BİLGİ SİSTEMLERİ VE İŞ SÜREÇLERİ BAĞIMSIZ DENETİMİ HAKKINDA YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 –(1) Bu Yönetmeliğin amacı, Kurum gözetimi ve denetimi altındaki kuruluşların bilgi sistemleri ile iş süreçlerinin, bu Yönetmelik kapsamında yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesi ile ilgili usul ve esasları düzenlemektir.

Kapsam

MADDE 2 –(1) Kurum gözetimi ve denetimi altındaki kuruluşlar ile bilgi sistemleri bağımsız denetimine ilişkin rapor oluşturulması amacıyla sınırlı olmak üzere bankaların konsolidasyon kapsamındaki ortaklıkları, bilgi sistemleri bağımsız denetimi yapmaya yetkili bağımsız denetim kuruluşları ve bilgi sistemleri bağımsız denetimi yapmak için dış hizmet alınan 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, 36 ncı, 93 üncü ve 95 inci maddeleri, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanununun 14 üncü ve 17 nci maddeleri ile 23/2/2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanununun 27 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 – (1) Bu Yönetmelikte geçen;

a) Bağımsız denetçi: BDY'nin 4 üncü maddesinin birinci fıkrasında tanımlanan bağımsız denetçileri,

b) Bağımsız denetim: BDY'nin 4 üncü maddesinin birinci fıkrasında tanımlanan bağımsız denetimi,

c) Bağımsız denetim kuruluşu (BDK): BDY'nin 4 üncü maddesinin birinci fıkrasında tanımlanan bağımsız denetim kuruluşlarını,

ç) Banka: Kanunun 3 üncü maddesinde tanımlanan bankaları,

d) BBDY: 2/4/2015 tarihli ve 29314 sayılı Resmî Gazete'de yayımlanan Bankaların Bağımsız Denetimi Hakkında Yönetmeliği,

e) BDY: Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunun 26/12/2012 tarihli ve 28509 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Yönetmeliğini,

f) Bilgi alışverişi kuruluşları: 5464 sayılı Kanunun 4 üncü maddesi çerçevesinde faaliyet izni alarak bilgi alışverişinde bulunan kuruluşları,

g) Bilgi sistemleri bağımsız denetimi: Bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ve denetlenenin faaliyetlerine ilişkin süreçler ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreci,

ğ) Bilgi sistemleri bağımsız denetim sicili (Sicil): Kurum tarafından elektronik ortamda tutulan ve bağımsız denetim kuruluşları ile denetçilerin kayıtlarının izlendiği sicili,

h) BSD: Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında bilgi sistemleri ve iş süreçleri bağımsız denetimi ile Kurum gözetimi ve denetimi altındaki diğer kuruluşlarda bilgi sistemleri bağımsız denetimini,

ı) Bilgi sistemleri denetimi dış hizmet kuruluşu (BSDDHK): BBDY kapsamında bankalarda bağımsız denetim yapma yetkisini haiz BDK'nın bu Yönetmelik kapsamında izin alarak BSD faaliyetini gerçekleştirmek için hizmet aldığı dış hizmet kuruluşunu,

i) Denetçi: Yetkili kuruluş ya da BSDDHK tarafından BSD yapmak üzere görevlendirilen ve unvanları 18 inci maddede sıralanan denetçi ile iş süreçleri denetimi faaliyetlerinde bulunan bağımsız denetçiyi,

j) Denetlenen: Kurum gözetimi ve denetimi altındaki kuruluşlar ile bu Yönetmelik kapsamında BSD raporu oluşturulması amacıyla sınırlı olmak üzere bankaların konsolidasyon kapsamındaki ortaklıklarını,

k) Dış hizmet: Bankalarda 5/11/2011 tarihli ve 28106 sayılı Resmî Gazete'de yayımlanan Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamındaki destek hizmetleri dâhil olmak üzere; bu Yönetmelik kapsamındaki denetlenenlerin bilgi sistemlerine ilişkin dışarıdan temin ettikleri verilerin gizliliği, bütünlüğü ve erişilebilirliği ile sunulan hizmetlerinin sürekliliğini etkileme potansiyeli olan verilere erişimi bulunan ya da bu verilerin paylaşıldığı hizmet alımlarını,

l) Diğer finansal kuruluşlar: Bankalar, Risk Merkezi ve bilgi alışverişi kuruluşları hariç Kurum gözetimi ve denetimi altındaki kuruluşları,

m) Genel kontroller: Bilgi sistemlerinden beklenen fonksiyonların doğru bir şekilde yerine getirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli güven ortamının oluşturulmasını ve iş süreçleri üzerindeki kontrollerin işlevselliği için güvenilir bir ortamın sağlanmasını hedefleyen, bilgi sistemlerini oluşturan sistemler, bileşenler, süreçler ve verinin tamamına veya büyük bir bölümüne tatbik edilen kontroller ile bu kontrollerin tatbik edilmesini sağlayan politika ve prosedürleri,

n) İş süreçleri: Bankaların, Kanunun 4 üncü maddesi çerçevesinde yürüttüğü faaliyetlere ilişkin tesis edilen iş süreçleri ile Risk Merkezi ve bilgi alışverişi kuruluşlarının ilgili mevzuatı çerçevesinde yürüttükleri faaliyetler kapsamındaki iş süreçlerini,

o) Kanun: 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununu,

ö) Kontrol: İş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,

p) Kontrol hedefi: Belirli bir bilgi sistemleri aktivitesi içinde kontrol prosedürleri oluşturarak istenen bir sonucun veya bir amacın gerçekleştirilmesini sağlayan hedefleri,

r) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

s) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

ş) Risk Merkezi: Kanunun ek 1 inci maddesi uyarınca Türkiye Bankalar Birliği nezdinde kurulan Risk Merkezini,

t) Yetkili kuruluş: Bu Yönetmelik kapsamında BSD yapma yetkisi verilen BDK'yı,

u) Yöneticiler: Denetlenenin yönetim kurulu, denetim komitesi ve kredi komitesi başkan ve üyeleri ile genel müdür, genel müdür yardımcıları ve imza yetkisine sahip mensuplarından; bölge müdürleri, şube müdürleri ve genel müdürlük merkez teşkilatında yer alan bölüm, kısım, grup ve bunlara eşdeğer isimler altında faaliyet gösteren birimlerin yöneticilerini,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Genel Kavramlar

Önemlilik

MADDE 5 –(1) Önemlilik; mesleki tecrübeye dayalı bir mütalaa konusu olup kontrol zayıflıkları sonucu ortaya çıkan ya da çıkabilecek hataların, ihmallerin, prosedürlere aykırılıkların ve hukuka aykırı fiillerin, denetlenenin finansal verilerini raporlamasına, güvenli ve kesintisiz hizmet sağlamasına olan ya da olabilecek etkisinin değerlendirilmesidir.

(2) BSD'de önemlilik kavramı, denetimin planlanması, gerekli alanlarda yoğunlaştırılması, bulguların değerlendirilmesi ve raporlanması için

kullanılabilir.

(3) Denetlenen açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliği önemlilik kavramı kapsamında dikkate alınması gereken temel unsurlardır.

(4) Finansal raporları etkileyen kontrollerin değerlendirilmesinde, süreç veya sistem tarafından yürütülen finansal işlemin değeri, işlem sıklığı gibi öğeler kullanılırken, finansal işlemlere ilişkin olmayan kontrollerin değerlendirilmesinde ise iş sürecinin kritikliği, sistem ve operasyonların maliyeti, hataların muhtemel sonuçlarının büyüklüğü, bir zaman aralığında gerçekleşen işlem/sorgu sayısı, tutulan dosyaların ve üretilen raporların niteliği, zamanlaması ve kapsamı, hizmet seviyesi anlaşmalarının gerekleri ve ceza maddelerindeki para cezası tutarları gibi öğeler kullanılır.

Kontrol zafiyetlerinin sınıflandırılması

MADDE 6 – (1) Denetçi, incelemeleri neticesinde tespit ettiği kontrol zafiyetlerini önemlilik kavramına göre kontrol zayıflığı, kayda değer kontrol eksikliği ve önemli kontrol eksikliği şeklinde aşağıda belirtilen üç farklı sınıfta tasnif eder:

a) Kontrol zayıflığı: Bir kontrolün tasarımının veya işletilmesinin, hataları zamanında önleme ve tespit etmeye olanak sağlamaması durumudur.

1) Tasarımdaki kontrol eksikliği, bir kontrol hedefinin gerçekleşmesini sağlayacak kontrolün bulunmaması ya da var olan bir kontrolün tasarlandığı şekilde çalışıyor olsa bile tasarımındaki hatalardan dolayı kendisinden beklenen kontrol hedefini gerçekleştirememesi durumudur.

2) İşletimdeki kontrol eksikliği, düzgün tasarlanmış bir kontrolün tasarlandığı şekilde çalışmaması ya da kontrolü gerçekleştiren personelin, kontrolün etkin bir şekilde yerine getirilmesi için gerekli yetki ve yeterliliğe sahip olmaması durumudur.

b) Kayda değer kontrol eksikliği: Denetlenenin verilerinin bütünlüğünün, tutarlılığının, güvenilirliğinin ve gereken durumlarda gizliliğinin sağlanmasına, faaliyetlerinin devamlılığının teminine olumsuz etki yapması muhtemel bir kontrol zayıflığı veya birkaç kontrol zayıflığının bir araya gelmesi sonucu oluşan önemsiz sayılamayacak eksiklik olarak tanımlanır. İş süreçlerinde denetlenenin finansal verilerinin güvenilir bir şekilde genel kabul görmüş muhasebe standartlarına uygun olarak kaydedilmesi, kayıtların yetkilendirilmesi, işlenmesi veya raporlanması sırasında oluşan hataların ve ihmallerin önlenmesine olumsuz etki yapması muhtemel eksiklikler de bu kapsamda değerlendirilir.

c) Önemli kontrol eksikliği: Bilgi sistemlerinin faaliyetlerini, verilerinin bütünlüğü, doğruluğu ile güvenliğini önemli düzeyde etkileyecek ve iş süreçlerinde denetlenenin dönemsel olarak yaptığı finansal raporlamalarında önemli bir yanlışlığın önlenmesini, düzeltilmesini engelleyecek veya bu süreçlere ilişkin bilgilerin bütünlüğünün ve tutarlılığının, güvenilirliğinin, devamlılığının ve gereken durumlarda gizliliğinin sağlanmasına önemli ve olumsuz etki etmesi kuvvetle muhtemel, bir veya birkaç kontrol zayıflığının bir araya gelmesidir.

Etkinlik, yeterlilik ve uyumluluk

MADDE 7 – (1) Bir kontrolün tasarımının etkin olarak kabul edilebilmesi için, tasarımdaki kontrol eksikliğinin bu kontrol bünyesinde bulunmaması veya bulunsa dahi önemli kontrol eksikliğine sebebiyet vermemesi gerekir.

(2) Bir kontrolün işletiminin etkin olarak kabul edilebilmesi için, işletimdeki kontrol eksikliğinin bu kontrol bünyesinde bulunmaması veya bulunsa dahi önemli kontrol eksikliğine sebebiyet vermemesi gerekir.

(3) Bilgi sistemleri ile iş süreçleri üzerindeki kontrollerin yeterli olması;

a) Önemlilik ilkesi çerçevesinde denetime tabi tutulan tüm kontrollerin tasarımlarının etkin olduğunu,

b) Bu kontrollerin; iş hedefleri çerçevesinde kendilerinden beklenen sonucu üretebilecek ve maruz kalınabilecek riskleri telafi edebilecek şekilde tasarlandıklarını,

ifade eder.

(4) Bilgi sistemleri ile iş süreçleri üzerindeki kontrollerin etkin olması;

a) Önemlilik ilkesi çerçevesinde denetime tabi tutulan tüm kontrollerin işletimlerinin etkin olduğunu,

b) Bu kontrollerin, kendilerinden beklenen işlevleri ve kontrol hedeflerini yerine getirdiklerini,

ifade eder.

(5) Bir kontrolün uyumlu sayılabilmesi için kontrole ilişkin kanunlar ve bu kanunlara istinaden yayımlanan alt düzenlemeler ve talimatlarda yer alan hususların ve yükümlülüklerin tamamının karşılanması gerekir. Önemlilik ilkesi çerçevesinde denetime tâbi tutulan tüm kontrollerin uyumlu olması, bilgi sistemleri ve iş süreçleri üzerindeki kontrollerin uyumlu olduğunu ifade eder.

Denetim riski

MADDE 8 – (1) Denetim riski, denetçinin aşağıdaki risklere bağlı olarak doğru görüş vermemesi olasılığıdır:

a) Yapısal risk: Kontrolün olmaması nedeniyle, en azından kayda değer olan bir kontrol eksikliğinin var olması riskini ifade eder.

b) Kontrol riski: Kontrolün beklendiği gibi çalışmaması sebebiyle, en azından kayda değer olan bir kontrol eksikliğini önleyememesi, ortaya çıkaramaması veya zamanında düzeltememesi riskini ifade eder.

c) Tespit riski: Denetçinin, denetlenenin iç kontrol sisteminde yer alan en azından kayda değer olan bir kontrol eksikliğini ortaya çıkaramaması riskini ifade eder.

(2) Önemli veya kayda değer kontrol eksikliği riski: Denetlenenin iç kontrol sisteminde en azından kayda değer olan bir kontrol eksikliğinin bulunması riskini ifade eder. Önemli ya da kayda değer kontrol eksikliği riski, yapısal risk ve kontrol riskinden kaynaklanır.

(3) Denetçi, denetim riskini kabul edilebilir bir seviyeye indirmek için, önemli veya kayda değer kontrol eksikliği riskinin yüksek olduğu alanlarda tespit riskini düşürecek şekilde uygun denetim tekniklerini kullanır.

ÜÇÜNCÜ BÖLÜM
Yetkilendirme, İzin ve Denetçiler

Yetkilendirilecek kuruluşlarda aranan şartlar

MADDE 9 – (1) Bu Yönetmelik kapsamında bankalar, Risk Merkezi ve bilgi alışverişi kuruluşlarında BSD yapmak için yetkilendirilecek kuruluşların;

a) BBDY kapsamında bankalarda bağımsız denetim yapma yetkisini haiz olması,

b) Bu Yönetmelik kapsamındaki faaliyetleri yürütecek yeterli sayı ve nitelikte denetçiye ve etkin bir bilgi sistemine sahip olması,

c) Kalite kontrol sistemine ilişkin yapı ve yazılı politikalar oluşturulması,

şarttır.

(2) Bu Yönetmelik kapsamındaki diğer finansal kuruluşlarda BSD yapmak için yetkilendirilecek kuruluşların;

a) Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından verilen kamu yararını ilgilendiren kuruluşlarda denetim yapma yetkisini haiz olması,

b) Bu Yönetmelik kapsamındaki faaliyetleri yürütecek yeterli sayı ve nitelikte denetçiye ve etkin bir bilgi sistemine sahip olması,

c) Kalite kontrol sistemine ilişkin yapı ve yazılı politikalar oluşturması,

şarttır.

Yetki başvurusu sırasında gerekli olan bilgi ve belgeler

MADDE 10 – (1) BSD faaliyetinde bulunmak isteyen BDK tarafından Kuruma verilecek başvuru dilekçesine, bilgi sistemleri bağımsız denetçilerinin;

a) Mesleki tecrübelerini, denetimle ilgili aldıkları eğitimleri, varsa katılmış olduğu denetim çalışmaları ve bu çalışmalarda almış olduğu görevleri de içeren Ek-1'de yer alan örneğe uygun olarak düzenlenecek ayrıntılı özgeçmişleri, lisans ve/veya lisansüstü eğitimlerine ilişkin diplomalarının/mezuniyet

belgelerinin aslı ya da Kurumca onaylı sureti,

b) Varsa bilgi sistemleri ve bilgi teknolojilerine ilişkin alanlarda sahip oldukları sertifikaların aslı ya da Kurumca onaylı sureti,

c) Bu Yönetmelik kapsamına ilişkin konularda aldığı veya verdiği eğitimlere ilişkin belgelerin kopyaları,

ç) Adli sicil kaydı,

d) Bu Yönetmelik kapsamında uygun görülmüş olan unvanları,

e) Birden fazla BDK'da ortaklığının bulunmadığına dair Ek-2'de yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

f) Denetlenenlerde veya 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununa tabi şirketlerde denetim yapma yetkisi iptal edilmiş olan BDK'larda ortak veya yetki iptaline neden olan denetim faaliyetinde bağımsız denetçi veya denetçi sıfatı ile yer almadığına dair Ek-3'te yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

g) Mesleki faaliyetler dışında çalışmadıklarına dair Ek-4'te yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

ğ) BDK'da tam zamanlı görev yaptıklarına veya yapacaklarına dair Ek-5'te yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

h) Daha önce yapılan ya da yapılacak bir disiplin kovuşturması sonucunda bağımsız denetimin yapılmasına engel teşkil edecek bir ceza alınmadığının ilgili kurumdan talep edilecek belge ile tevsik edilmesi kaydıyla, haklarında diğer yetkili kurumlar tarafından bir disiplin kovuşturması yapılıp yapılmadığına, böyle bir kovuşturma başlatıldığında en geç yedi gün içinde Kurumun bilgilendirileceğine, kovuşturma sonucunda BSD'nin yapılmasına engel teşkil edecek bir ceza alınması halinde bulunulan görevden en geç on beş gün içerisinde istifa edileceğine ilişkin, Ek-6'da yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

ı) BSD faaliyeti sırasında bağımsızlıklarının ortadan kalkması durumunda denetlenene verilen bağımsız denetim hizmetinden çekileceğini taahhüt etmesine yönelik Ek-7'de yer alan örneğe uygun olarak düzenlenecek yazılı taahhüt belgesi,

eklenir.

(2) BDK'nın vereceği hizmetlerden doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptıracaklarına ilişkin beyanlarına da başvuru dilekçesinde yer verilir.

BSD yapma yetkisinin verilmesi

MADDE 11 – (1) BSD yapma yetkisi almak üzere başvuruda bulunan BDK'lar bu Yönetmeliğin 10 uncu maddesinde belirtilen bilgi ve belgeler çerçevesinde Kurum tarafından değerlendirilir. Mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından yapılacak değerlendirme ve gerekirse yerinde incelemeler sonucunda faaliyet konularını yürütebilecek yeterliliğe sahip oldukları kanaatine varılması halinde BSD yapma yetkisi verilir, sicile kaydedilir ve bilgi sistemleri bağımsız denetim kuruluşları listesine eklenir.

(2) Yetki başvurularının değerlendirilmesi sürecinde, Kurum tarafından gerekli görülmesi halinde BDK'nın yetkinliğinin ve yeterliliğinin ölçülebilmesi amacıyla ilave bilgi ve belgeler talep edilebilir. Talep edilen bilgi ve belgeler yetkinin verilmesine ilişkin değerlendirmelerde dikkate alınır.

(3) Bu Yönetmelik kapsamında BSD yapma yetkisinin alınmasını sağlayan unsurların sürekliliği esastır. Kurum gerekli gördüğü durumlarda bu unsurların varlığını kontrol edebilir.

(4) Bu Yönetmelik kapsamında BSD yapma yetkisi verilen BDK'ların unvanları Kurum internet sitesinde duyurulur.

BSD yapma yetkisinin kaldırılması

MADDE 12 – (1) Aşağıdaki hallerin bir veya birkaçının tespit edilmesi halinde Kurul, yetkili kuruluşun BSD yapma yetkisini iki yıla kadar geçici olarak kaldırmaya yetkilidir:

a) Denetçiler tarafından kullanılan unvanların 18 inci maddede belirtilen hükümlere uygun olmaması.

b) Denetçilerin, denetlenenler ile Kuruma önceden bilgi verilmeden değiştirilmesi.

c) Bu Yönetmelik kapsamında Kurum tarafından uyarıyı gerektiren hususların üç denetim dönemi içerisinde tekrar edilmesi.

ç) Yeterli denetim kanıtı elde edilememesine rağmen olumlu görüş verilmesi.

d) Kurumca istenilen bilgi ve belgelerin verilmemesi.

(2) Aşağıdaki hallerin bir veya birkaçının tespit edilmesi halinde Kurul, yetkili kuruluşun BSD yapma yetkisini sürekli olarak kaldırmaya yetkilidir:

a) Denetime olan güveni sarsacak veya denetimi geçersiz kılacak derecede bağımsızlık ve tarafsızlık kaybedilerek BDY'nin 22 nci maddesine uygun hareket edilmeksizin BSD faaliyetinin gerçekleştirilmesi.

b) Birden fazla olmak üzere Kanunun 36 ncı maddesi uyarınca ve BBDY'nin 19 uncu maddesi kapsamında belirlenen usul ve esaslar çerçevesinde yaptırılması zorunlu olan mesleki sorumluluk sigortasının BSD'yi de kapsayacak şekilde yaptırılmaması.

c) Olumlu, şartlı ya da olumsuz görüş verilen BSD'nin, denetlenenin varlıklarının korunmasını, faaliyetlerin etkin ve verimli bir şekilde ilgili mevzuata, denetlenenin politika ve kurallarına uygun olarak yürütülmesini, muhasebe ve finansal raporlama sisteminin güvenilirliğini, bütünlüğünü, tutarlılığını ve bilgilerin zamanında elde edilebilirliğini sağlamasını önemlilik arz eden ölçüde etkileyecek hususlara yetkili kuruluş tarafından BSD raporunda yer verilmemiş olduğunun Kurumca tespit edilmesi halinde, yetkili kuruluşun bu hususta kusurlu olmadığını kanıtlayamaması.

ç) Birinci fıkra kapsamında yetkinin bir defadan fazla geçici olarak kaldırılması.

d) Bu Yönetmelik kapsamında devam eden BSD'ye ilişkin bir sözleşme bulunmaması ya da BSD'de, denetim sözleşmesinde yer alan unsurların gerçekleştirilmemesi veya eksik gerçekleştirilmesi.

e) 21 inci maddenin onuncu fıkrasına aykırılık oluşması.

f) Yetkili kuruluşun 9 uncu maddede belirtilen şartları kaybetmesi.

g) BSD raporunun yanıltıcı ve gerçeğe aykırı şekilde düzenlenmesi.

ğ) Kesintisiz olarak 5 yıl süreyle fiilen BSD faaliyetinde bulunulmamış olması.

(3) Birinci veya ikinci fıkra kapsamında tespit edilen hususların denetçiden kaynaklandığının veya BSD çalışmalarında yer alan denetçilerin dürüstlük, tarafsızlık, mesleki yeterlilik ve özen, bağımsızlık, güvenilirlik, mesleki davranış ve sır saklama gibi etik ilkelere uymadığının tespit edilmesi halinde Kurum, sorumluluğun içeriğine göre denetçilerin 18 inci maddede tanımlanan denetçi unvanlarını kullanarak BSD faaliyetlerinde bulunmasını geçici veya sürekli olarak yasaklayabilir.

(4) Yetkinin geçici veya sürekli olarak kaldırılmasından önce ilgili yetkili kuruluş ve/veya denetçinin savunması alınır. Savunma istendiğine ilişkin yazının tebliğ tarihinden itibaren bir ay içinde savunma verilmemesi halinde savunma hakkından feragat edildiği kabul edilir.

(5) Bu Yönetmelik kapsamında yetkili kuruluşun denetim yapma yetkisinin kaldırılması, bağımsız denetim yapma yetkisinin kaldırılması anlamına gelmez. Yetkili kuruluşun bağımsız denetim yapma veya bankalarda bağımsız denetim yapma yetkisinin kaldırılması halinde, bu Yönetmelik kapsamındaki denetim yapma yetkisi hiçbir işleme gerek kalmaksızın kaldırılmış sayılır.

(6) BSD yapma yetkisi geçici olarak kaldırılan yetkili kuruluş söz konusu süre sonunda yasağın kaldırılması için Kuruma başvurur; başvuru yapılmadığı takdirde yasak uygulanmaya devam eder. Kuruma yapacakları başvurular, yetkili kuruluş hakkında devam etmekte olan bir inceleme olup olmadığı da dikkate alınarak Kurulca değerlendirilerek karara bağlanır.

(7) BSD yapma yetkisi geçici olarak kaldırılan denetçi, söz konusu süre sonunda yasağın kaldırılması için Kuruma başvurur; başvuru yapılmadığı takdirde yasak uygulanmaya devam eder. Kuruma yapacakları başvurular, denetçi hakkında devam etmekte olan bir inceleme olup olmadığı da dikkate alınarak Kurumca değerlendirilerek karara bağlanır.

(8) Bu Yönetmelik kapsamında BSD yapma yetkisi kaldırılan BDK'ların unvanları Kurum internet sitesinde duyurulur.

BSD'nin dış hizmet alımı ile gerçekleştirilmesi

MADDE 13 – (1) BBDY kapsamında bankalarda bağımsız denetim yapma yetkisini haiz BDK Kurumdan izin alarak BSD faaliyetini dış hizmet alımı yoluyla gerçekleştirebilir.

(2) BDK'nın, BSD'yi dış hizmet alımı yoluyla gerçekleştirmesi durumunda da, ilgili faaliyetler ve bu Yönetmelik kapsamındaki yükümlülüklerden kendisi ve BSDDHK adına nihai anlamda sorumludur.

(3) Aynı BSDDHK birden fazla BDK'ya hizmet verebilir.

(4) Bir BDK bir seferde en fazla üç dönem için dış hizmet alımı ile BSD yapma izni başvurusunda bulunabilir. İzin süresi dolduğunda ilgili BDK dış hizmet alımı ile BSD yapma izni için tekrar başvuruda bulunabilir.

(5) Kurum, BSDDHK'lardan denetlenenin tabi olduğu kanun ve bu Yönetmelik hükümleri ile ilgili göreceği bütün bilgileri gizli dahi olsa istemeye, tüm kayıt ve belgelerini incelemeye yetkili olup, BSDDHK'da istenilen bilgileri vermekle yükümlüdür.

BSDDHK'da aranan şartlar

MADDE 14 – (1) BDK'nın BSD faaliyetini gerçekleştirmek üzere hizmet alacağı BSDDHK'ların;

a) Denetçilerinin bu Yönetmelikte tanımlanan denetçi niteliklerini haiz olması,

b) Denetim ekipleri içerisinde yeterli sayıda ve nitelikte denetçi istihdam etmesi,

c) Denetçisinin, geçmişte görev aldığı BSD faaliyetlerinde, denetim ilkelerine bağlı ve denetçi bağımsızlığı ilkesini zedelememiş olması,

ç) BDY'nin 26 ncı maddesinin birinci fıkrasının (ç) bendinde belirtilen koşulları sağlaması,

şarttır.

(2) BSDDHK'nın BSD gerçekleştirebilmesi için bu Yönetmelik kapsamında, BDK ile sözleşme yapmış olması gereklidir. Bu sözleşme ile BDK BSDDHK'nın denetim ilkelerine bağlılığını; bu Yönetmelik ve ilgili diğer düzenlemeler kapsamındaki hususlara ilişkin hükümlere uymasını sağlamak zorundadır.

İzin başvurusu sırasında gerekli olan bilgi ve belgeler

MADDE 15 – (1) BSD faaliyetinde dış hizmet alımında bulunmak isteyen BDK, Kuruma vereceği başvuru dilekçesine;

a) BDK ve BSDDHK ile ortakları ve denetçilerine ilişkin 10 uncu maddenin birinci ve ikinci fıkraları kapsamında yer verilmesi gereken belgeleri,

b) BDK ile BSDDHK arasında yapılmış olan, tarafların sorumluluklarının, denetim planının açıkça belirtildiği, BSDDHK'nın BSD raporun imzalamakla yetkilendirdiği Bilgi Sistemleri Bağımsız Başdenetçisi, denetim ilkeleri, denetçi bağımsızlığı, gizlilik ve çıkar çatışması, denetim ekipleri ve saatlik denetim ücreti ile toplam hizmet bedeli gibi hususların açıklığa kavuşturulmuş olduğu sözleşmeleri,

c) BSDDHK'nın merkezinin varsa şube ve/veya şubelerinin adreslerini,

ç) BSDDHK'nın başvuru tarihindeki bilançosunu,

d) BSDDHK'nın yurt dışında yerleşik bir şirket ile dış hizmet alımına konu alana ilişkin hukuki bağlantısı olması durumunda, ilgili şirket ile yapılan sözleşmelerin şirket yetkililerince tasdik edilmiş kopyasını,

e) BSDDHK'nın denetçilerinin, denetim ilkelerine bağlı olmak, gizlilik ve denetçi bağımsızlığı ilkesini zedelememek koşuluyla BSD'de görev alacaklarına dair Ek-8'de yer alan örneğe uygun olarak düzenlenecek yazılı beyanları,

ekler.

Dış hizmet alımı ile bilgi sistemleri ve bankalarda iş süreçleri bağımsız denetimi yapma izninin verilmesi

MADDE 16 – (1) Dış hizmet alımı ile BSD yapma iznini almak üzere başvuruda bulunan BDK ile BSDDHK'nın bilgi ve belgeler çerçevesinde değerlendirilerek, mesleki ve teknik açıdan yeterliliklerinin tespitine yönelik olarak Kurum tarafından gerektiğinde yerinde incelemede bulunulması neticesinde, faaliyet konularını yürütebilecek yeterliliğe sahip oldukları kanaatine varılması halinde, Kurul kararıyla, uygun görülen dönemler için BSD yapma izni verilir.

(2) BDK'nın dış hizmet alacağı kuruluşun bu Yönetmelik kapsamında yetkili bir kuruluş olması durumunda dış hizmet alımı ile BSD yapması Kurum değerlendirmesine tabidir.

(3) Dış hizmet alımı ile BSD yapma izni alan BDK ve BSD çerçevesinde sunduğu hizmetle sınırlı olmak üzere ilgili BSDDHK bu Yönetmeli kapsamında, aksi belirtilmedikçe, yetkili kuruluşlarla ilgili bütün hükümlere tâbidir.

Dış hizmet alımı ile bilgi sistemleri ve bankalarda iş süreçleri bağımsız denetimi yapma izninin iptali

MADDE 17 – (1) Bu Yönetmelik hükümlerine aykırı hareket ettikleri tespit edilen dış hizmet alımı ile denetim yapma izni alan BDK'lar ve ilgili BSDDHK'larda 12 nci maddenin birinci ve ikinci fıkralarında yer verilen hususların bir veya birkaçının varlığının tespiti halinde, aykırılıkların mahiyetine bağlı olarak, Kurum tarafından yapılan değerlendirme üzerine Kurul, BDK'nın dış hizmet alımı ile BSD yapma iznini geçici veya sürekli olarak kaldırır.

(2) Kurumun birinci fıkra kapsamında dış hizmet alımı ile BSD yapma yetkisini geçici ya da sürekli kaldırması durumunda, BSDDHK'nın ilgil denetçilerinin yetki kaldırılmasına sebep olan hususlarda sorumluluğunun içeriğine göre 18 inci maddede tanımlanan denetçi unvanlarıyla BSD faaliyetlerinde bulunmasını Kurum geçici veya sürekli olarak yasaklayabilir.

(3) BDK ve BSDDHK arasındaki sözleşmenin feshedilmesi halinde yedi gün içinde Kuruma bilgi verilir.

Denetçi unvanları

MADDE 18 –(1) Bu Yönetmelik kapsamında denetçiler kıdem sırasına göre Bilgi Sistemleri Bağımsız Başdenetçisi, Bilgi Sistemleri Bağımsız Kıdemli Denetçisi, Bilgi Sistemleri Bağımsız Denetçisi unvanlarını alırlar. Bu unvanlar haricindeki oluşturulacak unvanlar ve bu unvanların taşıması gereken şartları BDK takdirindedir.

(2) Bilgi sistemleri denetimi, bilgi sistemleri kontrolü veya güvenliği, yazılım geliştirme ve bilgi teknolojileriyle ilgili konularda fiilen geçirilen çalışma sürelerinin toplamı bu Yönetmelik kapsamında mesleki tecrübe olarak kabul edilir.

(3) Bilgi Sistemleri Bağımsız Denetçisinin aşağıdaki şartları taşıması zorunludur:

a) Üniversitelerin veya denkliği yetkili makamlarca kabul edilen yurt dışındaki yükseköğretim kurumlarının 4 yıllık lisans programlarını tamamlamış olmak.

b) En az 1 yılı fiilen bilgi sistemleri denetimi tecrübesi olmak üzere 3 yıl mesleki tecrübeye sahip olmak.

(4) Bilgi Sistemleri Bağımsız Kıdemli Denetçisinin aşağıdaki şartları taşıması zorunludur:

a) Bilgi Sistemleri Bağımsız Denetçisi unvanını haiz olabilmek için aranan şartlara sahip olmak.

b) En az 2 yılı fiilen bilgi sistemleri denetimi tecrübesi olmak üzere 6 yıl mesleki tecrübeye sahip olmak.

(5) Bilgi Sistemleri Bağımsız Başdenetçisinin aşağıdaki şartları taşıması zorunludur:

a) Bilgi Sistemleri Bağımsız Denetçisi unvanına sahip olabilmek için aranan şartları haiz olmak.

b) En az 3 yılı fiilen bilgi sistemleri denetimi tecrübesi olmak üzere 10 yıl mesleki tecrübeye sahip olmak.

(6) Beşinci fıkradaki şartları taşıyan denetçiler Kurumca yapılan değerlendirmeler sonucunda uygun görülmesi halinde Bilgi Sistemleri Bağımsız Başdenetçisi unvanına sahip olurlar ve sicile kaydedilirler. Kurum, Bilgi Sistemleri Bağımsız Başdenetçisi unvanını denetimin yapılacağı kuruluşa göre şartlı verebilir.

(7) Bilgi Sistemleri Bağımsız Başdenetçisi unvanı haricindeki diğer denetçi unvanlarına yapılan terfiler yetkili kuruluşlar tarafından yapılır, Kurumca belirlenen usul ve esaslara uygun olarak Kuruma bildirilir. Bilgi, yetenek ve liyakatleri bir üst kıdemin gerektirdiği nitelikte olmayanlar tecrübe şartını sağlasalar dahi bir üst unvana terfi ettirilemezler.

(8) Bu Yönetmelik kapsamındaki yetkili kuruluşların BSD'yle görevlendirilmiş denetçilerinin tümünün, yılda en az yirmi saat, üç yılda en az yüz

yirmi saat BSD kapsamında sürekli eğitim almaları veya vermeleri zorunludur.

(9) Kurumun BSD yapmakla görevli daire başkanlığında bu madde kapsamında belirtilen sürelerde görev yapmış meslek personeli ilgili unvanı haiz kabul edilir. Bu kapsamda 10 yıllık mesleki tecrübeye sahip meslek personeli de Bilgi Sistemleri Bağımsız Başdenetçisi unvanını alır ve sicile kaydedilir.

DÖRDÜNCÜ BÖLÜM
Tarafların Yükümlülükleri

Denetlenenin yükümlülükleri

MADDE 19 –(1) Denetlenen, bilgi sistemleri dokümantasyonunu, iş süreçlerine ait dokümantasyonu ve bu dokümantasyonla ilgili her türlü kayıt, bilgi, belge, yapı ve sistemlerini BSD'ye uygun ve hazır hale getirmek zorundadır.

(2) Denetlenen, denetçinin BSD'ye yönelik talep ettiği gizli dahi olsa her türlü bilgi ve belgeyi vermekle yükümlüdür.

(3) Denetlenen, denetçilere faaliyetlerinde kullandıkları tüm sistem ve uygulamaları kullanım amaçlarını kapsayan uygulama listesiyle birlikte bildirmek; kontrol mekanizmalarına ilişkin dokümantasyonu ve uygulamalarına ilişkin kullanıcı dokümanlarını, bankalar ayrıca 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete'de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin 9 uncu maddesi uyarınca hazırladığı iş akım şemalarını da sunmakla yükümlüdür.

(4) Denetlenen, denetçi tarafından BSD kapsamında talep edilen iç denetim ve iç kontrol raporlarının bir örneğini denetçiye iletir ve 35 inci madde kapsamında denetçi ile personeli arasındaki iş birliğinin sağlanması için gerekli tedbirleri alır, yetkili kuruluşun denetçileri tarafından yöneltilen soruların zamanında yanıtlanmasını ve ilgili konulara açıklık getirilmesini sağlar.

(5) Denetçilerce yapılacak tespitler hakkında denetlenenin yönetim kurulunun bilgilendirilmesi; bağımsız denetçiler ile yönetim kurulu üyeleri ve denetlenen personeli arasında koordinasyonun sağlanması bankalarda banka denetim komitesinin, Risk Merkezinde Risk Merkezi yönetiminin ve diğer denetlenenlerde ise yönetim kurulunun sorumluluğundadır.

(6) Denetlenen tarafından sözleşme süresi içinde anlaşmalı olunan yetkili kuruluşun değiştirilmesi istendiği ya da yetkili kuruluş tarafından BSD sözleşmesine aykırı hareket edildiği ve/veya BSD'nin bu Yönetmelikte belirtilen esaslara göre yapılmadığı hallerde, durumun gerekçesiyle birlikte Kuruma bildirilmesi ve BSD sözleşmesinin feshedilebilmesi için Kurumun uygun görüşünün alınması zorunludur.

(7) Denetlenen, BSD raporunda ortaya konulan bulguların çözümlerine ilişkin taahhütlerini bir aksiyon planı ile karara bağlar. Aksiyon planının yürütülmesinin ve bu planda yer alan taahhütlerin zamanında ve eksiksiz olarak yerine getirilmesinin sağlanmasından denetlenen yönetim kurulu sorumludur. Aksiyon planının hazırlanması ve raporlanmasına ilişkin usul ve esaslar Kurum tarafından belirlenir.

Yönetim Beyanı

MADDE 20 – (1) Banka, yönetim kurulu tarafından denetim dönemi itibarıyla düzenlenen Yönetim Beyanını denetçiye sunar. Yönetim Beyanı ile yönetim kurulu, 15/3/2020 tarihli ve 31069 sayılı Resmî Gazete'de yayımlanan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliğin 32 nci maddesi kapsamında yapılan çalışmalara ve bankacılık süreçlerine ilişkin iç kontrollerin etkinlik, yeterlilik ve uyumluluğuna ilişkin değerlendirmede bulunarak, mevcut durum ve yürütülen çalışmalara ilişkin güvence sunar.

(2) Yönetim Beyanına mesnet teşkil edecek çalışmalar, banka iç sistemler birimlerince bu Yönetmeliğin beşinci ve altıncı bölümleri çerçevesindeki usul ve esaslar dikkate alınarak gerçekleştirilir.

(3) Banka Yönetim Kurulu, Yönetim Beyanını, cari BSD dönemine ilişkin yürütülen çalışmalar ve değerlendirmeler neticesinde oluşturur. Bu bağlamda esas alınacak dönem 1 Ocak-31 Aralık dönemi olup, Banka Yönetim Kurulu bu dönemin sonu itibarıyla, BSD raporu tarihi ile uyumlu olarak beyanda bulunur.

(4) Yönetim Beyanında asgari olarak;

a) Banka Yönetim Kurulunun 5411 sayılı Kanunun 29 uncu ve 30 uncu maddeleri ve Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin 4 üncü maddesinin birinci fıkrasına istinaden etkin, yeterli ve uyumlu bir iç kontrol sistemi kurma ve işletme yükümlülüğünün bulunduğu,

b) İlgili banka birimlerince, iç kontrol sisteminin incelenmiş ve bu sistem hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılmış olduğu,

c) İç kontrol sistemi üzerinde -varsa- tespit edilen önemli kontrol eksiklikleri,

ç) İç kontrol sistemi üzerinde yapılan değerlendirmelerde -dönem sonu itibarıyla düzeltilmiş olsa dahi- tespit edilen iç kontrol sistemine ilişkin tüm kontrol zayıflıklarının, kayda değer ve önemli kontrol eksikliklerinin sınıflandırılarak denetçiye sunulduğu,

d) Finansal tablolarda önemli yanlış beyana sebep olan veya başta finansal veriler olmak üzere banka açısından hassasiyet arz eden verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve faaliyetlerin sürekliliğini önemli ölçüde etkileyen ya da önemli seviyede olmasa da yöneticilerin veya iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu tüm suistimal veya yolsuzluklar,

e) İç kontrol sisteminde gerçekleştirilen incelemeleri takiben, önemli ve kayda değer kontrol eksiklikleri konularında banka tarafından alınmış olan düzeltici önlemleri de içerecek şekilde, iç kontrol sisteminde veya iç kontrol sistemini önemli derecede etkileyebilecek diğer hususlarda meydana gelmiş olan değişiklikler,

beyan edilir.

(5) Yönetim Beyanı kapsamında;

a) Bankacılık süreçleri iç denetimlerinin kritik banka servisleri, süreçleri ve kritik varlıkları içerecek ve bunlara ilişkin güvence verecek derinlikte ve detayda olması,

b) Bankacılık süreçleri iç denetimlerinin sıklığı ve denetim döngülerinin; banka servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olması,

c) 25 inci maddede yer alan süreçlere ilişkin kontrollere güvence vermek üzere yapılacak bankacılık süreçleri iç denetimleri için denetim döngüsünün her yıl olması,

ç) Yapılan denetimlere ilişkin çalışma kanıtlarının en az üç yıl banka nezdinde saklanması,

esastır.

(6) Yönetim Beyanı, denetim dönemini takip eden Ocak ayı sonuna kadar bağımsız denetim kuruluşuna iletilir.

(7) BDK, Yönetim Beyanını ve bu beyana mesnet teşkil eden çalışmaların yeterliliğini inceler. Denetçi beyanda, içerik açısından eksiklik veya bağımsız denetim çalışması sonuçları itibarıyla varsa uyumsuzlukları tespit eder. BDK Yönetim Beyanına ilişkin değerlendirme ve tespitlerine BSD'de ayrı bir bölüm halinde yer verir.

Yetkili kuruluşların ve denetçilerin yükümlülükleri

MADDE 21 –(1) Denetçiler bu Yönetmelik ile BDY'nin 21 inci maddesinin birinci fıkrasında belirlenen ilkelere uymak, bilgi sistemleri ve iş süreçleri içerisinde yer alabilecek riskleri ve zayıflıkları dikkate alarak ve mesleki şüphecilik çerçevesinde bir denetim planı hazırlamak, denetlenene sunmak ve uygulamak, yöneticilerin açıklamalarını yeterli denetim kanıtı olarak kabul etmemek ve BSD raporunu oluşturmak ile yükümlüdür.

(2) BDY'nin 20 nci maddesine göre BDK tarafından tesis edilmesi gerekli olan kalite kontrol sistemi bu Yönetmelik kapsamında yapılan BSD çalışmalarını ve BSD raporlarını da kapsayacak şekilde yürütülür.

(3) Denetçi, ortaya çıkan hata ve suistimaller hakkında denetlenenin yöneticilerine ve denetlenenin iç sistemlerden sorumlu yönetim kurulu