Bankacılık Düzenleme ve Denetleme Kurumundan:

FİNANSAL KİRALAMA, FAKTORİNG VE FİNANSMAN ŞİRKETLERİNİN BİLGİ SİSTEMLERİNİN YÖNETİMİNE VE DENETİMİNE İLİŞKİN TEBLİĞ

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

Amaç ve kapsam

MADDE 1 - (1) Bu Tebliğin amacı, Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Kanun kapsamındaki faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimine ve yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesine ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Tebliğ, 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanununun 14 üncü maddesinin ikinci fıkrası ve 24/04/2013 tarihli ve 28627 sayılı Resmî Gazete'de yayımlanan Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Kuruluş ve Faaliyet Esasları Hakkında Yönetmeliğin 14 üncü maddesi uyarınca düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Tebliğ'de yer alan,

a) Birincil sistemler: Kanunda yer alan hususlarla ilgili bütün bilgilerin, elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanıldığı sistemler ile faaliyetlerin yürütülmesinde kullanılan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamını,

b) BSDHY: 13/01/2010 tarihli ve 27461 sayılı Resmi Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliği,

c) Denetim izi: Bir operasyonel ya da finansal işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile ilgili bilgi sistemi varlığına kimin eriştiğini, erişmeye çalıştığını ve kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtları,

ç) Dış hizmet: Kuruluşların bilgi sistemlerine ilişkin dışarıdan temin ettikleri her türlü hizmet alımlarını,

d) İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği, herhangi bir kesinti durumunda personelin çalışmasına imkân tanıyacak ve birincil sistemlerin tesis edildiği yapı ile deprem, yangın vb. aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

e) İkincil sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin bilgi sistemleri süreklilik planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve Kanunda yer alan hususlarla ilgili bütün bilgilere erişilmesini sağlayan birincil sistem yedeklerini,

f) Kanun: 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Hakkında Kanunu,

g) Kontrol: BSDHY'nin 3 üncü maddesinde tanımlanan kontrolü,

ğ) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu

h) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

ı) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amaçlı gerçekleştirilen testleri,
i) Şirket: Kanunun 3 üncü maddesinde tanımlanan şirketi,
j) Uyumluluk: BSDHY'nin 7 nci maddesinde tanımlanan uyumluluğu,
k) Üst yönetim: Şirket yönetim kurulu ile genel müdür ve genel müdür yardımcıları ve başka unvanlarla istihdam edilseler dahi, danışmanlık birimleri dışındaki birimlerin, yetki ve görevleri itibarıyla genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticilerini

ifade eder.

İKİNCİ BÖLÜM

Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler

Bilgi sistemleri yönetimi

MADDE 4 – (1) Şirket, kurumsal yönetim ilkelerinin uygulandığı yönetim kurulu onaylı bir bilgi sistemleri yönetim yapısı tesis eder. Şirketin bilgi sistemlerine ilişkin stratejisinin iş hedefleri ile uyumlu olması sağlanır. Bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde uygun yere yerleştirilir ve bilgi sistemlerinin güvenliği ve gerektiği şekilde yönetimi için gerekli finansman ve insan kaynağı tahsis edilir.

(2) Şirket, bu amaçla bilgi sistemlerine ilişkin politika, prosedür ve süreçlerini tesis eder. Politika, prosedür ve süreçler düzenli olarak gözden geçirilerek, güncellenir ve yönetim kurulu tarafından onaylanır. Politika, prosedür ve süreçlerin fiili olarak işlemesi sağlanır. Bu kapsamda işleyişin sağlanması için süreç sahipleri ve sorumlulukları ile kontrol noktaları tanımlanır. Bilgi sistemlerinin kendisinden beklenen hizmetleri zamanında, doğru ve güvenilir şekilde sağlaması için gereken kontroller belirlenir ve bu kontrollerin etkinliği sağlanır.

(3) Bilgi sistemleri kullanılarak gerçekleştirilen işlemlerin kontrolü, izlenmesi ve inkar edilemezliğin sağlanması için gerekli süreç ve altyapılar tesis edilir, ilgili sorumlular belirlenir.

(4) Şirket iç kontrol birimi yılda bir kez, yönetim kuruluna sunulmak üzere, politika ve prosedürlere uyuma ilişkin hususları da içeren mevzuata uyum değerlendirmesi raporu hazırlar.

Bilgi sistemleri risk yönetimi

MADDE 5 - (1) Şirket, faaliyetlerinde bilgi teknolojilerinin kullanılmasından kaynaklanan riskleri tespit etmek, analiz etmek, ölçmek, izlemek ve raporlamak üzere üst yönetim tarafından onaylanmış bir risk yönetim süreci oluşturur. Şirket, riskleri takip ederek gözden geçirir ve günceller. Süreç asgari olarak aşağıdaki hususları içerir:

a) Şirket, bu Tebliğin 10 uncu maddesinin birinci fıkrası uyarınca bilgi varlıkları envanterini çıkarır. Envantere, yazılım ve donanımın yanı sıra elde bulunan ve saklanan veriyi de dahil eder. Şirket envanterdeki varlıklara yönelik tehditleri, riskin ortaya çıkma ihtimalini, riskin gerçekleşmesi durumunda ortaya çıkacak olası sonuçları ve alınabilecek önlemlere ilişkin olarak bir değerlendirmede bulunulur.
b) Şirket yapacağı risk analizinde, belirlediği her riske ilişkin; riski azaltma, riskten kaçınma, riski kabul etme veya riski transfer etme yöntemlerinden birini seçer.

(2) Şirket risk analizi yaparken, hizmetlerini sunmak için kullandığı teknoloji altyapısı, uygulama mimarisi, programlama teknikleri, dış hizmet sağlayıcılardan kaynaklanabilecek riskleri ve teknolojik gelişmeleri de dikkate alır. Yapılacak risk analizinde kullanıcı bilgilerinin güvenliğini ve gizliliğini tehdit eden riskler dikkate alınır.

(3) Şirket, bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce olası riskleri değerlendirir, veri kaybını, hizmetlerde aksamayı önlemeye ve ilave risk oluşturmamaya yönelik tedbirleri alır.

(4) Şirket, yılda bir kez risk üst yönetime sunulmak üzere bilgi sistemlerine ilişkin öngörülen risk ve tehditleri içeren risk değerlendirme raporu hazırlar.

Bilgi güvenliği yönetimi

MADDE 6 - (1) Şirket, bilgi güvenliğine ilişkin süreci tesis eder. Bilgi güvenliğine ilişkin süreci, rolleri ve sorumlulukları dokümante eder

(2) Şirket, bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemleri tesis eder.

(3) Şirket, bilgi sistemleri üzerinde edinilen, saklanan, iletilen, işlenen verileri güvenlik hassasiyet derecelerine göre sınıflandırır ve her sınıf için uygun düzeyde güvenlik kontrolü tesis eder.

(4) Şirket, kendi kurumsal ağı dışındaki ağlarla iletişimde bulunduğu hallerde bu dış ağlardan gelebilecek tehditler için ağ kontrol güvenlik sistemlerini tesis eder. Şirket dış ağdan iç ağına yapılacak erişimleri kontrol altında tutmak, ayrıca, iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçiş temin etmek üzere gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan bir veya birden fazla güvenlik duvarı kullanır.

(5) Şirket, dışarıdan gelecek bir siber saldırıya karşı gerekli önlemleri alır ve veri gizliliğine ilişkin 2 yılda bir sızma testi yaptırır.

(6) Şirket, asgari olarak aşağıdaki faaliyetleri yerine getirir:

a) Bilgi güvenliği sürecinin işlevselliğini değerlendirir ve sorumlulukları belirli periyotlarla gözden geçirir ve günceller.
b) Bilgi kaynaklarına yönelik tehditleri periyodik olarak değerlendirir.
c) Bilgi güvenliği hususunda personelin farkındalığını arttıracak bilgilendirme veya çalışmalar yapar.

(7) Şirket, yılda bir kez üst yönetime sunulmak üzere; bilgi güvenliği sürecine uyum durumunu, bilgi güvenliği ihlaline ilişkin olaylarını içeren güvenlik ihlalleri raporu hazırlar.

Yetkilendirme ve erişim kontrolü

MADDE 7 – (1) Şirket, veritabanlarına, uygulamalara ve sistemlere erişim için uygun bir yetkilendirme ve erişim kontrolü tesis eder. Amaç, görev ve sorumluluklar göz önünde bulundurularak, gerekli olan en kısıtlı yetki ve erişim hakkı verilir. Yetkiler ve erişim hakları en az yetki prensibini açısından asgari yılda bir kez gözden geçirilir. Sistem, servis ve veriye sadece gerekli yetkiye sahip kullanıcı, taraf ve sistemlerin erişimi mümkün kılınır.

(2) Yetkilendirme veritabanlarının güvenliği sağlanır, yetkisiz erişim teşebbüsleri kayıt altına alınır ve gözden geçirilir.

(3) Şirket, sunmakta olduğu hizmetlerin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesi aşamalarında, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir.

(4) Şirket, yetkilendirme kapsamındaki faaliyetlerini dış hizmet kuruluşlarına devredemez.

(5) Geçici yetkilendirmeler için yetkilendirmenin yapılacağı şartlar ve geçerli olacağı süre belirlenir. Geçici yetkilendirmeye ilişkin iz kaydı tutulur.

(6) Şirket veya dış hizmet sağlayıcı bünyesinde görev yapan çalışanların görevlerinin sonlanması durumunda ilgili tüm yetkilendirmeler ivedilikle iptal edilir.

Kimlik doğrulama

MADDE 8 - (1) Bilgi sistemleri üzerinde gerçekleşen işlemler için işlemlerin türü, niteliği, bir ihlal halinde oluşabilecek kayıplar, işlem çeşidi ve verinin hassasiyet derecesi dikkate alınarak uygun bir kimlik doğrulama mekanizması kurulur. Aynı hesabın birden fazla kullanıcı tarafından kullanılması engellenir.
(2) Kimlik doğrulamada kullanılacak parolaların karmaşıklığının ve uzunluğunun günün teknolojisine ve işlemin niteliğine uygun olması sağlanır.
(3) Şirket, kimlik doğrulamada inkar edilemezliği sağlar. Tüm kullanıcılara ait kimlik doğrulama bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri alır. Parola gibi kritik öneme sahip veriler günün teknolojisine uygun şekilde şifreli olarak saklanır.

(4) Donanım ve yazılımlara ait kurulumda tanımlanmış varsayılan şifreler değiştirilir. Yeni şifreler güvenli bir şekilde saklanır.

(5) Başarısız kimlik doğrulama teşebbüsleri sırasında, kullanıcıya, kaç kez hatalı giriş yapıldığına ilişkin bilgi verilir, başarısız teşebbüslerin belirli bir sayıyı aşması halinde erişim engellenir ve işlemin kullanıcı adından veya paroladaki bir hatadan kaynaklandığı şeklinde gereksiz bilgi verilmez.

(6) Kimlik doğrulamada, önceden izin verilen durumlar hariç olmak üzere, aynı kullanıcıya ait birden fazla oturum açılması engellenir ve kullanıcıya birden fazla oturum açtığı uyarı verilir. Belli bir süre işlem yapılmayan oturumun sonlandırması sağlanır.

(7) Dış hizmet personelinin şirket sistemlerine uzaktan erişimi esnasında yapılacak kimlik doğrulama en az şirket personeli ile aynı seviyede güvenlik sağlanarak yapılır.

Denetim izlerinin oluşturulması

MADDE 9 - (1) Şirketin faaliyetlerine ilişkin etkin bir denetim izi mekanizması tesis edilir. Şirket faaliyetlerine ve müşterilere ilişkin bilgilere erişilmesi, sorgulanması, bunlara yönelik erişim yetkilerinin verilmesi veya değiştirilmesine yönelik tüm işlemler ve bunlara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları tutulur.

(2) Şirketin, web servisleri, API ya da benzeri metotlarla diğer kurum/kuruluşlar nezdinde tutulan hassas veriler ile kişisel verilere ilişkin yaptıkları sorgulamalar ve bu sorgulamaları hangi amaçla yaptıklarına ilişkin iz kayıtları da denetim izi kapsamındadır. Şirket, sorguladığı verinin amacı dışında kullanımının önüne geçmek için gerekli tedbirleri alır.

(3) Denetim izlerinin yeterli detayda, açıklıkta, bütünlüğünün bozulmasına, değiştirilmesine müsaade edilemeyecek şekilde ve raporlanabilir bir formatta tutulması esastır. Denetim izleri, işleme ilişkin olarak; tarih, zaman, uygulama bilgisi, kullanıcı adı, hangi bilginin sorgulandığı, değiştirildiği vb. bilgileri içerir.

(3) Denetim izi kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır. Denetim izlerinin bulunduğu sistemlerde yönetici hesapları dahil hiçbir kullanıcının kayıtlar üzerinde değişiklik yapabilmesine izin verilmez.

(4) Sistem ve veritabanlarında, yüksek yetkili veya yönetici hesapları ile yapılan erişimler kontrol altına alınır, iz kayıtları tutulur ve işlemi yapanların kendi faaliyetlerine ilişkin denetim izlerine müdahalesi engellenir.

(5) Denetim izleri asgari 5 yıl süreyle denetime hazır bulundurulur ve yedek alınması suretiyle, yaşanacak olası felaketler sonrasında da erişilebilir olmaları temin edilir.

(6) Şirket, dış hizmet sağlayıcıdan aldığı hizmet kapsamında; dış hizmet sağlayıcı tarafından tutulan denetim izlerinin kendi standartlarına uygunluğunu ve denetim izlerinin kendisi tarafından erişilebilir olmasını temin eder.

(7) Denetim izlerinin tutulması, şirketin belge ve kayıtların saklanmasına ilişkin ilgili düzenlemelerde yer alan diğer yükümlülüklerini ortadan kaldırmaz.

Bilgi varlıklarının yönetimi

MADDE 10 - (1) Şirket bilgi varlıkları envanterini aşağıdaki çerçevede oluşturur:

a) Donanım envanteri: Donanım envanteri, kurumsal ağa bağlı olan ve olmayan, üzerinde şirkete ait bilgi bulunan tüm donanım, sunucu ve ortamları içerir. Kurumsal kaynaklara erişmek ve işlem yapmak için personelin kullandığı kişisel cihazları da envantere dahil edilir. Envanterde, donanımın türü, markası, modeli, alım tarihi, envantere giriş ve çıkış tarihi, fiziksel lokasyonu, üzerinde bulunan uygulamalar ile konfigürasyon veya diğer değişiklikleri yapmaya yetkililer, sahiplik bilgisi, yedeğinin olup olmadığı, kritiklik düzeyi ve benzeri bilgiler yer alır.
b) Yazılım envanteri: Kurumsal olarak kullanılan ve şirket donanımları üzerinde bulunan, hizmet verip vermediğine bakılmaksızın tüm yazılımları içerir. Bu yazılımlar haricinde, şirket tarafından uzaktan kullanılan yazılım hizmetleri ve kurumsal kaynaklara erişmek için kullanılan kişisel cihazlardaki ilgili uygulamalar da envantere dahil edilir. Envanterde, versiyon, eriştiği veri, üzerinde çalıştığı donanım, geliştirme ortamı, kritiklik vb. bilgiler yer alır.
c) Veri envanteri: Şirketin bilgi sistemleri üzerinde bulunan tüm verilerini içerir. Verinin kritikliği, bulunduğu veritabanı, yedeğinin alınıp alınmadığı, yedeğin mantıksal adresi, veriyi kullanan uygulamalar, kimin erişebildiği vb. bilgiler belirtilir.

(2) Bilgi varlıkları envanteri güncel olarak takip edilir, son 3 yıla ait envanter kayıtları saklanır. Envanterden çıkarılan donanımların Şirkete ait bilgi taşımaması için gerekli tedbirler alınır.

(3) Şirket bilgi sistemleri üzerinde yer alan yazılımların güncelliğini sağlar. Kullanılan yazılımların önceki versiyonları ve çalışmaya hazır kopyaları güvenli şekilde saklanır. Bunun için yama yönetimi ile ilgili süreç tesis edilerek güncel yamalar takip edilir.

(4) Üretim ortamında kullanılan yazılımların bütünlüğü güvence altına alınır ve üretim ortamındaki değişiklikler ilgili yönetici onayı alınarak gerçekleştirilir. Bu amaçla, üretim ortamına erişim kısıtlanır, ihtiyaç halinde geçici süreyle verilen yetkiler kayıt altına alınır. Yazılım değişiklikleri sistemsel olarak izlenebilir hale getirilir, manuel müdahale en aza indirilir.

(5) Şirket, bilgi sistemlerinin fiziksel güvenliği amacıyla için;

a) Bilgi sistemlerinin bulunduğu alanın güvenliğini sağlar, alanın içeriden ve dışarıdan gelebilecek tehditlerden korunması için gerekli tedbirleri alır.
b) Sistem odasına giriş ve çıkışları kartlı veya kilitli şekilde kontrol altına alır, giriş ve çıkışa ilişkin bilgiler yazılı kayıt altında tutulur.
c) Birincil, ikincil sistem odaları ve girişleri kamera ile izlenir hale getirilir. İlgili kayıtlar 3 ay saklanır.

Bilgi sistemleri süreklilik planı

MADDE 11 - (1) Şirket, faaliyetlerini ve önemli iş fonksiyonlarını destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere üst yönetim tarafından onaylanmış bir bilgi sistemleri süreklilik planı hazırlar.

(2) Planın hazırlanması sürecinde, bilgi sistemleri varlıklarının önem düzeyi değerlendirilerek her bir servis için kabul edilebilir kesinti süreleri belirlenir ve bu süreler içinde servislerin tekrar erişime açılabilmesini sağlayacak kurtarma prosedürleri geliştirilir.

(3) Planda ilgili sistem, altyapı, iletişim vb. bilgi sistemleri bileşenleri sorumluları ve iş sorumluları belirtilir. Uygulanması gereken kurtarma ve geri döndürme adımları, bu adımların hangi koşullarda uygulanacağı tanımlanır.

(4) Plan, şirketin bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra her yıl gözden geçirilerek güncellenir ve üst yönetim tarafından onaylanır.

(5) Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedekleri ikincil merkezde kullanıma hazır bulundurulur.

(6) Planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa ikincil merkez üzerinden testler yapılır, testlere varsa dış hizmet sağlayıcılar da dahil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre planın güncellenmesi sağlanır.

Dış hizmet alımı ve yönetimi

MADDE 12 – (1) Bilgi sistemlerinin dış hizmete konu edilebilmesi ancak Kanun ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görev ve sorumlulukların yerine getirilmesi sırasında yönetim, içerik tasarımı, erişim, kontrol, denetim, güncelleme, bilgi/rapor alma gibi fonksiyonlarda karar alma gücü ve sorumluluğunun Şirkette olması ile mümkündür.

(2) Şirket üst yönetimi, bilgi sistemleri kapsamında dış hizmet alımına ilişkin olarak, söz konusu hizmetin dış hizmet alımı yoluyla gerçekleştirilmesinin şirket açısından doğuracağı riskleri değerlendirir. Bu kapsamda, Şirket üst yönetimi, dış hizmet alımı yoluyla gerçekleştirilen servisler için servisin içeriğine uygun olarak; hizmet seviyesini, kalitesini ve güvenlik kontrollerini, firmanın mali yapısını da değerlendirerek hizmet alımını gerçekleştirir. Firmanın hizmet verememe ihtimaline karşı alternatif tedarikçileri belirler.

(3) Dış hizmet alımına ilişkin sözleşme, asgari olarak aşağıdaki hususları içerir:

a) Dış hizmet alımı kapsamındaki tüm sistem ve süreçlerin şirketin kendi risk yönetimi, güvenlik ve gizlilik politikalarına uygun olmasını sağlayacak hükümler.
b) Sözleşmeye konu ürün ve hizmetlerin sahipliği ve fikri mülkiyet haklarına ilişkin hükümler.
c) Dış hizmet sağlayıcılar için yükümlülük teşkil eden hükümlerin alt yükleniciler ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler.
ç) Dış hizmet alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler.
d) Şirketin tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde dış hizmet sağlayıcı kuruluşlar için de uygulanmasını sağlayacak hükümler.
e) Dış hizmet alımı kapsamındaki faaliyetlerin şirket bünyesinde gerçekleştirilmesi durumunda, bağımsız denetim açısından hangi denetimlere tabi tutulması öngörülüyorsa, kapsam daraltılmasına gidilmeden aynı denetimlere tabi tutulmasını sağlayacak hükümler.
f) Dış hizmet sağlayıcıların, gerçekleştirdiği faaliyetlere ilişkin olarak Kurumca talep edilen her tür bilgi ve belgeyi zamanında ve doğru olarak vermekle ve bunlara ilişkin her türlü

elektronik, manyetik ve benzeri ortamlardaki kayıtları ve bu kayıtlara erişim ve kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifreleri incelemeye hazır bulundurmak ve işletmekle yükümlü olduğuna ilişkin hükümler.

g) Kurul veya Kurum talimatı ile şirketin bilgi sistemleri üzerinde gerçekleştirilmesi gereken değişikliklerin, alınan hizmet kapsamında dış hizmet sağlayıcı tarafından talimat süresi içerisinde yerine getirilmesini sağlayacak hükümler.

(4) Şirket, dış hizmet sağlayıcıların erişimleri için gerekli kontrolleri tesis eder. Veri ve sistem güvenliği açısından sağlanan erişimler, verilen erişim hakları ve tesis edilen kontroller düzenli olarak gözden geçirilir.

(5) Şirket dış hizmet olarak bulut bilişim hizmetlerini kullanabilir. Bulut hizmeti, tek bir şirkete tahsis edilmiş donanım ve yazılım kaynakları üzerinden özel bulut hizmet modeliyle alınabilir. Bunun yanında, sadece kanuna tabi şirketlere tahsis edilmiş donanım ve yazılım üzerinde, şirketler arasında mantıksal ayrıma gidilerek topluluk bulutu hizmet modeliyle dış hizmet alınması Kurum iznine tabidir.

(6) Şirket, dış hizmet alımlarında şirketin kendisine ve kullanıcılarına ait gizli bilgilerin güvenliğinin sağlanması için gerekli tedbirleri almakla yükümlüdür. Dış hizmet sağlayıcılara verilecek sisteme erişim, veriye erişim veya veriyi görme yetkisi işin gerektirdiği bilgiyi kapsayacak şekilde sınırlandırılır. Dış hizmet sağlayıcı tarafından şirkete ve kullanıcılarına ait gizli bilgilerin korunmasına yönelik tedbirlerin alınmasını sağlamak şirketin sorumluluğundadır.

(7) Şirket, veriyi kendi bünyesinde ya da bir hizmet sağlayıcıda yedekleyebilir. Yedekleme hizmetinin güvenlik ve iş sürekliliğine ilişkin gereksinimleri, bu hizmetin şirket tarafından verilmesi ile aynı şartları sağlar.

İşlem bilgilerinin gizliliği

MADDE 13 - (1) Şirket faaliyetlerinin yürütülmesi sırasında edindiği işlediği, ilettiği veya sakladığı işlem ve müşteri bilgilerinin gizliliğini ve güvenliğini sağlamaya yönelik politika, prosedürleri oluşturur ve gerekli tedbirleri alır.

(2) Şirket, mevzuatla yetkili kılınmış taraflar haricinde, kullanıcı bilgilerini kişinin açık rızası olmadan, toplandığı amaçlar dışında kullanamaz veya kullanılması için başkasına aktaramaz.

(3) Şirket tarafından sunulacak bir hizmet, kişiye ait verilerin paylaşılması amacıyla açık rıza vermesi şartına bağlanamaz.

ÜÇÜNCÜ BÖLÜM

Sınırlamalar ve Bilgi Sistemlerinin Bağımsız Denetimi

İnternet hizmetleri ve bilgi sistemlerine ilişkin sınırlamalar

MADDE 14 - (1) Şirketlerin sundukları internet hizmetleri kapsamında;

a) Müşterinin işlem gerçekleştirdiği platformun şirkete ait olduğunu garanti eden,
b) İşlemin taşıdığı risklerle uyumlu olarak gerekli kimlik doğrulama mekanizmasını sağlayan,
c) Kullanıcıların güvenlik risklerine ilişkin bilgilendirmesine yönelik

altyapı tesis edilir.

(2) Şirketlerin birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur. Bu kapsamda dış hizmet alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların tüm yedekleri de yurt içinde tutulur.

Bilgi sistemlerinin bağımsız denetimi

MADDE 15 - (1) Bilgi sistemleri denetimi; şirketin bu Tebliğ hükümlerine uyum durumunun tespit edilmesi amacıyla, bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım, donanım gibi bilgi sistemi unsurları ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin bağımsız denetim kuruluşları tarafından değerlendirilmesi sonucunda, söz konusu iç kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş oluşturulması ve sonuçların rapora bağlanması aşamalarından oluşan süreçtir.

(2) Şirketin bilgi sistemleri denetimi ve denetim sonuçlarının Kuruma raporlanması birinci fıkradaki tanımla sınırlı olmak üzere, Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumu tarafından belirlenen standartlara uygun olarak BSDHY ile belirlenen usul ve esaslar çerçevesinde, bağımsız denetçi tarafından gerçekleştirilir. Bu fıkranın uygulanmasında, BSDHY'nin 27 nci maddesinin ikinci fıkrasındaki koşul aranmaz.

(3) BSDHY ile belirlenen usul ve esaslar bu Tebliğ çerçevesinde uygulanırken BSDHY'de geçen "banka" ve "denetlenen" ibareleri şirketi, "bilgi sistemleri denetimi" ibaresi bu maddenin birinci fıkrasında tanımlanan denetimi ifade eder.

(4) Bağımsız denetçi, şirketin dış hizmet alarak gerçekleştirdiği hizmetlerin, bilgi sistemlerini nasıl etkilediğini göz önünde bulundurur, buna göre gerekli görmesi halinde denetimini dış hizmet sağlayıcıları da kapsayacak şekilde planlar ve etkin bir denetim yaklaşımı geliştirir.

(5) Şirkette bilgi sistemleri denetimi üç yılda bir yapılır. Hangi şirketlerde hangi yıl denetime başlanacağını belirlemeye Kurum yetkilidir. Kurum, gerekli gördüğü hallerde bilgi sistemleri denetiminin kapsamını ve sıklığını farklılaştırabilir.

(6) Denetim görüşünün oluşturulması ve denetim mektubu; şirkette gerçekleştirilen denetim sonucunda BSDHY'nin 5 inci ve 7 nci maddelerinde belirtilen hükümler ile 34 üncü maddesinde belirtilen görüş çeşitleri çerçevesinde; olumlu, şartlı veya olumsuz görüşe varılması hallerinde, sırasıyla ek-1, ek-2, ek-3'te yer alan örneklere uygun olarak denetim mektubu düzenlenir. Görüş bildirmekten kaçınmayı gerektirecek şartların varlığı halinde ise, denetim mektubu ek-4'te yer alan örneğe uygun olarak düzenlenir.

DÖRDÜNCÜ BÖLÜM

Son Hükümler

Geçiş Süreci

GEÇİCİ MADDE 1 – (1) Şirket, bu Tebliğ hükümleri ile ilgili mevcut faaliyet ve sistemlerini, yürürlük tarihinden itibaren azami bir yıl içerisinde Tebliğ hükümlerine uygun hale getirir.

Yürürlük

MADDE 16 – (1) Bu Tebliğ 1/1/2019 tarihinde yürürlüğe girer.

Yürütme

MADDE 17 – (1) Bu Tebliğ hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.

EK-1

BİLGİ SİSTEMLERİ DENETİMİ RAPORU

Olumlu Görüş

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı

EK-2

BİLGİ SİSTEMLERİ DENETİMİ RAPORU

Şartlı Görüş

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Bağımsız denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleri üzerinde tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemlerinin bütününü veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, yukarıda *(....ncı paragrafta)* açıklanan *husus(lar) nedeniyle,* denetlenenin bilgi sistemleri üzerinde bu *hususun/hususların* muhtemel etkileri haricinde bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı

EK-3

BİLGİ SİSTEMLERİ DENETİMİ RAPORU

Olumsuz Görüş

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri üzerindeki kontrollerin etkin, yeterli veya uyumlu bulunmama sebepleri)

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, bütün önemli taraflarıyla, ... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı

EK-4

BİLGİ SİSTEMLERİ DENETİMİ RAPORU

Görüşten Kaçınma

..... A.Ş. Yönetim Kuruluna:

..... A.Ş.'nin ...../...../..... tarihi itibarıyla Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ kapsamında bilgi sistemlerini denetlemekle görevlendirilmiş bulunuyoruz.

[Kuruluş Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri üzerindeki kontrollerin denetlenen nezdinde Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması ……. A.Ş. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve Finansal Kiralama, Faktoring ve Finansman Şirketlerinin Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğde belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri ve bu sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir. Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetçinin görüş bildirmemesinin nedenleri)

[Bağımsız Denetçi Görüşü]

Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle ..... A.Ş.'nin ...../...../..... tarihi itibarıyla bilgi sistemleri üzerinde tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Raporun Düzenleme
Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Baş Denetçisinin
Adı ve Soyadı, İmzası
Kuruluşun Ticari Unvanı