Yönetmelik ile BDİY’de belirlenen denetim ilkelerine uymak, bilgi sistemleri içerisinde yer alabilecek riskleri ve zayıflıkları dikkate alarak ve mesleki şüphecilik çerçevesinde bir bilgi sistemleri denetimi planı hazırlamak, denetlenene sunmak ve uygulamak, yöneticilerin açıklamalarını yeterli denetim kanıtı olarak kabul etmemek ve bilgi sistemlerine ve finansal veri üretim süreçlerine ilişkin bilgi sistemleri denetimi raporunu oluşturmak ile yükümlüdür.

(6) Bilgi sistemleri denetimi faaliyeti sırasında uygunsuz işlemlerin, suiistimal veya hataların tespiti durumunda, denetlenen bunları gidermiş olsa dahi bu hususun bilgi sistemleri denetçisi tarafından ivedilikle Kuruma ve yöneticilere bildirilmesi ve bilgi sistemleri denetimi raporunun bu çerçevede hazırlanması zorunludur. Adli yargıya intikali gerekli olan ve suç teşkil eden hallerin de Kuruma yazılı olarak ivedilikle bildirilmesi şarttır.

(7) Denetçi, yöneticileri bilgi sistemleri denetimi sırasında ortaya çıkan, aşağıda belirtilen konular da dahil olmak üzere, önemli bulduğu her konuda yazılı veya sözlü olarak derhal bilgilendirir:

a) Muhtemel kısıtlamalar ve ilave çalışmalar da dâhil olmak üzere bilgi sistemleri denetiminin genel yaklaşımı ve kapsamı,

b) Bilgi sistemleri üzerinde önemli bir etkisi olan ya da olabilecek bilgi sistemleri politika oluşturma süreci ile ilgili aksaklıklar, politika uygulamalarındaki sorunlar ya da politika uygulamalarındaki değişiklikler,

c) Banka faaliyetlerinin sürekliliği üzerinde şüphe uyandırabilecek belirsizlikler,

ç) Bilgi sistemlerine veya bilgi sistemleri denetimi raporuna etkisi önemli olabilecek konularda yöneticilerle olan görüş aykırılıkları,

d) Bilgi sistemleri içerisinde yer alan önemli zayıflıklar ve riskler.

(8) Sözlü olarak bilgilendirmenin yapıldığı durumlarda denetçi çalışma kâğıtlarında bildirilen hususları ve alınan cevapları belgelendirir.

(9) Denetçiler, bilgi sistemleri denetimi çerçevesinde ilgililerce kendilerine tevdi edilen dokümantasyon ve belgeleri işlerinin gerektirdiği süre içinde iyi niyetle ve değiştirmeden muhafaza etmekle ve işin bitiminde iadesiyle yükümlüdürler. Denetim kanıtı oluşturan dokümanların kopyaları yetkili kuruluş tarafından saklanabilir.

(10) Yetkili kuruluşlar ve denetçiler, bilgi sistemleri denetimi faaliyetleri dolayısıyla öğrendikleri ve ilgili düzenleme hükümlerine göre sır kapsamında bulunan bilgileri kanunen açıkça yetkili kılınanlardan başkasına açıklayamaz ve doğrudan veya dolaylı şekilde kendi yararlarına kullanamazlar.

(11) Denetlenen tarafından bilgi sistemleri denetimine ilişkin bilgi ve belgelerin yetkili kuruluşa verilmemesi halinde bu durum Kuruma ivedilikle bildirilir.

(12) Bilgi sistemleri denetimi faaliyetinin düzenli ve etkin bir şekilde yapılmasını engelleyen denetçi, bankaların bilgi sistemleri denetiminde görev alamaz ve bu amaçla düzenlenen denetçi listesinde ismine yer verilemez.

(13) Yetkili kuruluşlar, bilgi sistemleri denetiminin gerçekleştirileceği dönemde, denetlenenin bağımsız denetim faaliyetini de yürütüyor olmak zorundadırlar.

## **DÖRDÜNCÜ BÖLÜM**

### **Bilgi Sistemleri Denetimi**

#### **Bilgi sistemleri denetiminin kapsamı**

**MADDE 12** – (1) Yetkili kuruluşlar, denetlenenin faaliyetlerinin kapsam ve yapısını dikkate alarak bilgi sistemlerine dair; Planlama ve organizasyon, Tedarik ve uygulama, Hizmet sunumu ve destek ile İzleme ve değerlendirme ana başlıkları kapsamındaki süreçlere ilişkin genel kontroller ile uygulama kontrollerini önemlilik ilkesi çerçevesinde denetlemek, değerlendirmek; bilgi sistemleri yönetim süreçlerinin düzeyini ortaya koyan olgunluk modeline göre durumlarını belirlemek ve raporlamak zorundadır.

(2) Bilgi sistemleri denetimi, yetkili kuruluşlar tarafından, denetçiler ve yardımcıları eliyle gerçekleştirilir. Bilgi sistemleri denetiminin gerçekleştirilebilmesi için bağımsız denetim kuruluşunun bilgi sistemleri denetimi yetkisini haiz olması ve bu Yönetmelik kapsamında, denetlenenle bilgi sistemleri denetimi sözleşmesi yapmış olması gereklidir.

(3) Uygulama kontrolleri, BDKYY kapsamında denetçi olarak tanımlanan yetkili meslek personeli tarafından, denetçiler arası işbirliği gereksinimlerine uygun olarak bilgi sistemleri denetçisi ile birlikte gerçekleştirilir.

#### **Bilgi sistemleri denetimi türleri**

**MADDE 13** – (1) Bilgi sistemleri denetimi, kapsam bakımından üçe ayrılır. Bunlar uygulama kontrollerinin denetimi, genel kontrol alanlarının denetimi ile uygulama kontrolleri ile genel kontrol alanlarının birlikte gerçekleştirildiği geniş kapsamlı denetimdir.

(2) Uygulama kontrolleri, asgari olarak bu Yönetmeliğin 18 inci maddesinde açıklanan kontroller üzerinden kapsam açısından önemlilik ve uygulanabilirlik kriterleri ölçüsünde denetlenir. Genel kontrol alanlarının denetimi ise bu Yönetmeliğin 14, 15, 16 ve 17 nci maddelerinde açıklanan genel kontrol alanlarının denetlenmesi ile gerçekleştirilir. Bu Yönetmelikteki uygulama kontrolleri kavramı, 8/2/2001 tarihli ve 24312 sayılı Resmî Gazete’de yayımlanan Bankaların İç Denetim ve Risk Yönetimi Sistemleri Hakkında Yönetmelik’te geçen iç kontrol sistemi ile paralel anlamda kullanılmıştır.

(3) Uygulama kontrolleri her yıl, genel kontrol alanları ise iki yılda bir kez denetlenir. Kurul, gerekli gördüğü hallerde herhangi bir banka veya tüm bankalar için, denetim türlerinden herhangi birinin kapsamını ve/veya denetim sıklığını farklılaştırabilir.

(4) Denetçi, denetim sürecinde denetlenenin bu Yönetmeliğin 10 uncu maddesinin dördüncü fıkrası çerçevesinde tesis etmek durumunda olduğu hususları değerlendirir.

#### **Planlama ve organizasyon faaliyetlerinin denetimi**

**MADDE 14** – (1) Planlama ve organizasyon faaliyetleri, iş hedeflerinin yerine getirilmesi amacıyla bilgi teknolojileri desteğinin en uygun verilme şeklinin belirlenmesine yönelik strateji ve yöntemleri içerir. Farklı bakış açılarını içerecek şekilde planlanan stratejiler, organizasyon içerisinde ilgili birim ve kişilere iletilir. Teknolojik alt yapının, sağlıklı bir örgütsel yapı içerisinde verimli ve etkin çalışabileceği hususu bilgi sistemleri denetimi sürecinde dikkate alınır.

(2) Planlama ve organizasyona ilişkin genel kontroller çerçevesinde;

a) Stratejik bilgi teknolojileri planının tanımlanması,

b) Bilgi mimarisinin tanımlanması,

- c) Teknolojik yönün belirlenmesi,
  - ç) Bilgi teknolojisi süreçlerinin, organizasyonunun ve ilişkilerinin tanımlanması,
  - d) Bilgi teknolojisi yatırımlarının yönetimi,
  - e) Yönetimin amaçlarının ve talimatlarının iletilmesi,
  - f) İnsan kaynakları yönetimi,
  - g) Kalite yönetimi,
  - ğ) Bilgi sistemleri riskinin değerlendirilmesi ve yönetimi,
  - h) Proje yönetimi,
- süreçleri ile ilgili kontrol hedefleri denetlenir.

#### **Tedarik ve uygulama faaliyetlerinin denetimi**

**MADDE 15** – (1) Tedarik ve uygulama faaliyetleri, bilgi teknolojisi stratejilerinin gerçekleştirilmesiyle ilgili bilgi teknolojisi çözümlerinin tanımlanması, geliştirilmesi veya harici destek sağlayıcılardan temin edilmesi, uygulanması ve iş süreçleriyle bütünleştirilmesini kapsar. Sistemlerdeki bakımlar ve değişiklikler de bu kontrol alanında değerlendirilir.

(2) Tedarik ve uygulamaya ilişkin genel kontroller çerçevesinde;

- a) Otomasyon çözümlerinin belirlenmesi,
  - b) Uygulama yazılımının geliştirilmesi ve bakımı,
  - c) Teknoloji alt yapısının oluşturulması ve bakımı,
  - ç) Operasyon ve kullanımın sağlanması,
  - d) Bilgi sistemleri kaynaklarının karşılanması,
  - e) Değişiklik yönetimi,
  - f) Sistem çözümlerinin ve değişikliklerin uygulanması ve akredite edilmesi,
- süreçleri ile ilgili kontrol hedefleri denetlenir.

#### **Hizmet sunumu ve destek faaliyetlerinin denetimi**

**MADDE 16** – (1) Hizmet sunumu ve destek faaliyetleri, gerekli eğitimin verilmesi de dahil olmak üzere ihtiyaç duyulan hizmetlerin güvenli ve sürekli bir şekilde sunulmasını ifade eder.

(2) Hizmet sunumu ve destek faaliyetlerine ilişkin genel kontroller çerçevesinde;

- a) Hizmet seviyelerinin tanımlanması ve yönetimi,
  - b) Üçüncü kişilerden alınan hizmetlerin yönetimi,
  - c) Performans ve kapasite yönetimi,
  - ç) Hizmet sürekliliğinin sağlanması,
  - d) Sistem güvenliğinin sağlanması,
  - e) Maliyetlerin belirlenmesi ve dağıtılması,
  - f) Kullanıcıların eğitimi,
  - g) Hizmet sunumu yönetimi ve olay yönetimi,
  - ğ) Konfigürasyon yönetimi,
  - h) Problem yönetimi,
  - ı) Veri yönetimi,
  - i) Fiziksel çevre yönetimi,
  - j) Operasyon yönetimi
- süreçleri ile ilgili kontrol hedefleri denetlenir.

#### **İzleme ve değerlendirme faaliyetlerinin denetimi**

**MADDE 17** – (1) İzleme faaliyetleri, bilgi teknolojilerine ilişkin tesis edilen kontrollerin uygunluk ve kalitesinin, denetlenen tarafından düzenli aralıklarla değerlendirilmesini kapsar.

(2) İzlemeye ve değerlendirmeye ilişkin genel kontroller çerçevesinde;

- a) Bilgi sistemleri performansının izlenmesi ve değerlendirilmesi,
- b) İç kontrolün izlenmesi ve değerlendirilmesi,

- c) Denetlenenin iç usul ve esasları dahil ilgili mevzuata uyumun sağlanması,  
ç) Bilgi sistemlerine ilişkin kurumsal yönetişimin temini,  
süreçleri ile ilgili kontrol hedefleri denetlenir ve değerlendirilir.

#### **Bilgi sistemleri uygulama kontrolleri**

**MADDE 18 –** (1) Uygulama kontrolleri, bilgi sistemleri içerisinde yer alan ve bankacılık faaliyetlerini yürütmek veya desteklemek için kullanılan finansal verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi gibi tüm iş süreçlerinde kullanılması gereken iç kontrollerin etkinliğinin ve yeterliliğinin denetlenmesini ve değerlendirilmesini kapsar.

(2) Uygulama kontrolleri, denetlenenin iş süreçlerinin kontrolünü ifade eden iş döngüsü kontrolleri içerisinde yer alan, bilgisayar destekli ve/veya manüel yordamlarla gerçekleştirilen özelleşmiş kontrollerdir.

(3) Uygulama kontrolleri aşağıdaki unsurları içerir;

a) Veri oluşturma/yetkilendirme kontrolleri:

1) Veri hazırlama prosedürleri: Girdi form tasarımları, hataların ve eksikliklerin en aza indirilmesine yardım eder. Veri oluşturma sürecinde kullanılan hata ele alma prosedürleri, hataların ve düzensizliklerin tespit edilmesini, raporlanmasını ve düzeltilmesini temin eder.

2) Kaynak belge yetkilendirme prosedürleri: Yetkilendirilmiş personel, yetkilerine uygun bir biçimde kaynak belgeleri hazırlar. Kaynak belgelerin oluşturulması ve onaylanması konusunda görevler ayrılığı prensibine göre hareket edilir.

3) Kaynak belge verilerinin toplanması: Yetkilendirilmiş kaynak belgelerin bütünlüğünü ve doğruluğunu, hesap verilebilirliğini ve zamanında iletimini temin eden prosedürler bulunmalıdır.

4) Kaynak belgelerdeki hataların ele alınması: Veri oluşturma sürecinde kullanılan hata ele alma prosedürleri, hataların ve düzensizliklerin tespit edilmesini, raporlanmasını ve düzeltilmesini temin eder.

5) Kaynak belgelerin muhafazası: Gerektiğinde veriye ulaşılabilmesini sağlamak amacıyla, orijinal kaynak belgelerin yeterli bir süre boyunca saklanmasını veya yeniden oluşturulabilir biçimde tutulmasını temin etmek için prosedürler bulunmalıdır.

b) Girdi kontrolleri:

1) Girdi yetkilendirme prosedürleri: Yalnızca yetkilendirilmiş kaynaklardan veri girişi yapılabilmesini temin eden prosedürler bulunmalıdır.

2) Doğruluk, bütünlük ve yetkilendirme kontrolleri: Personel veya sistem tarafından üretilen, ya da ara yüzlerden işlenmek üzere girilen hareket verileri doğruluk, bütünlük ve geçerlilik kontrolü için çeşitli testlere tabi tutulur. Ayrıca, girdi verilerinin kaynak noktasına en yakın yerde değiştirilmesini ve onaylanmasını temin eden prosedürler bulunmalıdır.

3) Veri girdilerindeki hataların ele alınması: Hatalı girilen verilerin düzeltilmesini ve tekrar işleme alınmasını temin eden prosedürler bulunmalıdır.

c) Veri işleme kontrolleri:

1) Veri işlemede bütünlük: Veri işleme prosedürleri, görevler ayrılığı prensibine uyulmasını ve yapılan işlerin doğrulanmasını temin eder. Bu prosedürler ayrıca, çalıştırmadan çalıştırmaya kontrol toplamları ve esas dosya güncelleme kontrolleri gibi yeterli güncelleme kontrollerinin varlığını da temin eder.

2) Veri işlemede onaylama ve değiştirme: Veri işlemede onaylama, kullanıcı doğrulaması ve değiştirilmenin kaynak noktasına en yakın yerde gerçekleştirilmesini temin eden prosedürler bulunmalıdır.

3) Veri işlemedeki hataların ele alınması: Veri işlemedeki hataların ele alınmasına ilişkin prosedürler, hatalı hareketlerin işlenmeden belirlenmesini sağlar ve diğer geçerli hareketleri kesintiye uğratmasını engeller.

ç) Çıktı kontrolleri:

1) Çıktıların ele alınması ve muhafazası: Bilgi sistemleri uygulamalarının çıktılarının ele alınması ve muhafazasında belirlenmiş prosedürler izlenmeli, gizlilik ve güvenlik gereksinimleri dikkate alınmalıdır.

2) Çıktıların dağıtımı: Bilgi sistemleri çıktılarının dağıtımı ile ilgili prosedürler tanımlanmış, duyurulmuş ve takip ediliyor olmalıdır.

3) Çıktı uyumluluğu ve mutabakatı: Çıktıların kontrol toplamlarıyla uyumluluğu rutin olarak kontrol edilmelidir. Log kayıtları, hareketlere ilişkin işlemlerin takip edilmesini ve sorunlu verilerle ilgili mutabakat sağlanmasını kolaylaştırır.

4) Çıktıların gözden geçirilmesi ve hataların ele alınması: Çıktı raporlarının doğruluğunun, çıktıları sağlayan kişiler ve uygun kullanıcılar tarafından gözden geçirilmesini temin eden prosedürler bulunmalıdır. Ayrıca, çıktılarda bulunan hataların tanımlanması ve ele alınması ile ilgili de prosedürler olmalıdır.

5) Çıktı raporlarının güvenliğinin sağlanması: Hem kullanıcılara dağıtımı yapılmış hem de dağıtım için bekleyen çıktı raporlarının güvenliğinin sağlanmasıyla ilgili prosedürler bulunmalıdır.

d) Sınır kontrolleri:

1) Aslına uygunluk ve bütünlük kontrolleri: Organizasyon dışında üretilen, telefon, sesli posta, kağıt, faks veya e-posta ile alınmış verinin aslına uygunluğu ve bütünlüğü, veri üzerinde kritik bir işlem yapılmadan uygun bir şekilde kontrol edilmelidir.

2) Hassas bilginin iletim ve nakil esnasında korunması: Hassas bilginin, iletim ve nakil esnasında, yetkisiz erişim, değişiklik ve yanlış yönlendirmeye karşı uygun bir biçimde korunması gerekir.

(4) Denetçi, uygulama kontrollerinin denetlenmesinde;

a) Önemli uygulama bileşenlerinin ve hareketlerin sistem üzerinden akışının tanımlanması, mevcut dokümantasyonun gözden geçirilmesi ve uygun personelle görüşülmesi suretiyle uygulamanın detaylarının anlaşılması,

b) Uygulama kontrollerinin güçlü yanlarının tanımlanması ve toplanan bilgiler incelenerek kontrol zaafalarının test stratejisine etkisinin değerlendirilmesi,

c) Uygun denetim prosedürleri kullanılarak kontrollerin fonksiyonellik ve etkinliklerinin test edilmesi,

ç) Test sonuçlarının ve diğer denetim bulgularının incelenmesi ile kontrol ortamının değerlendirilmesi,

hususlarını dikkate alır.

(5) Uygulama kontrolleri asgari olarak aşağıdaki alanlara ilişkin denetim ve değerlendirme faaliyetlerini kapsar;

a) Mükerrer bilgi sistemleri ve çift kayıt sisteminin varlığının ve bunların önlenmesine ilişkin kontrollerin incelenmesi,

b) Faiz ve gelir tahakkuk ve reeskont hesaplamaları, gider reeskontları ve amortisman hesaplamaları, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, yaşlandırma raporlarının hazırlanması,

c) Muhasebe fişi kesilmesine ilişkin yetkili personelin belirlenmesi ve yetkilendirilmesi süreçleri ile mizanın oluşumu, geriye dönük muhasebe fişi kesilmesi işlemleriyle ilgili yetkilendirmelerin varlığı ve ilgili kayıtların bütünlüğü ve izlenebilirliği, işlem numaralarının ardışıklığının korunmasını sağlamak gibi genel muhasebe kontrolleri, işlem limitlerinin ve yetkilerinin kontrolü,

ç) Elektronik Fon Transferi, Elektronik Menkul Kıymet Transferi ve Takasbank işlemleri, SWIFT işlemleri ve bunlarla ilgili güvenlik kayıtları gibi ödeme sistemi kontrolleri,

d) Nostro, vostro ve loro bakiyelere ilişkin mutabakatlar ve muhabir kayıtları, şube ve genel müdürlük kayıtları arasındaki mutabakatlar, yasal ve yardımcı defterler arası mutabakatlar, banka ile kart merkezi mutabakatları gibi mutabakat kontrolleri,

e) Banka ve kredi kartına limit tahsisi, banka kartlarının kullanımı ve hediye puanı gibi uygulamalara ilişkin kontrolleri,

f) Kredi başvuruları ve onayları, kredi limitleri ile kredi geri ödeme tabloları ve hesaplamalarına ilişkin kontroller, mevduat işlemleri ve mevduatın sınıflandırılması gibi hesaplama ve kontrolleri,

g) Banka kayıtlarının ve bilgi kaynaklarının finansal raporlamalarda kullanım sürecinin kontrolü,

ğ) Menkul kıymet ve fon yönetimi iş süreçlerinin kontrolü,

h) Vade ve valör tarihlerine ilişkin kayıtların güvenilirliği ve bütünlüğünün kontrolü,

i) Elektronik bankacılık/alternatif dağıtım kanalları (internet, telefon, televizyon, WAP/GPRS, Kiosk, ATM, vb) ile ilgili muhasebe ve süreç kontrolleri.

(6) Denetçiler, uygulama kontrolleri ile birlikte, bankaların finansal raporlama sistemi ile ilgili iç kontrollerinin yeterliliğini ve yöneticilerin bu iç kontrollerin yeterliliğini ve etkinliğini ölçmedeki performansını da değerlendirir. Bu değerlendirme kapsamındaki,

a) İç kontrol sisteminin denetim sürecinde;

1) Planlama,

2) Yönetimin iç kontrollerle ilgili değerlendirme sürecinin gözden geçirilmesi,

3) İç kontrollerle ilgili değerlendirmenin oluşturulması,

4) İç kontrollerin tasarımının test edilmesi, etkinliğinin ve yeterliliğinin değerlendirilmesi,

5) İç kontrollerin uygulanmasının test edilmesi, etkinliğinin ve yeterliliğinin değerlendirilmesi,

6) İç kontrollerin etkinliği ve yeterliliği ile ilgili görüşün oluşturulması,

b) Finansal raporlama ile ilgili iç kontrollerde;

1) Kontrol ortamı,

2) Risk değerlendirme süreci,

3) Kontrol faaliyetleri,

4) Bilgi ve iletişim kanalları, yetkilendirme, kayıtların saklanması süreçleri,

5) Oluşturulan kontrollerin denetlenen tarafından izlenmesi

hususları değerlendirilir.

**Bilgi sistemleri denetiminde bilgi kriterleri, teknoloji kaynakları ve yönetsel ölçütler**

**MADDE 19** – (1) Bu Yönetmeliğin 14, 15, 16 ve 17 nci maddelerinin ikinci fıkralarında yer alan süreçler kapsamında gerçekleştirilen her bir kontrol hedefi; uygulanabilirlikleri ölçüsünde bilgi kriterleri, teknoloji kaynakları ve yönetsel ölçütlerin birlikte dikkate alınması suretiyle Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (COBIT) çerçevesinde yer alan yöntemlere uygun olarak değerlendirilir ve denetlenen her bir süreç için uygunluk seviyesi belirlenir. Yönetsel ölçütlerin varlığı, uygunluğu ve bilgi sistemleri gelişimine katkıları, bu hükmün uygulanmasında dikkate alınır.

## **BEŞİNCİ BÖLÜM**

### **Genel İlkeler ve Sorumluluklar**

#### **Bilgi sistemleri denetimi sözleşmesi**

**MADDE 20** – (1) Bilgi sistemleri denetimi, yetkili kuruluş ile denetlenen arasında imzalanacak yazılı sözleşme çerçevesinde yürütülür. Bilgi sistemleri denetimi sözleşmesi, yapılacak bilgi sistemleri denetiminin kapsam ve içeriği üzerinde taraflar arasında tam bir mutabakat sağlandığının göstergesidir. Bilgi sistemleri denetim sözleşmesi, BDKYY'nin 9 uncu maddesi kapsamında yapılacak sözleşmeye dahil edilebilir.

(2) Bilgi sistemleri denetimi sözleşmeleri, denetlenenin yönetim kurulunca onaylanarak yürürlüğe girer. Sözleşmenin bir örneği, yürürlüğe girdikten itibaren beş iş günü içinde denetlenen tarafından Kuruma iletilir.

(3) Yetkili kuruluş, denetlenen ile denetim sözleşmesi yapmadan önce bilgi sistemleri denetiminin kapsam ve planlamasını belirlemek amacıyla gerekli ön araştırmayı yapmak zorundadır. Ön araştırma kapsamında, denetim sürecini olumlu ya da olumsuz etkileyebilecek hususların varlığı ve yetkili kuruluş değişikliği halinde bunun nedenleri ile ilgili olarak önceki dönemlerde denetimi üstlenen yetkili kuruluşlardan bilgi talep edilebilir. Denetlenen, önceki yetkili kuruluşa cari dönem için sözleşme yaptığı yetkili kuruluşun unvanını bildirir ve talep edilen bilgilerin verilmesi için yetkilendirir. Önceki yetkili kuruluş, bu kapsamda kendilerinden talep edilen bilgileri vermek zorundadır.

(4) Bilgi sistemleri denetimi sözleşmelerinde, asgari olarak aşağıdaki unsurların bulunması zorunludur;

- a) Denetçinin uymakla yükümlü bulunduğu düzenlemeler,
- b) Bilgi sistemleri denetiminin amacı, kapsamı, varsa özel nedenleri,
- c) Yetkili kuruluş tarafından anlaşma kapsamında sunulacak hizmetler,
- ç) Tarafların sorumluluk ve yükümlülükleri,
- d) Denetimde görevlendirilecek denetçiler ile bunların yedekleri,
- e) Denetim ekibinde görevlendirilenlerin unvanları, öngörülen çalışma süreleri ve her biri için uygun görülen ücret tutarının ayrıntılı dökümü,
- f) Denetimin başlama ve bitiş tarihleri,
- g) Bilgi sistemleri denetimi raporunun ve istenmesi halinde özel amaçlı denetim raporunun şekli ve bu raporların hazırlanma nedenleri,
- ğ) Denetim raporunun teslim edileceği tarih.

(5) Denetlenen, bilgi sistemleri denetimi sözleşmesine aykırı hareket edildiğini veya denetimin bilgi sistemleri denetimi ilkelerine göre yapılmadığını gerekçe göstermek suretiyle sözleşmeyi feshedebilir ve bu durumu kanıtlarıyla birlikte beş iş günü içerisinde Kuruma bildirir.

(6) Denetçinin çalışma alanının önemli ölçüde sözleşme hükümlerine aykırı olarak sınırlandırılması, bilgi sistemlerine ilişkin bilgi ve belgelerin elde edilememesi veya benzeri durumların oluşması halinde sözleşme, yazılı gerekçe göstermek ve Kuruma önceden bildirimde bulunmuş olması koşuluyla, yetkili kuruluş tarafından feshedilebilir. Yetkili kuruluş bu durumu, denetimden çekilme gerekçeleriyle birlikte derhal Kuruma bildirir. Çekilme halinde, yetkili kuruluşun çalışma kağıtlarını ve gerekli tüm bilgileri, yerine geçecek olan yetkili kuruluşa devretmek üzere Kuruma vermesi zorunludur. Çekilen yetkili kuruluşun yerine geçecek yetkili kuruluşun Kurum tarafından uygun görülmesi şarttır.

(7) Denetçi, denetlenenin bazı faaliyetlerini destek hizmeti kuruluşu aracılığı ile yürütmesi halinde bilgi sistemleri denetimi sözleşmesinde, destek hizmeti kuruluşu ile denetim konularına ilişkin toplantı ve görüşme yapılabilmesini temin eden hükümler bulunmasını sağlar.

#### **Yöneticilerin bilgilendirilmesi**

**MADDE 21** – (1) Bilgi sistemleri ile ilgili önemli risklere uygun kontroller oluşturulmaması sebebiyle denetlenenin bilgi sistemlerinde önemli zayıflıkların doğduğu tespit edilirse, denetçi, Kurum ile denetlenenin yöneticilerini derhal durumdan haberdar eder ve risk değerlendirmesinde bu hususların etkisini dikkate alır.

#### **Belgelendirme**

**MADDE 22** – (1) Denetçi, aşağıdaki hususları belgelendirir;

- a) Bilgi sistemlerinde ve finansal veri üretim süreçlerinde hata ya da suiistimalden dolayı denetlenenin beyan riskine duyarlılığı hakkındaki değerlendirmeler ve ulaşılan önemli kararlar,

b) Kontrol ortamı, denetlenenin yeterli ve düzenli risk ölçüm, kontrol ve yönetim tekniklerine sahip olup olmadığı, bilgi işlem sistemi, kontrol faaliyetleri, kontrollerin izlenmesi dahil, denetlenen ortam hakkında edinilen bilgilerin temel unsurları ve kaynakları ile risk değerlendirme teknikleri,

c) Tespit edilen riskler ve ilgili kontroller.

## ALTINCI BÖLÜM

### Denetlenenin Destek Hizmeti Alması ve Bunların Denetimi

#### Denetlenenin destek hizmeti alması

**MADDE 23** – (1) Denetçi, denetlenenin dış kaynak kullanımı ile gerçekleştirdiği hizmetlerin bilgi sistemlerini ve finansal veri üretim süreçlerini nasıl etkilediğini göz önünde bulundurur, bilgi sistemleri denetimini buna göre planlar ve etkin bir denetim yaklaşımı geliştirir.

#### Destek hizmeti kuruluşunun bilgi sistemleri denetimi raporu

**MADDE 24** – (1) Denetçi, destek hizmeti kuruluşu hakkında hazırlanan bilgi sistemleri denetimi raporunu talep edebilir, destek hizmeti kuruluşunu denetleyen bilgi sistemleri denetçisinin mesleki uzmanlığını, raporun yapısını, içeriğini, kullanılabilirliği ile uygunluğunu inceler ve değerlendirir. Yetkili kuruluş, destek hizmeti kuruluşunu denetleyen denetçi tarafından yapılan bilgi sistemleri denetiminin kapsamını göz önünde bulundurur.

(2) Denetçi, destek hizmeti kuruluşunun bilgi sistemleri denetimi raporunu kullandığında bu raporu kendi hazırladığı raporda referans olarak gösteremez.

## YEDİNCİ BÖLÜM

### Bilgi Sistemleri Denetiminde İşbirliği

#### Denetçiler arası işbirliği

**MADDE 25** – (1) Önceki bilgi sistemleri denetimini gerçekleştiren yetkili kuruluş ve denetçi, bilgi sistemleri denetimine esas teşkil eden her türlü bilgi ve belgeyi gizlilik ilkesi çerçevesinde, bilgi sistemleri denetimini yapacak yetkili kuruluş ve kişilere sağlamakla yükümlüdür.

(2) Denetlenenin iç denetçileri ve iç kontrol faaliyetlerinden sorumlu olanlar, kendi raporları dahil ihtiyaç duyulan bütün bilgileri bilgi sistemleri denetçilerine verirler.

(3) Denetçinin, denetlenenin iç denetim, iç kontrol ve risk yönetim sistemlerinin yeterliliği hakkındaki kanaatine bağlı olarak, denetlenenin iç denetim faaliyetleri ile bilgi sistemleri denetim faaliyetlerinde mümkün olduğunca tekrardan kaçınılmasına özen gösterilir.

#### Kurum ve yetkili kuruluşlar arası işbirliği

**MADDE 26** – (1) Kurum ile yetkili kuruluş ve denetçiler arasında ortak ilgi alanına giren konularda karşılıklı mütalâa veya bilgi teatisinde bulunulmak üzere belirli aralıklarla toplantılar düzenlenebilir. Bu konuda Kurum veya denetçiler tarafından girişimde bulunulabilir.

(2) Kurum tarafından bankalarda yapılan bilgi sistemleri denetimi faaliyetlerinde sağlanan bilgiler, gerektiğinde denetçiler ile paylaşılabilir.

(3) Kurum personeli, yetkili kuruluşların bilgi sistemleri denetimi sürecinin her aşamasına, bilgi ve becerilerini geliştirmek amacıyla, denetçi bağımsızlığı ilkesini zedelemeksizin izleyici sıfatı ile eşlik edebilir. Kurum personeli, yetkili kuruluşun bilgi birikimini şahsına veya bir başka yetkili kuruluşa çıkar sağlamak için kullanamaz. Yetkili kuruluş, Kurum personelinin süreçte yer alması ve bilgi birikimini artırması bakımından gerekli katkı ve çabayı gösterir.

(4) Denetçiler ve yetkili kuruluşlar, Kurumu ilgilendirebilecek veya onun adına ivedi olarak harekete geçilmesini gerektirebilecek;

- a) Bir bankanın varlığını tehlikeye düşürebilecek olgular,
- b) Bilgi sistemlerinin araç olarak kullanıldığı yolsuzluk ihtimali,
- c) Bilgi sistemleri denetçisinin istifa etme niyeti,
- ç) Bankanın faaliyet risklerinin veya olası risklerinin artması,
- d) Kontrol ortamında önemli eksiklikler bulunması,
- e) Bankanın bankacılık yapma yetkisi için gerekli ölçütlerden birini yerine getirmedigini gösteren bilgiler,
- f) Bankanın finansal durumunu önemli ölçüde olumsuz etkileyen veya etkileyebilecek bilgiler,
- g) Bankanın, karar organları ile ciddi bir çatışma, kilit bir konumdaki bir yöneticinin beklenmedik şekilde işten ayrılması gibi idari ve iç kontrol sisteminde önemli bir etkisi olan veya olabilecek bilgiler,
- ğ) Denetlenenin tabi olduğu kanunların, yönetmeliklerin, anasözleşmesinin veya tüzüğünün önemli ölçüde ihlal edildiğini gösteren bilgiler,
- h) Bilgi sistemleri içerisinde yer alan önemli zayıflıklar ve riskler, gibi önemli bilgileri öğrendiklerinde bunları ivedilikle Kuruma bildirir.

## SEKİZİNCİ BÖLÜM

### Bilgi Sistemleri Denetiminde Dış Hizmet Alımı

#### Bilgi sistemleri denetiminin dış hizmet alımı ile gerçekleştirilmesi

**MADDE 27** – (1) Bağımsız denetim kuruluşu, denetlenenin faaliyet yapısını dikkate alarak bilgi sistemleri denetimini dış hizmet alımı ile gerçekleştirebilir. Dış hizmet sağlayıcı kuruluşun bilgi sistemleri denetimini gerçekleştirebilmesi için bu Yönetmelik kapsamında, bağımsız denetim kuruluşu ile sözleşme yapmış olması gereklidir. Bu sözleşme ile bağımsız denetim kuruluşu, dış hizmet sağlayıcı kuruluşun denetim ilkelerine bağlılığını; bu Yönetmelik ve ilgili diğer düzenlemeler kapsamında denetçiler için düzenlenen tüm şartları taşımasını ve ilgili maddelere uymasını sağlamak zorundadır.

(2) Dış hizmet sağlayıcı kuruluşların;

- a) Denetçisinin bu Yönetmelikte tanımlanan denetçi niteliklerini haiz olması,
- b) Bilgi sistemleri denetim ekipleri içerisinde yeterli sayıda denetçi istihdam etmesi,
- c) Denetlenen kuruluşa asgari son üç yıldır yönetim ve danışmanlık hizmeti vermemesi ve ticari ilişki içinde bulunmaması,
- ç) Denetçisinin, denetim ilkelerine bağlı olmak ve denetçi bağımsızlığı ilkesini zedelememek koşuluyla bilgi sistemleri denetiminde görev alması, şarttır.

(3) Bağımsız denetim kuruluşu ile dış hizmet sağlayıcı kuruluş arasında yapılması planlanan sözleşme, denetim çalışması başlamadan önce bağımsız denetim kuruluşu tarafından Kuruma ve denetlenecek bankaya gönderilir ve gerekli mutabakat sağlanır. Yetkili kuruluş, gerçekleştireceği bilgi sistemleri denetiminde dış hizmet alımına yönelik gereksiniminin denetim çalışması başladıktan sonra ortaya çıkması halinde gerekli sözleşme değişikliğini yapmak ve bunları mutabakatları alınmak üzere Kuruma ve denetlenece beş iş günü içinde göndermekle yükümlüdür.

(4) Dış hizmet sağlayıcı kuruluşun, sözleşme süresi içinde denetimden çekilmesi ya da sözleşmenin feshedilmesi hallerinde, bağımsız denetim kuruluşu durumu gerekçesiyle birlikte Kuruma bildirmek zorundadır.

(5) Bağımsız denetim kuruluşunun dış hizmet sağlayıcı kuruluşla sözleşme yapması sorumluluklarını devrettiği anlamına gelmez.

(6) Bağımsız denetim kuruluşu, dış hizmet sağlayıcı kuruluşun performansını ve sağlaması gereken niteliklerde oluşan değişiklikleri anlaşma süresi boyunca izler. Bağımsız denetim kuruluşu, hizmet seviyesi anlaşmalarını, dış hizmet sağlayıcısının iç kontrol mekanizmalarını, denetim ve finansal raporlamalarını değerlendirmek zorundadır.

(7) Bağımsız denetim kuruluşu, uzmanlık alanlarının farklılık göstermesi sebebiyle dış hizmet alımını, bu maddede yazılı olan hususlara uygun olmak koşuluyla, birden fazla dış hizmet sağlayıcı kuruluştan alabilir.

(8) Dış hizmet sağlayıcı kuruluş, bilgi sistemleri denetimini bu Yönetmelik kapsamında gerçekleştirir ve bilgi sistemleri denetimi raporunu bu Yönetmelikte açıklanan hususlara uygun olarak bağımsız denetim kuruluşu ile birlikte imzalar. Dış hizmet sağlayıcı kuruluş, denetim raporunu imzalamakla yetkilendirdiği kişiye sözleşmede açıkça yer vermek zorundadır.

(9) Dış hizmet sağlayıcı kuruluş, mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından yerinde incelenir.

(10) Bir dış hizmet sağlayıcı kuruluş, aynı bankaya sürekli olarak 7 yıldan fazla süreyle bilgi sistemi denetimi hizmeti veremez.

## **DOKUZUNCU BÖLÜM**

### **Bilgi Sistemleri Denetimi Raporu ve Bildirimi**

#### **Bilgi sistemleri denetimi raporu**

**MADDE 28** – (1) Bilgi sistemleri denetimi raporu, önemlilik kavramı da dikkate alınarak, bilgi sistemleri ve finansal veri üretim süreçleri üzerinde değerlendirmelere yer verilen ve bilgi sistemleri denetçisi kanaatinin net bir dille yazılı olarak açıklandığı metindir. Denetçinin görevi, genel kontroller ve uygulama kontrolleri hakkında denetim kanıtlarını toplayıp incelemek, değerlendirmek ve bu kanıtlar üzerinde bir sonuca ulaşarak bilgi sistemleri denetimi hakkında kanaat oluşturmaktır.

(2) Denetçi, denetim çalışmaları sonrasında bilgi sistemleri denetimi raporu düzenlemek zorundadır. Rapora ilişkin esas ve usûller Kurulca yayımlanacak tebliğ ile düzenlenir.

(3) Bilgi sistemleri denetimi raporu, bilgi sistemleri denetiminin gerçekleştirildiği döneme ait faaliyetlerin tamamını kapsar. Tamamlanan raporlar, yetkili kuruluş sorumlu bilgi sistemleri başdenetçisi veya bilgi sistemleri denetimi dış hizmet alımı ile gerçekleştirilmiş ise ilgili firmanın imzalamaya yetkili kıldığı kişi ile BDKYY’de tanımlanan sorumlu ortak baş denetçi tarafından imzalanır. Yetkili kuruluşun, bu Yönetmelikte sayılan tecrübe koşullarını sağlaması kaydıyla, bir sorumlu ortak başdenetçiyi bilgi sistemleri denetimini yürütmekle görevlendirmesi halinde, bağımsız denetim raporu, sorumlu bilgi sistemleri başdenetçisi yerine diğer sorumlu ortak başdenetçi ile birlikte bu kişi tarafından imzalanabilir.

(4) Bilgi sistemleri denetimi raporu, Kurul tarafından aksi belirtilmedikçe denetim dönemini takip eden yılın ilk ayı içerisinde tamamlanır ve yetkili kuruluşu temsil ve ilzama yetkili olanların imzasını taşıyan bir yazı ekinde denetlenenin yönetim kurulu başkanlığına, denetim komitesine, Türkiye Cumhuriyet Merkez Bankasına ve üç nüsha olarak Kuruma iletir. 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu hükümlerine göre oluşturulan güvenli elektronik imza ile imzalanmış bilgi sistemleri denetim raporunun elektronik ortamdaki kopyası da aynı süre içerisinde Kuruma gönderilir. Kurum gerekli gördüğü hallerde söz konusu raporun bağımsız denetim raporuyla birlikte gönderilmesini öngörebilir.

(5) Bilgi sistemleri denetimi raporunun içeriği gizli bilgi niteliği taşır ve herhangi bir ortamda yayımlanmaz. Bu bilgilerin gizliliği ve güvenliği, Kurumun, Türkiye Cumhuriyet Merkez Bankasının, yetkili kuruluşların, bu Yönetmelik kapsamında bağımsız denetim kuruluşlarının, dış hizmet sağlayan kuruluşların ve denetlenenin sorumluluğundadır. Denetlenenler, denetim sonuçlarını içerecek beyanatlar veremezler ve bu hususları reklam amaçlı kullanamazlar.

## **ONUNCU BÖLÜM** **Çeşitli ve Son Hükümler**

### **Bilgi sistemleri denetçilerinin bankalarda görev almaları**

**MADDE 29** – (1) Denetçiler son iki yıl içinde denetim sürecine katıldıkları bankalarda görev alamazlar.

### **Yönetmelikte hüküm bulunmayan haller**

**MADDE 30** – (1) Bu Yönetmelikte hüküm bulunmayan hallerde; BDİY, BDKYY, uluslararası denetim standartlarında benimsenen esaslar, Avrupa Birliği düzenlemelerinin getirdiği normlar ve uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan, Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından yayınlanmış Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (COBIT) dokümanlarında yer alan usul ve esaslar uygulanır.

### **Konsolidasyon kapsamındaki kuruluşların denetimi**

**GEÇİCİ MADDE 1** – (1) Bankalarla konsolidasyon kapsamına giren kuruluşların bu Yönetmelik hükümleri çerçevesinde denetimine 1/1/2007 tarihinden itibaren başlanır.

### **İmza zorunluluğu**

**GEÇİCİ MADDE 2** – (1) 2006 yılı için gerçekleştirilecek bilgi sistemleri denetimine ilişkin sözleşmelerin bu Yönetmeliğin yayımından itibaren 3 ay içinde imzalanması zorunludur.

### **Yürürlük**

**MADDE 31** – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

### **Yürütme**

**MADDE 32** – (1) Bu Yönetmelik hükümlerini Kurum Başkanı yürütür.