Bankacılık Düzenleme ve Denetleme Kurumundan:
Görüşlerinizi bsmevzuat@bddk.org.tr adresine e-posta ile iletebilirsiniz.

BANKALARIN BİLGİ SİSTEMLERİ VE ELEKTRONİK BANKACILIK HİZMETLERİ HAKKINDA YÖNETMELİK TASLAĞI

BİRİNCİ KISIM
Başlangıç Hükümleri

Amaç ve kapsam

MADDE 1 – (1) Bu Yönetmeliğin amacı, bankaların faaliyetlerinin ifasında kullandıkları bilgi sistemlerinin yönetimi ile elektronik bankacılık hizmetlerinin sunulmasında ve bunlara ilişkin risklerin yönetiminde esas alınacak asgari usul ve esaslar ile tesis edilmesi gereken bilgi sistemleri kontrollerini düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Yönetmelik, 19/10/2005 tarihli ve 5411 sayılı Bankacılık Kanununun 93 üncü maddesi ve 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete'de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliğin 11 inci maddesinin beşinci fıkrası ile 16 ncı maddesinin üçüncü fıkrası uyarınca düzenlenmiştir.

Tanımlar ve kısaltmalar

MADDE 3 – (1) Bu Yönetmelikte yer alan;

a) Acil ve beklenmedik durum müdahale planı: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan acil ve beklenmedik durum planını,

b) Açık bankacılık servisleri: Müşterilerin ya da müşteriler adına hareket eden tarafların API, web servis, FTP gibi yöntemlerle bankanın sunduğu bir takım finansal servislere uzaktan erişerek bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri elektronik dağıtım kanalını,

c) Açık rıza: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununda tanımlanan açık rızayı,

ç) Akıllı kart: Üzerinde, bilginin kaydedilebildiği ve işlenebildiği çip barındıran kartı,

d) API: Bir yazılımın başka bir yazılımda tanımlanmış işlevlerini kullanabilmesi için oluşturulmuş uygulama programlama arayüzünü,

e) ATM: Otomatik para çekme işleminin yanı sıra diğer bankacılık işlemlerinin tamamının veya bir bölümünün gerçekleştirilmesine imkân veren elektronik işlem cihazlarını,

f) Banka: Kanunun 3 üncü maddesinde tanımlanan bankaları,

g) Bilgi sistemleri: Bilginin toplanması, işlenmesi, saklanması, dağıtımı ve kullanımına yönelik insan kaynağı, operasyonel faaliyetler ve süreçler ile bunlarla etkileşim içinde bulunan bilgi teknolojilerini,

ğ) Bilgi sistemleri süreklilik planı: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan bilgi sistemleri süreklilik planını,

h) Bilgi sistemleri yönetimi: Bankaca gerçekleştirilen faaliyetlerin ve verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesi; mevzuattan kaynaklanan yükümlülüklerinin yerine getirilmesi; muhasebe ve finansal raporlama sisteminden sağlanan bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin, zamanında elde edilebilirliğinin ve gereken durumlarda gizliliğinin sağlanması amacıyla uygun bilgi sistemleri ortamının tesis edilmesine, bilgi sistemleri kaynaklarının verimli olarak kullanılmasına, söz konusu bilgi sistemlerinin kullanılmasından kaynaklanacak risklerin kontrolünün ve izlenmesinin sağlanmasına, bu amaçla gerekli sistemsel ve yönetsel önlemlerin alınmasına ilişkin

faaliyetleri,

ı) Bilgi teknolojileri: Herhangi bir biçimdeki verinin, girişinin yapılması, saklanması, işlenmesi, iletilmesi ve çıktılarının alınması için kullanılan donanım, yazılım, iletişim altyapısı ve ilgili diğer teknolojileri,

i) Bilgi varlığı: Bankacılık faaliyetlerinin yürütülmesinde kullanılan veriler ile bu verilerin taşındığı, saklandığı, iletildiği veya işlendiği sistem, yazılım, ağ cihazları, BT donanımları, iş süreçleri ve aktiviteleri gibi Banka için değeri olan her türlü varlığı,

j) Birincil merkez: Birincil sistemlerin tesis edildiği yapıyı,

k) Birincil sistemler: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan birincil sistemleri,

l) Biyometrik kimlik doğrulama bileşeni: Kimlik doğrulama işlemlerinin gerçekleştirilmesini sağlamak amacıyla kullanılan bir kişiye özgü ölçülebilir biyolojik veya davranışsal karakteristiği,

m) BS: Bilgi sistemlerini,

n) BT: Bilgi teknolojilerini,

o) Dış hizmet: 5/11/2011 tarihli ve 28106 sayılı Resmî Gazete'de yayımlanan Bankaların Destek Hizmeti Almalarına İlişkin Yönetmelik kapsamındaki destek hizmetleri dahil olmak üzere bankaların dışarıdan temin ettikleri her türlü hizmet alımlarını,

ö) DMZ: Bir kuruluşun dışa dönük BT servislerinin, internet gibi daha büyük ve güvenilmeyen bir ağa dahil edilmesini veya açılmasını sağlayan, iç ağdan yalıtılmış ve dış güvenlik duvarı tarafından korunan fiziksel veya mantıksal alt ağı,

p) DNS: İnternet alan adlarının IP adreslerine çevrilmesini sağlayan hiyerarşik alan adı isimlendirme sistemini,

r) Elektronik bankacılık hizmetleri: İnternet bankacılığı, mobil bankacılık, telefon bankacılığı, televizyon bankacılığı, açık bankacılık servisleri ile ATM ve kiosk cihazları gibi müşterilerin, bankanın fiziksel şubelerine gitmeden uzaktan bankacılık işlemlerini gerçekleştirebildikleri veya gerçekleştirilmesi için bankaya talimat verebildikleri her türlü elektronik dağıtım kanalını,

s) Elektronik imza: 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanan elektronik imzayı,

ş) Erişim kontrol kuralları: Bilgi sistemleri üzerindeki bir kullanıcının hangi uygulama işlevlerine, sistem kaynaklarına ve verilere erişebileceğini belirleyen kuralları,

t) Güvenli iletişim kanalı: Bankanın kendi müşterilerine sunduğu, kendisi veya diğer güvenli göndericiler dışındakilerin iletilerine kapalı olan elektronik posta kutusu, bankaya ait mobil bankacılık uygulaması veya internet bankacılığı sayfası gibi hem müşteri kimliğinin hem de müşterilere iletilmek istenen bilgilerin kaynağının banka olduğunun doğrulandığı iletişim kanalını,

u) Güvenlik duvarı: Farklı güvenlik seviyelerine sahip ağlar veya ağa bağlı cihazlar arasındaki trafik akış kontrolünü sağlayan donanım ya da yazılımları,

ü) Hassas veri: Sır niteliğindeki veriler ile kimlik doğrulamada kullanılan verileri,

v) İkincil merkez: İkincil sistemlerin kullanıma hazır olacak şekilde tesis edildiği ve birincil sistemlerde herhangi bir kesinti yaşanması durumunda personelin çalışmasına imkan tanıyacak ve birincil merkez ile aynı riskleri taşımayacak şekilde oluşturulmuş yapıyı,

y) İkincil sistemler: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan ikincil sistemleri,

z) İnternet bankacılığı: Bankaların kendi ticaret unvanı, işletme adı ya da herhangi başka bir ad altındaki bir web sayfası üzerinden sundukları hizmetlere müşterilerin, kullandıkları cihaz ya da platformdan bağımsız olarak, internet yoluyla ulaşmalarını ve kendilerine ait finansal veya kişisel verileri görüntüleyebildiği, değiştirebildiği ya da finansal sorumluluk yaratacak işlemler gerçekleştirebildiği elektronik dağıtım kanallarını,

aa) İSEDES Yönetmeliği: 11/7/2014 tarihli ve 29057 sayılı Resmî Gazete'de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmeliği,

bb) İş etki analizi: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan iş etki analizini,

cc) İşlem doğrulama kodu: Kimlik doğrulama yöntemlerinden biriyle kendisini sisteme tanıtan bir kişinin gerçekleştirmek istediği bir işlem için, bu işlemi onaylayıp onaylamadığına dair sisteme tanıttığı kimliğe yöneltilen, bir kereye mahsus kullanılmak üzere oluşturulmuş belirli uzunlukta harf ve/veya rakamlardan oluşan kodu,

çç) İz kayıtları: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile bir bilgi varlığına kimin eriştiğini veya erişmeye çalıştığını ve kullanıcının hangi işlemleri gerçekleştirdiğini gösteren kayıtları,

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

ee) Kesinti: Bir bankanın faaliyetlerinde veya bir sistemin fonksiyonlarındaki sürekliliğin, planlı geçişler haricinde sekteye uğramasını,

ff) Kimlik doğrulama: Bildirilen bir kimliğin gerçekten bildiren şahsa ait olduğuna dair güvence sağlayan mekanizmayı,

gg) Kişisel veri: 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununda tanımlanan kişisel veriyi,

ğğ) Kontrol: Banka içerisinde bilgi teknolojileri süreçleriyle ilgili olarak gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvenceyi oluşturma amacı güden politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,

hh) Kullanıcı: Banka personeli, dış hizmet sağlayıcı çalışanı veya banka müşterisi gibi bankanın bilgi sistemleri üzerinde işlem gerçekleştirmek üzere kendilerine hesap tanımlanmış olan her türlü kullanıcıyı,

ıı) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,

ii) Kurumsal SOME: 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 5 inci maddesinde ifade edilen Kurumsal SOME'yi,

jj) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,

kk) Mobil bankacılık: Akıllı telefon veya tablet gibi mobil bir cihaz üzerinde yüklü, bankaya ait mobil uygulama üzerinden müşterilerin bankacılık işlemlerini gerçekleştirebildikleri özelleşmiş internet bankacılığı dağıtım kanalını,

ll) MTBF: İki arıza veya kesinti arası ortalama süreyi,

mm) MTTR: Yaşanan arıza veya kesinti sonrası ortalama tamir süresini,

nn) Oturum: Veri aktarımı, sunuşu veya gerçekleştirilecek finansal işlemler için taraflar arasında kurulan mantıksal bağı,

oo) Parola: Kimlik doğrulamada kullanılan, değiştirilmesi zorunlu kılınmayan gizli harf ve/veya rakamlar dizisini,

öö) Parolanın sıfırlanması: Bir kullanıcıya ait parolanın kullanım dışı kaldığı, unutulduğu, kullanıcı hesabının kilitlendiği ya da ilk defa parolanın atanmasının gerektiği gibi durumlarda, bir yardım masası vasıtasıyla ya da sistemsel bir takım sorgulardan geçerek, kullanıcıya kendi parolasını belirleme imkânının verilmesini veya rastgele oluşturulmuş bir harf ve/veya rakamlar dizisinin yeni kullanıcı parolası olarak atanarak, bu parolanın kullanıcıya iletilmesini,

pp) Risk limitleri: İSEDES Yönetmeliğinin 38 inci maddesinde açıklanan risk limitlerini,

rr) Sektörel SOME: 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 7 nci maddesinde ifade edilen Kurum bünyesinde teşkil edilmiş Sektörel SOME'yi,

ss) Sızma testi: Sistemin güvenlik açıklarını istismar edilmeden önce tespit etmek ve düzeltmek amacıyla gerçekleştirilen güvenlik testlerini,

şş) Siber olay: Bilgi sistemlerinin veya bu sistemler tarafından işlenen bilgilerin gizlilik, bütünlük veya erişilebilirliğinin ihlal edildiği veya buna teşebbüste bulunulduğu durumlar ile banka ya da müşterilerinin zarar görmesine neden olabilecek bilgi sistemlerinden kaynaklanan her türlü olayı,

tt) Siber olaya müdahale: 11/11/2013 tarihli ve 28818 sayılı Resmî Gazete'de yayımlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğin 3 üncü maddesinde tanımlanan siber olaya müdahaleyi,

uu) SMS OTP: Elektronik haberleşme işletmecilerinin sunduğu kısa mesaj servisi aracılığıyla iletilen tek kullanımlık parolayı,

üü) Süreklilik Yüzdesi: MTBF / (MTBF+MTTR) formülü ile bulunacak yüzdesel değeri,

vv) Şifreleme açık anahtarı: Açık anahtarlı şifrelemede kullanılan, herkesin erişimine ve kullanımına açık olan, şifreleme gizli anahtarı ile matematiksel bağlantısı bulunan ve şifreleme gizli anahtarı ile atılan imzayı kontrol etmek, yapılan şifrelemeyi çözmek ya da sadece şifreleme gizli anahtarının çözebileceği şekilde verinin şifrelenmesi için kullanılan şifreleme anahtarını,

yy) Şifreleme anahtarı: Şifreleme algoritmasının şifreleme ve şifre çözme amacıyla kullandığı karakter dizisini,

zz) Şifreleme gizli anahtarı: Açık anahtarlı şifrelemede imza atma, şifreleme ve karşılığı olan şifreleme açık anahtarıyla şifrelenmiş veriyi çözmek için kullanılan, sadece sahibi tarafından bilinmesi ve kullanılması gereken anahtarı,

aaa) Tek kullanımlık parola: Kimlik doğrulamada sadece bir kez kullanılmak üzere rastgele oluşturulan harf ve/veya rakamlar dizisini,

bbb) Uçtan uca güvenli iletişim: İletişime konu veriye sadece alıcısının erişebilmesi amacıyla, söz konusu verinin gönderen tarafından sadece alıcının çözebileceği şekilde şifrelenerek iletilmesini,

ccc) Üst düzey yönetim: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan üst düzey yönetimi,

çççç) Üst yönetim: İSEDES Yönetmeliğinin 3 üncü maddesinde tanımlanan üst yönetimi,

ddd) Varlık muhafızı: Varlık sahibinin tanımladığı güvenlik gereksinimlerine uygun olarak, bir bilgi varlığının saklanması, taşınması, işlenmesi veya iletilmesi esnasında korunmasından sorumlu olan kişiyi,

eee) Varlık sahibi: Bilgi varlıklarına yönelik güvenlik gereksinimlerini belirleyerek varlık muhafızlarına ileten ve bu gereksinimlere uygun güvenlik kontrollerinin varlık muhafızları tarafından uygulandığını gözeterek bilgi varlığının idamesi ve erişilebilirliğinden sorumlu olan kişiyi,

fff) Yama: Programlarda tespit edilen güvenlik açıkları veya programın içeriğindeki hatalı bir fonksiyonu düzeltme amaçlı hazırlanan program eklentisini,

ggg) Yetkilendirme veritabanı: Müşteri ve kullanıcı erişim haklarının ve yetkilendirmeye ilişkin bilgilerin tutulduğu yapıyı

ifade eder.

İKİNCİ KISIM
Bilgi Sistemlerine İlişkin Risk Yönetimi ve Kontrollerin Tesisi

BİRİNCİ BÖLÜM
Bilgi Sistemleri Yönetişimi

Yönetim gözetimi, roller ve sorumluluklar

MADDE 4 – (1) Banka yönetim kurulu, bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele almakla, bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağını tahsis etmekle, bilgi varlıklarının güvenliği, gizliliği, bütünlüğü ve erişilebilirliğini sağlamak amacıyla bilgi sistemleri üzerinde etkin kontrollerin tesis edilmesini sağlamakla ve bilgi sistemlerinin kullanımından kaynaklanan risklerin yönetilmesi için etkin bir gözetim yürütmekle sorumludur. Bu amaçla, yönetim kurulu tarafından onaylanacak şekilde bir BS strateji planı, BS Strateji Komitesi ve BS Yönlendirme Komitesi oluşturulur ve bu komitelerin görev tanımları ve çalışma esasları da yönetim kurulu tarafından onaylı olacak şekilde yazılı hale getirilir.

(2) BS Strateji Komitesi, yönetim kurulu adına, BS strateji planı doğrultusunda BS yatırımlarının uygun bir şekilde kullanılıp kullanılmadığının ve bankanın iş hedefleri ile BS hedeflerinin birbiriyle uyumluluğunun gözetimini yürütmekle; bu hususlarda yönetim kuruluna doğrudan ve düzenli olarak raporlama yapmakla; BS strateji planını düzenli olarak gözden geçirerek gerekli olduğu durumlarda revize ederek yönetim kurulu onayına sunmakla ve BS Yönlendirme Komitesinin faaliyetlerini gözetmekle sorumludur.

(3) BS Strateji Komitesinde en az bir yönetim kurulu üyesinin bulunması ve BS'den sorumlu en üst düzey yönetici ile bankanın iş birimlerinden üst düzey yöneticilerin bu komiteye üye olması esastır. BS Strateji Komitesi, BS strateji planının düzgün bir şekilde uygulanıp uygulanmadığını gözden geçirmek ve önemli BS yatırım kararlarını değerlendirmek üzere yılda en az iki defa bir araya gelir ve yılda en az bir defa yönetim kuruluna rapor sunar.

(4) BS stratejisinin yönetim kurulu onayı doğrultusunda uygulanmasında, BS Strateji komitesine ve üst düzey yönetime yardımcı olmak maksadıyla bir BS Yönlendirme Komitesi oluşturulur. BS Yönlendirme Komitesi, BS yatırımlarının ve projelerinin öncelik sırasını belirlemek, devam eden BS projelerinin durumunu takip etmek, projeler arasındaki kaynak çatışmalarını çözüme kavuşturmak, BS mimarisi ve BS projelerinin mevzuata uyumluluğunu sağlamak üzere gerekli yönlendirmeleri yapmak ve BS servislerine ilişkin hizmet seviyelerini izlemekten sorumludur. BS Yönlendirme Komitesinde BS, insan kaynakları, hukuk, uyum ve bankanın iş birimlerinden temsilcilerin bulunması esastır. BS Yönlendirme Komitesi, yılda en az iki defa bir araya gelir ve yılda en az iki defa BS Strateji Komitesine rapor sunar.

(5) BS organizasyonu ve bilgi sistemlerinin kapsamlılık düzeyinin, bankanın büyüklüğü ve faaliyetlerinin karmaşıklığı ile orantılı olması ve BS organizasyon şemasının da bu doğrultuda oluşturulması esastır. BS organizasyon şeması kapsamındaki tüm birimlerin görev ve sorumlulukları ile bu birimlerdeki personelin görev tanımları açık bir şekilde yazılı hale getirilir, yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği üst düzey yöneticilerce onaylanır, bu görev tanımlarının uygunluğu düzenli olarak gözden geçirilir.

(6) BS personelinin kendilerine atanan görev ve sorumluluklar hakkında farkındalığa sahip olması ve kendilerine ait görev ve sorumluluklarda değişiklik yapılması halinde bu değişikliklerden haberdar olmaları sağlanır.

BS politika, prosedür ve süreç dokümanları

MADDE 5 - (1) Banka, bilgi sistemlerinin kullanımından kaynaklanan riskleri yönetmek ve bilgi varlıklarını korumak amacıyla uygulanması gereken usul ve esaslar ile tesis edilmesi gereken kontrolleri tarif eden BS politika, prosedür ve süreç dokümanlarını oluşturur.

(2) BS politikaları asgari olarak bu kısım altında yer verilen diğer bölümlere yönelik; BS prosedürleri ve süreç dokümanları ise asgari olarak bu kısım altında yer verilen diğer bölümlerin ilgili maddelerine yönelik oluşturulur ve oluşturulan tüm dokümanlara, dokümanların gizlilik derecesi ve banka çalışanlarının görev ve sorumluluklarının uygunluğu nispetinde erişim imkanı verilir. Dokümantasyon içerisinde, asgari olarak doküman kodu, dokümanın gizlilik derecesi, dokümanı onaylayan, revizyon tarihi, gözden geçirme tarihi, revizyon tarihçesi bilgileri yer alır.

(3) BS politikalarının yönetim kurulu tarafından onaylanması; BS prosedürleri ve süreç dokümanlarının ise yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği üst düzey yöneticilerce onaylanması esastır.

(4) BS politika, prosedür ve süreç dokümanlarının gerekleri, bankanın organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir, bunların işlerliğine ilişkin gözetim ve takip gerçekleştirilir. Bu kapsamda, politika ve prosedürlerin işletilmesinden sorumlu birimler ve görev tanımları ile süreç dokümanlarının işletilmesinden sorumlu süreç sahipleri ilgili politika, prosedür ve süreç dokümanları içinde belirtilir.

(5) BS politika, prosedür ve süreç dokümanları en az yılda bir defa gözden geçirilir ve gerekli olduğu durumlarda güncellenir.

İKİNCİ BÖLÜM
BS Risklerinin Yönetilmesi

BS risk yönetim süreci

MADDE 6- (1) Banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri analiz etmek, azaltmak, takip etmek ve raporlamak üzere bir BS risk yönetim süreci tesis eder.

(2) BS risk analizi kapsamında aşağıdaki faaliyetler yerine getirilir:

a) Bilgi varlıklarının tespit edilerek envanterinin çıkarılması ve bu varlıkların önem derecesine göre sınıflandırılması,

b) Bilgi varlıklarına ilişkin tehdit ve güvenlik açıklarının tespit edilmesi suretiyle risklerin belirlenmesi,

c) Tespit edilen tehdit ve güvenlik açıklarına göre bilgi varlıklarının riske maruz kalma olasılıklarının belirlenmesi,

ç) Risklerin gerçekleşmesi durumunda ilişkili bilgi varlığının gizliliği, bütünlüğü, erişilebilirliği gibi kriterlerine olan etkilerin belirlenmesi suretiyle ilgili bilgi varlığına yönelik etki hesaplaması yapılması,

d) Bilgi varlıklarını tehdit eden risklerin belirlenen olasılık ve etki değerlerine göre risk derecelendirmesinin yapılması,

e) Riski analizinde gerçekleştirilen çalışmaların bütününü temsil ederek özetleyecek ve üst yönetimin de anlayacağı risk kategorisini içerecek şekilde bilgi varlıklarına ilişkin varlık, varlık sahibi, risk kategorisi, tehdit, güvenlik açığı, risk ve risk seviyesini gösteren risk değerlendirme raporunun oluşturulması.

(3) Risk analizi sonuçlarına göre tespit edilen her bir BS riskine ilişkin, bu risklerin ilişkili olduğu bilgi varlıklarının değerine ve bankanın risk limitlerine uygun olacak şekilde risk azaltma ve kontrol stratejileri belirlenir. Bilgi varlıklarının değeri ele alınırken bu varlıkların ilişkili olduğu iş hedefleri ve iş süreçleri ile bunların bağlı olduğu diğer iş hedefleri ve iş süreçleri dikkate alınır. Risk azaltma ve kontrol stratejilerinin belirlenmesi aşamasında, riskin ilgili olduğu iş tarafının temsilcileriyle beraber risk analizi sonucu tespit edilen her bir riskin riskin azaltılması, riskten kaçınma, riskin kabulü ve riskin transferi gibi yöntemlerle nasıl ele alınacağına karar verilir. Bu kapsamda,

a) Riskin azaltılması, uygulanacak kontroller ile riskin azaltılmasını veya tamamen

ortadan kaldırılmasını,

b) Riskten kaçınma, riski doğuran sebebi ortadan kaldırmayı veya ilgili sistem veya teknolojiyi kullanmaktan vazgeçmeyi,

c) Riskin kabulü, riskin var olduğunu kabul ederek ilgili sistem veya teknolojiyi kullanmaya devam etmeyi,

ç) Riskin transferi, riskin gerçekleşmesi durumunda meydana gelebilecek zarardan etkilenmemek amacıyla sigorta yaptırmak gibi yöntemlerle riskin başkalarına aktarılmasını ifade eder.

(4) Risk azaltma ve kontrol stratejilerinin belirlenmesi aşamasında risklerin nasıl ele alınacağına karar verildikten sonra bu kararların uygulanmasını sağlayacak risk aksiyon planları oluşturulur. Alınacak aksiyonlar için yapılacak kaynak aktarımında ve aksiyonların tamamlanma tarihlerinin önceliklendirilmesinde, risk analizi aşamasında belirlenen risk dereceleri dikkate alınır.

(5) Risk aksiyon planında belirlenen aksiyonların alınması risk analizi sonucu tespit edilen riskleri ortadan kaldırmıyorsa, aksiyon planının uygulanması sonucu kalacak artık riskler tespit edilir ve artık risklerin, riskin azaltılması, riskten kaçınma, riskin kabulü ve riskin transferi seçeneklerinden hangisi kapsamında ele alınacağı tekrar belirlenerek risk aksiyon planı güncellenir.

(6) Riskin kabul edilebilmesi için BS'den sorumlu en üst düzey yöneticinin yazılı onayının bulunması ve söz konusu riskin mevzuata aykırılık teşkil etmemesi şarttır. Kabul edilecek riskin aynı zamanda bir iş süreci veya iş uygulamasıyla ilgili olması durumunda bu iş tarafının en üst düzey yöneticisinin de riskin kabul edildiğine ilişkin yazılı onayının bulunması gerekir. Kabul edilen riskler için, sonradan telafi edici yeni kontrol tekniklerinin ya da yeni güvenlik çözümlerinin ortaya çıkmış olması veya riskin eskiye nazaran artıp artmadığı yönünde koşulların değişmiş olması ihtimaline karşı, önceden kabul edilmiş olan riskler periyodik olarak gözden geçirilir.

(7) Risk analizleri sonucu hazırlanan güncel risk değerlendirme raporu ve güncel risk aksiyon planı birleştirilerek bankanın BS risk envanteri oluşturulur. Banka, yılda en az bir defa veya bilgi sistemlerinde meydana gelecek önemli değişikliklerden önce risk analizlerini tekrarlar. Tekrarlanan risk analizi sonuçlarına göre risk aksiyon planı ve BS risk envanterinin güncellenmesi sağlanır. Banka bünyesinde gerçekleştirilen BS iç kontrol ve iç denetim çalışmalarının sonuçlarının veya tespit edilen bulguların risk envanterine girdi teşkil etmesi sağlanır.

(8) BS güvenlik fonksiyonu, bu madde altında belirtilen BS risk yönetimi çalışmalarına, bütüncül bir güvenlik bakış açısıyla, bilgi varlıklarına yönelik olarak gizlilik, bütünlük, erişilebilirlik kriterleri bakımından aktif katkı sağlamakla yükümlüdür.

(9) Bankanın, kurumsal risk yönetimi sürecinin, BS risklerini de kapsaması esastır. Bu çerçevede, BS risklerinin bankacılık faaliyetlerinden kaynaklanan diğer risklerin de bir çarpanı olabileceği dikkate alınarak banka genelinde, bilgi teknolojilerinden kaynaklanan riskleri de içerecek şekilde, bütünleşik bir risk yönetim metodolojisi uygulanır ve BS risk yönetim süreci çıktılarından elde edilen verilerin bankanın bütünsel risk yönetim çerçevesinin bir parçası haline gelmesi sağlanır. Bu doğrultuda, BS risk envanteri kapsamında riskler takip edilerek yönetim kuruluna ve üst düzey yönetime yılda en az bir defa raporlanır.

ÜÇÜNCÜ BÖLÜM
Bilgi Güvenliği Yönetimi

Bilgi güvenliği organizasyonu, roller ve sorumluluklar

MADDE 7– (1) Banka bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk yönetim kurulundadır. Yönetim kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin uygun düzeye getirilmesi hususunda gerekli kararlılığı göstermekle ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis etmekle yükümlüdür. Bu sorumluluk kapsamında yönetim kurulu, banka genelinde uygulanmasını gözetmekle yükümlü olduğu bir bilgi güvenliği yönetim sistemi tesis eder. Bilgi güvenliği yönetim sisteminin ulusal veya uluslararası bir standart ya da en iyi uygulamaları temel alması ve aşağıdaki faaliyetleri de içermesi esastır.

a) Bilgi varlıklarına yönelik olarak düzenli bir şekilde tehdit ve risk değerlendirme çalışmalarının yapılması,

b) Bilgi varlıklarının sınıflandırılarak varlık sahipliklerinin belirlenmesi ve varlık sınıflarına uygun güvenlik önlemlerinin alınması,

c) Bilgi güvenliği ihlaline ilişkin olayların izlenmesi ve raporlanması,

ç) Banka genelinde ve verilen tüm bankacılık hizmetlerinde, görevler ayrılığı prensibi ile tutarlı etkin bir kimlik doğrulama ve erişim yönetiminin tesis edilmesi,

d) Bilgi güvenliğinin sağlanmasına ilişkin kontrollerin ve tesis edilen yapıların test edilmesi ve test sonuçlarının takip edilerek raporlanması,

e) Bilgi varlıklarına yönelik güncel güvenlik açıklarının takip edilmesi ve gerekli güncelleme ve yamaların uygulanması,

f) Üst yönetim de dahil olmak üzere tüm banka çalışanları, dış hizmet sağlayıcılar ve müşteriler gibi bankanın bilgi güvenliğini ilgilendiren tüm paydaşlara yönelik, bilgi güvenliği farkındalığını artıracak çalışmaların yapılması,

g) İş sürekliliği yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması,

ğ) Dış hizmet alımlarının yönetimi kapsamında bilgi güvenliğini ilgilendiren hususların da yer almasının sağlanması.

(2) Bilgi güvenliği yönetim sisteminin banka genelinde nasıl uygulanacağı bilgi güvenliği politikası, prosedürleri ve süreç dokümanları ile tarif edilir. Bankanın bilgi güvenliği politikası yönetim kurulu tarafından onaylanır ve banka çapında yayımlanarak tüm çalışanlara ulaştırılması sağlanır.

(3) Bilgi güvenliği politikasının oluşturulması ve uygulanması faaliyetleri yönetim kurulu adına Bilgi Güvenliği Komitesi tarafından gerçekleştirilir. Bilgi Güvenliği Komitesine, Genel Müdür başkanlık eder ve komitenin koordinasyonunu Bilgi Güvenliği Sorumlusu yerine getirir. Bilgi Güvenliği Komitesi toplantılarına BS'den sorumlu en üst düzey yönetici ile insan kaynakları, hukuk, uyum, risk yönetimi, iç denetim ve bankanın iş birimlerinden üst düzey yöneticilerin de katılması, böylelikle bilgi güvenliği çalışmalarının koordinasyonunun bankanın farklı birimlerden gelen yetkililer tarafından gerçekleştirilmesi esastır. Bilgi Güvenliği Komitesinin görev tanımları ve çalışma esasları, yönetim kurulu tarafından onaylı olacak şekilde yazılı hale getirilir, yılda en az iki defa toplanması ve yılda en az bir defa yönetim kuruluna rapor sunması sağlanır.

(4) Bilgi güvenliği prosedür ve süreç dokümanlarının onaylanması ve bunların sürekli bir şekilde bakımının sağlanması da Bilgi Güvenliği Komitesinin sorumluluğundadır. Bilgi güvenliği politikası, prosedürleri ve süreç dokümanları en az yılda bir defa gözden geçirilir ve önemli güvenlik olayları, yeni güvenlik açıkları ya da teknik altyapıdaki önemli değişikliklerden sonra da bunların ayrıca gözden geçirilmesi sağlanır.

(5) Banka bünyesinde, BS'den sorumlu en üst düzey yönetici ve onun altındaki

birimlerden meydana gelen BS fonksiyonundan ayrı ve bağımsız olacak şekilde bir BS güvenlik fonksiyonu oluşturulur. BS güvenlik fonksiyonunun doğrudan Genel Müdüre bağlı olması esastır. Bankanın BS güvenlik fonksiyonu, Bilgi Güvenliği Sorumlusu tarafından yönetilir.

(6) Bilgi güvenliği sorumlusu aşağıdaki görevleri yerine getirir:

a) Bilgi güvenliği politikası, prosedürleri ve süreç dokümanlarının oluşturulması, bunların bakımının yapılması ve onaylanmak üzere yönetim kurulu veya Bilgi Güvenliği Komitesine sunulması,

b) BS risk yönetimi çalışmalarında, bilgi güvenliği bakış açısıyla, ilişkili bilgi varlıklarına yönelik olarak gizlilik, bütünlük, erişilebilirlik kriterleri bakımından BS risk yönetimi ekibine aktif katkı sunulması ve yardımcı olunması,

c) Bilgi varlıklarının ve kritik sistemlerin sınıflandırılması çalışmalarına yardım edilmesi,

ç) İlgili birimlerle uyum içinde, iş gereksinimleri ve iş hedefleriyle uyumlu banka çapında bilgi güvenliğinin tesis edilmesi,

d) Banka bünyesinde uygulanacak güvenlik çözümlerini geliştirecek bilgi güvenliği personelinin işe alınmasının ve yetiştirilmesinin sağlanması,

e) Bilgi güvenliği ile ilgili mevzuat hükümleri, standartlar, politika, prosedür ve süreç dokümanlarına uyumun takip edilmesi,

f) Bilgi güvenliği aktivitelerinin ve testlerinin yürütülmesinin sağlanması ve bunların takip edilmesi,

g) Önemli projeler ve değişiklikler için bilgi güvenliği gereksinimlerinin belirlenmesi çalışmalarına katkıda bulunulması,

ğ) Bankanın bilgi güvenliğini ilgilendiren tüm paydaşlara yönelik bilgi güvenliği farkındalık programının yürütülmesi.

Varlık envanteri ve verilerin sınıflandırılması

MADDE 8– (1) Banka, bilgi varlıklarının güvenlik gereksinimlerine uygun kontroller tesis etmek için bu varlıkları sınıflandırarak tüm bilgi varlıkları için detaylı bir varlık envanteri hazırlar. Hazırlanacak varlık envanterinde her bir bilgi varlığı için,

a) Varlığın ne olduğunu açıkça belirtecek tanımına,

b) Banka için görece değerine,

c) Bulunduğu konuma,

ç) Varlığın güvenlik sınıfına ve bu sınıfın belirlenmesine neden olan gizlilik, bütünlük, erişilebilirlik gibi değerlerine,

d) Varlığın sahibine,

e) Varlığın muhafızına

yer verilir.

(2) Bilgi varlıklarının bir parçası olan ve bilgi sistemleri üzerinde işlenen, iletilen, saklanan ve yedek olarak tutulan banka için değer ifade eden tüm veriler için bilgi varlığı envanterinin haricinde birinci fıkrada belirtilen detayları içerecek şekilde bir veri envanteri hazırlanır. Söz konusu veri envanterinde varlık sahibi yerine veri sahibi, varlık muhafızı yerine veri muhafızı bilgilerine yer verilir.

(3) Varlık ve veri sahipleri ile birlikte çalışılmak suretiyle, her bir varlık ve verinin tanımlı ve onaylı bir güvenlik sınıfına ve erişim kısıtlamasına sahip olması sağlanır. Söz konusu güvenlik sınıfları ve erişim hakları iki yıldan uzun olmayacak periyotlarla düzenli olarak gözden geçirilir.

(4) Bilgi varlıklarının, nasıl sınıflandırılacağına yönelik olarak Bilgi Güvenliği Komitesi tarafından onaylı bir varlık sınıflandırma kılavuzu hazırlanır. Varlıkların güvenlik sınıfı belirlenirken yasal statüsü, gizlilik derecesi, bütünlük gereksinimleri, erişilebilirlik gereksinimleri, saklama süresi ve asgari yedekleme sıklığı gibi kriterler göz önünde bulundurulur.

(5) Verilerin güvenlik sınıfı belirlenirken asgari olarak bu verilerin gizlilik derecesi,

bütünlük gereksinimleri, erişilebilirlik gereksinimleri ve hassas ya da kişisel veri olup olmadığı gibi kriterler göz önünde bulundurulur.

Veri gizliliği

MADDE 9– (1) Banka, bankacılık faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu sırada gizliliğini sağlayacak önlemleri alır. Verilerin tutulduğu ortamın kağıt veya elektronik ortam olmasından bağımsız olarak alınacak önlemlerin, gizliliği sağlanmaya çalışılan verilerin gizlilik derecesine uygun olması ve gerekli yerlerde ek kontrollerin tesis edilmesi esastır. Veri barındıran medya ya da cihazların kullanımdan kaldırılması durumunda, içerdikleri verilerin gizlilik derecesine uygun olarak güvenli bir şekilde imha edilmesi sağlanır.

(2) Veri gizliliğini sağlamada kullanılacak şifreleme teknikleri için güncel durum itibariyle güvenilirliğini yitirmemiş ve günün teknolojisine uygun algoritmalar temel alınır. Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanılabileceği zaman zarfında kırılamayacak şekilde uzun seçilir ve ilgili veri ya da operasyonun kritiklik seviyesine göre bu anahtarların geçerlilik süresi belirlenir. Geçerlilik süresi dolan ya da güvenilirliğini yitirdiği bilinen şifreleme anahtarlarının kullanımı engellenir. Şifreleme anahtarlarının tüm yaşam döngüsü boyunca güvenliğinin sağlanması, güvenli bir şekilde oluşturulması, müşteri ve personel kullanımına sunulması ve saklanması esastır.

(3) Hassas verilerin iletiminde uçtan uca güvenli iletişimin kullanılması ve bu verilerin şifrelenmiş bir şekilde saklanması esastır. Bu kapsamda, bankanın personeline tahsis ettiği hassas veri içeren tüm masaüstü, dizüstü ve mobil cihazların içeriğinin şifrelenmesi sağlanır ve ağa bağlı sunucu cihazlar üzerinde açık metin halinde banka kartı veya kredi kartı numarası, TC kimlik numarası gibi hassas verilerin bulunup bulunmadığını belirlemek için sunucu makineleri periyodik olarak taranır.

Kimlik ve erişim yönetimi

MADDE 10– (1) Banka, tüm bilgi varlıklarına olan erişimlerin, görevler ayrılığı prensibine göre belirlenmiş kullanıcılarca ve bu kullanıcıların sorumluluğu gereği kendileri için tanımlanan erişim kontrol kuralları uyarınca, ilişkili bilgi varlığının güvenlik sınıfına uygun bir kimlik doğrulama yöntemiyle gerçekleştirilmesini sağlamakla yükümlüdür.

(2) Bilgi sistemleri üzerindeki kullanıcılara uygulanacak kimlik doğrulama mekanizması, kullanıcıların bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde tesis edilir ve kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek önlemler alınır.

(3) Banka, bilgi sistemleri üzerindeki kullanıcılara ait kimlik doğrulama bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri alır. Bu kapsamda kimlik doğrulama bilgilerinin veritabanlarında şifreli olarak muhafaza edilmesi, kimlik doğrulama amacıyla aktarılırken şifrelenmesi, yetkisiz erişimlere veya görevler ayrılığı prensibine aykırı olarak kontrolsüz bir şekilde gerçekleştirilecek değişikliklere karşı korunması, bu veritabanları üzerinde gerçekleştirilen işlemlere ilişkin yeterli iz kayıtlarının tutulması ve bu iz kayıtlarının güvenliğinin sağlanması gibi önlemler alınır.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasının aşağıdaki fonksiyonları yerine getirmesi sağlanır:

a) Başarısız kimlik doğrulama teşebbüsleri hakkında, ilgili kullanıcının sisteme ilk girdiği anda bilgi vermesi, başarısız teşebbüslerin belirli bir sayıyı aşması halinde ise ilgili kullanıcının erişimini bloke etmesi,

b) Başarısız kimlik doğrulama teşebbüsleri sonrasında, bu teşebbüsü gerçekleştiren kişiye, hatalı girilen kullanıcı adı bilgisi veya parola ile ilgili, böyle bir kullanıcı adının sistemde olmadığı veya parolanın hatalı girildiği gibi, gereksiz bilgi vermemesi,

c) Hiçbir işlem yapılmayan hareketsiz oturumlar için oturumu belirli bir süre sonra

sonlandırması,

ç) Birden fazla kullanıcının aynı kullanıcı hesabını kullanmaları ya da aynı anda farklı oturumlar açabilmeleri konusunda yetkilendirildiği durumlar hariç olmak üzere, aynı kullanıcı için aynı anda birden fazla oturum açılmaya çalışılması durumunda buna izin vermemesi ve kullanıcıya uyarı vermesi.

(5) Kullanıcılara uygulanacak erişim kontrol kuralları ve atanacak yetkilerin belirlenmesinde görevler ayrılığı prensibi esas alınır. Bu kapsamda süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından başlatılması, onaylanması ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir. Bu çerçevede, erişim yetkilerinin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin de birbirinden ayrılması sağlanır. Görevlerin tam manasıyla ve uygun şekilde ayrıştırılmasının mümkün olmadığı durumlarda, bu durumdan kaynaklanabilecek hata ve suistimalleri önlemeye yönelik risk azaltıcı veya telafi edici ilave kontroller tesis edilir.

(6) Kullanıcılar, geçerli bir iş ihtiyacının mevcut olduğu ve erişimin gerekli olduğu süre zarfında, bilgi varlıklarına erişebilmeleri için yetkilendirilir. Bu çerçevede bilgi varlıklarına erişim yetkisi olan tüm kullanıcıların, ilgili bilgi varlığı sahibi tarafından düzenli olarak gözden geçirilmesi, kullanıcıların görev ve sorumlulukları göz önünde bulundurularak sadece bu görevleri yerine getirmelerine yetecek ve sadece bilmeleri gereken verilere erişmelerini sağlayacak kadar yetkiye sahip olmaları sağlanır.

(7) Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesapları ile ilgili olarak aşağıdaki tedbirlerin alınması sağlanır:

a) Ayrıcalıklı yetkilere sahip kullanıcılar için çok bileşenli kimlik doğrulamanın uygulanması,

b) Ayrıcalıklı yetkilere sahip kullanıcı ve uygulama hesaplarının sayısının kısıtlanması ve yalnızca gerekli olan kullanıcılara bu yetkilerin atanması ve sadece gerekli olan durumlarda bu hesapların kullanılması,

c) Bu tür hesaplar ile gerçekleştirilen işlemleri daha yakından takip edecek şekilde iz kayıtlarının tutulması ve bunların düzenli olarak gözden geçirilmesi,

ç) Banka içinde kullanılan sistemlerde ayrıcalıklı yetkilere sahip bir kullanıcı hesabı oluşturulduğunda veya silindiğinde bu tür işlemler için iz kaydı tutulması ve uyarı üretilmesi,

d) Ayrıcalıklı yetkilere sahip kullanıcı hesaplarına yapılan başarısız giriş denemeleri için iz kaydı tutulması ve uyarı üretilmesi,

e) Ayrıcalıklı yetkilere sahip kullanıcı hesaplarının ortaklaşa kullanılmasının engellenmesi veya bu hesapları kullanan gerçek kişilere sorumluluk atayacak tekniklerin kullanılması,

f) Ayrıcalıklı yetkilere sahip kullanıcı hesaplarının parolalarının güvenli ortamlarda saklanması ve bu parolaların belirli periyotlarda değiştirilmesini sağlayacak konfigürasyonların yapılması,

g) Ayrıcalıklı yetkilere sahip uygulama hesaplarına ilişkin parolaların tahmin edilmesi zor ve günün teknolojisine uygun uzunluk ve zorlukta olacak şekilde sıklıkla değiştirilmesi.

(8) Acil durumlara özgü yetkilendirmeler geçici olarak yapılır ve bu yetkilendirme süresince gerçekleştirilecek işlemlerin takibine imkan verecek iz kayıtlarının tutulması sağlanır.

(9) Personelin işe alınması, işten ayrılması ve görev değişikliği gibi insan kaynaklarında yaşanan değişikliklerde, ilgili kullanıcı hesaplarının silinmesi, askıya alınması, kullanıcıya atanmış yetkilerin geri alınması ya da değiştirilmesi gibi işlemler olayın gerçekleşmesine müteakip yerine getirilir. İnsan kaynakları değişikliklerine dayanan yetkilendirme işlemleri otomatik olarak gerçekleştirilmiyorsa, manuel değişiklik gerçekleştirme sürecinde görevler ayrılığı prensibi uygulanır ve değişikliği gerçekleştirmeye yetkili personelin faaliyetlerine ilişkin iz kayıtları ile insan kaynaklarındaki değişikliklerin uyumlu olup olmadığı düzenli olarak gözden geçirilir.

(10) Bilgi sistemleri üzerindeki tüm kullanıcılar için benzersiz kullanıcı tanımlama

kodları tanımlanır ve zorunlu olmadığı müddetçe ortak veya jenerik kullanıcı hesapları kullanılmaz. Ortak veya jenerik kullanıcıların kullanımının zorunlu olduğu durumlarda ise bu kullanıcı hesapları ile işlemi yapan kişiye sorumluluk atamaya yönelik ilave kontroller tesis edilir.

(11) Kullanıcı parolalarının yönetiminde asgari olarak aşağıdaki tedbirlerin alınması sağlanır:

a) Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesi,

b) Kullanıcıların, parolalarını belirlerken tahmin edilmesi zor, günün teknolojisine uygun uzunluk ve zorlukta kompleks parola seçimine zorlanması,

c) Kullanıcıların, sistem güvenliği ile ilgili bir kuşku oluşması halinde ve düzenli aralıklarla parolalarını değiştirmeye zorlanması,

ç) Kullanıcıların eski parolalarının hatırlanması suretiyle geriye dönük olarak belirli sayıda eski parolanın kullanılmasının engellenmesi.

(12) Banka, kullanıcı hesaplarına yönelik olarak kilitli hesaplar, devre dışı bırakılmış hesaplar, maksimum parola yaşını aşan hesaplar ve parola son kullanma süresi hiçbir zaman dolmayacak şekilde ayarlanmış hesaplar için otomatik olarak rapor üreten yöntemler kullanır ve bu raporları gerekli önlemleri alması için ilgili sistem yöneticisine iletir.

Bütünlük kontrolleri

MADDE11- (1) Banka, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli tedbirleri alarak bunların doğruluğunu, tamlığını ve güvenilirliğini temin eder. Bütünlüğü sağlamaya yönelik tedbirler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir. Dış hizmet sağlayıcılar nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.

(2) Bilgi sistemlerine ilişkin işlemlerin doğruluğu ve güvenilirliği asgari olarak, yapılmak istenen işleme ait anahtar öneme sahip bilgilerin işlemin başlangıcından tamamlanışına kadar doğruluğunu yitirmemesini ve yapılmak istenen işlemin kendinden beklenen sonucu yerine getirmesini; tamlığı ise asgari olarak bütün işlemlerin hata üretmeden gerçekleşmesini ve mükerrer olmamasını gerektirir.

İz kayıtlarının oluşturulması ve takibi

MADDE 12- (1) Banka, bilgi sistemlerinin ve faaliyetlerinin boyutu ve karmaşıklığıyla orantılı olacak şekilde bilgi sistemleri dahilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması tesis eder. Tesis edilecek iz kayıt mekanizmasının yaşanan siber olayların sonradan incelenmesine ve bunlar hakkında güvenilir delillerin elde edilmesine imkan tanıyacak nitelikte olması sağlanır.

(2) İz kayıtları, işlemin doğasına uygun detay ve içerikte, asgari olarak aşağıdaki bilgileri barındırır:

a) Kaydı oluşturan sistem,

b) Kaydın oluşturulduğu tarih, saat ve zaman dilimi bilgisi,

c) Kaydı oluşturan işlem ya da olayla birlikte, gerçekleştirilen değişikliğin ne olduğunu gösterecek bilgi,

ç) Kaydın ilişkili olduğu tekil kullanıcı veya sistemi gösteren bilgi.

(3) Bilgi sistemleri dahilinde gerçekleşen ve bankacılık faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemler ile hassas verilere erişilmesi veya bunların sorgulanması, görüntülenmesi, kopyalanması, değiştirilmesine yönelik işlemler ve kritik bilgi varlıklarına yönelik erişim yetkilerinin verilmesi, değiştirilmesi ve geri alınmasına yönelik tüm aktiviteler ile bu varlıklara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları asgari üç yıl boyunca banka nezdinde erişime açık tutulur. Bankanın, web servisleri, API ya da benzeri metotlarla diğer kurum veya kuruluşlar nezdinde tutulan hassas veriler ile kişisel verilere ilişkin yaptığı

sorgulamalar ve bu sorgulamaları hangi amaçla yaptığına ilişkin iz kayıtları da bu kapsamdadır. Bunlar dışındaki iz kayıtlarının erişime açık tutulma süresini banka kendisi belirler. Bilgi varlıklarının kritikliğinin değerlendirilmesi hususunda 8 inci maddede belirtilen varlık sınıfları baz alınır.

(4) İz kayıtları erişime açık tutulma süresinden bağımsız olarak güvenilir ortamlarda yedeklenir ve ihtiyaç duyulması halinde makul bir sürede bu yedeklerden geri dönüş sağlanarak inceleme yapılmasına imkan verecek şekilde Kanunun 42 nci maddesinde belirtilen süre boyunca banka nezdinde saklanır.

(5) İz kayıtlarının bütünlüğünün bozulmasının önlenmesine ve herhangi bir bozulma durumunda bunun tespit edilebilmesine ilişkin teknikler kullanılır. İz kayıtlarına, bilmesi gerektiği kadar prensibine uygun olarak sadece erişim yetkisi verilen kişilerin ulaşabilmesi ve kayıt sisteminin her türlü yetkisiz değişiklik ve müdahalelere karşı korunması sağlanır. Kullanıcıların kendi faaliyetlerine ilişkin iz kayıtlarına müdahalesi engellenir ve iz kayıt sisteminin durdurulmasını önlemeye veya durdurulması halinde bu durumu tespit etmeye yönelik teknikler kullanılır.

(6) Banka, iz kayıt sisteminin önceden belirlenmiş ve belirli periyotlarla güncellenen senaryolar çerçevesinde düzenli olarak gözden geçirilmesine, takip edilmesine ve olağandışı durumlar ile şüpheli ya da yüksek riskli işlemlerin raporlanmasına ilişkin süreçleri tesis eder. Olağandışı durumlar ile şüpheli ya da yüksek riskli işlemlere yönelik rapor üretilmesi ve rapor sonuçlarının takip edilmesi sağlanır.

(7) Banka bilgi sistemlerine ilişkin dış hizmet alması halinde, dış hizmet sağlayıcı tarafından tutulan iz kayıtlarının kendi standartlarına uygunluğunu ve bu iz kayıtlarının kendisi tarafından erişilebilir olmasını temin eder.

Siber olay yönetimi, acil ve beklenmedik durum müdahale planı

MADDE 13- (1) Banka, siber olaylardan sonra bankacılık faaliyetlerini en az etkileyecek şekilde ve mümkün olan en kısa sürede BS hizmetlerini normal işleyişine döndürmek üzere gerçekleşen siber olayların ele alınmasına ve takibine yönelik siber olay yönetimi ve siber olaylara müdahale süreci oluşturur. Bu kapsamda, BS fonksiyonundan ayrı ve bağımsız olacak şekilde yeterli teknik ve operasyonel becerilere sahip bir Kurumsal SOME kurulması, bu Kurumsal SOME'ye ilişkin güncel iletişim bilgilerinin Kuruma iletilmesi ve güvenlik olaylarının Kuruma ve ilgili yönetim birimlerine raporlanması sağlanır.

(2) Kurumsal SOME siber olay öncesinde, bilgi işlem varlıkları üzerinde rutin sızma testi çalışması yapmak veya yaptırmakla, kayıt yönetimi sistemi arayüzünden rutin olarak iz kayıtlarını takip etmekle ve kurum içi siber güvenlik farkındalık çalışmalarını yürütmekle; siber olay esnasında ise, BS fonksiyonunun yapacağı müdahaleyi yönetmekle ve BS fonksiyonunda görevli ilgili personeli koordine etmekle sorumludur.

(3) Siber olayların önem derecelerine uygun olacak şekilde ele alınmasını sağlamak üzere, siber olayların önemlilik sınıflandırmasına yönelik kriterler yazılı hale getirilir ve gerçekleşen her bir siber olayın bu kriterlere göre belirlenen önem düzeyiyle orantılı olan bir zaman zarfında ele alınması ve çözüme kavuşturulmasına yönelik prosedürler ile acil ve beklenmedik durum müdahale planları oluşturulur. Oluşturulan müdahale planlarında öngörülen senaryolar için, faaliyetlerin güvenilir bir şekilde sürdürülmesini sağlayan hızlı, etkili ve düzenli bir tepki süreci tesis edilir. Bu kapsamda müdahale planlarının işlerliği yılda en az bir kez test edilir ve test sonuçları üst yönetime raporlanır.

(4) Acil ve beklenmedik durum müdahale planları kapsamında, bilgi sistemlerine ilişkin olayın kaynağını hızlı bir şekilde bulmayı sağlama, yetkili birimlere ulaşmayı sağlama, olayın potansiyel boyutunu, etkisini, hasarı ve etkilenen müşterileri tespit etme ve olayı çözüme kavuşturma süreçleri ele alınır.

(5) Banka, yaşanan bir siber olayın büyüyerek bir krize dönüşmesi, hassas verilerin ya da

kişisel verilerin sızması ya da ifşası ile sonuçlanması, Bilgi Sistemleri Süreklilik Planının ya da ikincil merkezin devreye alınması gibi hallerde derhal Sektörel SOME'yi bilgilendirir. Yaşanan siber olayın müşterilere sunulan hizmetlerde iki saatten daha uzun süreli bir kesintiye yol açacağı öngörüldüğünde, uygun yöntemlerle müşterilerin ve kamuoyunun bilgilendirilmesi sağlanır.

(6) Banka, BS hizmetlerinde ciddi kesintilere veya bozulmalara yol açan önemli siber olaylar için bir kök neden ve etki analizi yapmak ve benzer olayların tekrarını önlemek için iyileştirici önlemleri almakla yükümlüdür.

Ağ güvenliği

MADDE 14- (1) Banka, gerek kendi kurumsal ağı gerek dış ağlardan gelebilecek tehditler için gerekli ağ kontrol güvenlik sistemlerini tesis eder. Güvenlik önlemlerinin tesis edilmesinde, bir güvenlik katmanının aşılması halinde diğer güvenlik katmanının devreye girdiği katmanlı güvenlik mimarisi esas alınır.

(2) Banka, dış ağı ve iç ağı arasındaki trafiği kontrol altında tutmak için gerektiği şekilde konfigürasyonu yapılmış ve sürekli gözetim altında tutulan güvenlik duvarı çözümleri ile saldırıları tespit edebilecek ve önleyebilecek günün teknolojisine uygun sistemler kullanır.

(3) İç ağdan gelebilecek tehditlerin etkisini azaltmak ve banka iç ağının farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere banka iç ağındaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşmasını sağlayacak şekilde banka iç ağı alt bölümlere ayrılır. Farklı ağ segmentleri arasındaki hassas veri trafiği kontrol edilir ve güvenliği sağlanır. Ayrıca iç ağa sadece yetkilendirilmiş cihazların bağlanabilmesi sağlanır.

(4) İnternetten erişilebilen herhangi bir sistemin DMZ'de olması ve DMZ'de yer alan sistemlerin hiç bir şekilde hassas veri içermemesi esastır. Hassas verilere sahip tüm sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanır. DMZ sistemleri, özel iç ağdaki sistemlerle yalnızca vekil uygulamalar veya güvenlik duvarı cihazları üzerinden iletişim kurmalıdır.

(5) Ağ üzerinde kimlik ve erişim yönetimine yönelik kurulan etki alanı yönetimi sunucuları gibi tüm yapıların bankaya özgü bağımsız bir yapıda olması ve banka dışındaki başka bir etki alanı ya da benzerinin parçası olmaması esastır.

(6) Kritik ağ segmentlerine yapılan tüm bağlantılar düzenli olarak tespit edilerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz tüm bağlantıların sonlandırılması sağlanır. Benzer şekilde, ağa bağlı her bir sistem üzerindeki portların, protokol ve servislerin sadece gerekliliği onaylanmış iş ihtiyaçlarına istinaden açık ve çalışıyor olması sağlanır. Bu doğrultuda, güvenli bir baz konfigürasyonu temel alarak önemli tüm sunucu ve sistemler için düzenli olarak port taraması gerçekleştirilir ve güvenli baz konfigürasyonda bulunmadığı halde açık durumda olan portların kapatılması sağlanır.

(7) Zorunlu bir iş gereksinimi olmadıkça ve Bilgi Güvenliği Sorumlusu tarafından onaylanmadıkça banka personeli ya da dış hizmet sağlayıcıları tarafından banka içi uygulama ve sistemlere, banka dışından uzaktan erişim gerçekleştirilmez. Uzaktan erişimin zorunlu olduğu hallerde ise çok bileşenli kimlik doğrulamaya dayanan güvenli bağlantı yöntemleri uygulanır, erişimler kayıt altına alınır, söz konusu bağlantının süresi ve bağlantının yapılabileceği cihazlar kısıtlanır ve kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanır.

(8) İnternet üzerinden veya banka dış ağından görünür olan tüm sunucu ve sistemler, görünür olmalarını gerektirecek geçerli bir iş ihtiyacının olup olmadığı açısından düzenli olarak kontrol edilir ve eğer gerekli değilse bu sunucu ve sistemlerin banka iç ağına taşınması ve iç ağ IP adreslerine sahip olması sağlanır.

(9) Banka iç ağından internete doğru akan tüm dış ağ trafiğinin, en az bir vekil sunucu üzerinden geçmesi ve bu vekil sunucuların dışarıya akan tüm trafiğin içeriğini kontrol etmesi sağlanır. Yapılacak içerik kontrolünün, zararlı IP adreslerine olan trafik akışını ve banka kartı veya kredi kartı numarası, TC kimlik numarası gibi hassas verilerin sızdırılmasını engelleyecek nitelikte olması ve aynı zamanda TCP oturum bilgilerini kayıt altına alarak olağandışı uzun süreli oturumları tespit edecek ve bunlar için uyarı üretebilecek yetenekte olması sağlanır.

(10) Bankaya ait e-posta hesaplarını taklit eden sahte e-posta iletilerinin engellenmesi amacıyla e-posta sunucularında gönderici kimliğini doğrulayıcı teknikler kullanılır.

Güvenlik konfigürasyonu yönetimi

MADDE 15- (1) Banka, tüm masaüstü, dizüstü, mobil cihazlar, iş istasyonu makineleri ve sunucuları üzerindeki işletim sistemi, veritabanları ve uygulamalar ile güvenlik duvarları, yönlendirici ve anahtarlama cihazları gibi tüm ağ cihazları için sıkılaştırılmış ve test edilmiş güvenli standart konfigürasyon bilgilerini oluşturur. Bu standart konfigürasyon bilgileri bankanın değişiklik yönetimi sürecine entegre edilerek bir değişiklik kontrol yöneticisinin gözetiminde belgelendirilir, gözden geçirilir ve onaylanır. Standart konfigürasyondan sapmalar veya standart konfigürasyondaki güncellemeler değişiklik yönetiminin bir parçası olarak kayıt altına alınır ve onay mekanizmasına tabi tutulur. Bu çerçevede güvenli standart konfigürasyon dışında kalacak her türlü değişiklik isteği için bu değişikliği gerektiren iş gereksinimi ve bu iş gereksinimine ihtiyaç duyan iş sorumlusunun kim olduğu ve gereksinim süresi gibi bilgiler de kayıt altına alınır.

(2) Birinci fıkradaki kontrollere ek olarak, banka kullanmakta olduğu veya ihtiyaç duyabileceği tüm uygulamalar için bir beyaz liste uygular. Böylelikle yalnızca ihtiyaç duyulan uygulamaların sistemlerde yüklü olması ve bu beyaz liste dışındaki herhangi bir uygulamanın sistemlere yüklenmesi veya çalıştırılmasının engellenmesi sağlanır. Banka aynı zamanda, sistemleri üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirir. Beyaz listedeki uygulamaların çalıştırılabilir dosyalarının veya bunların kullandığı kütüphane dosyalarının zararlı yazılımlar yoluyla değiştirilip değiştirilmediği, dosya bütünlük kontrol araçları kullanılarak sürekli bir şekilde kontrol edilir. Zorunlu bir iş gereksinimi olmadıkça ve Bilgi Güvenliği Sorumlusu tarafından onaylanmadıkça banka personelinin ya da dış hizmet sağlayıcıların yerel yönetici haklarına sahip olması engellenir.

(3) Banka, tüm masaüstü, dizüstü, iş istasyonu ve sunucular üzerindeki işletim sistemleri için bu işletim sistemlerinin tipi, versiyon numarası, yama seviyesi ve üzerinde yüklü olan veritabanları ve uygulamaların listesini gösterecek şekilde bir yazılım envanteri tutar. Kullanılacak yazılım envanterinin aynı zamanda donanım envanteri ile de entegre olması ve tek bir noktadan hangi donanım üzerinde hangi yazılımların olduğu bilgisinin takip edilebilir olması sağlanır.

Güvenlik açıkları ve yama yönetimi

MADDE 16- (1) Bankacılık faaliyetlerini kesintiye uğratacak veya önemli ölçüde olumsuz etkileyecek durumların ortaya çıkma olasılığını azaltmak için sistem, yazılım ve cihazlardaki güvenlik açıklarını hızlı ve etkin bir şekilde ele alacak bir yama yönetimi süreci tesis edilir. Yama yönetim süreci kapsamında aşağıdaki faaliyetler yerine getirilir:

a) Uygulanacak yamaların güvenilir bir kaynaktan gelmesini sağlayacak ve bunu doğrulayacak teknikler kullanılması,

b) Banka tarafından kullanılan sistem, yazılım ve cihazlarda yer alan güvenlik açıklarının ve bu açıklara yönelik yamaların tespit edilmesi,

c) Tespit edilen yamaları uygulamanın ya da uygulamamanın etkisinin değerlendirilmesi,

ç) Uygulanacak yamaların uygulama öncesi test edilmesi,

d) Yamaların nasıl uygulanacağına ilişkin metotların tanımlanması,

e) Uygulanan ya da uygulanmamasına karar verilen yamalarla ilgili olarak Bilgi Güvenliği Sorumlusuna düzenli rapor verilmesi,

f) Yamaların yanlış uygulanması ya da uygulanması sırasında sorun çıkması halinde sorunun ne şekilde çözüme kavuşturulacağına dair metotların tanımlanması,

g) Uygulanamayan yamaların gidermeye çalıştığı güvenlik açıklarına ilişkin riskleri azaltmaya yönelik telafi edici kontrollerin tesis edilmesi.

(2) Sağlayıcı veya üretici desteği biten sistem, yazılım ve cihazlar artık yamalanamadığında, bunlar için yüklenebilen en son güncellemelerin günün şartlarına göre artık güvenli olmaması ve telafi edici kontroller ile de makul seviyede bir güvenlik sağlanamaması halinde söz konusu sistem, yazılım ve cihazlar kullanımdan kaldırılır.

(3) Banka, ağa bağlı olan tüm sistem ve cihazlarına yönelik olarak otomatik güvenlik açığı tarama araçları kullanır ve tespit edilen her bir güvenlik açığıyla ilgili olarak Bilgi Güvenliği Sorumlusuna ve açığın tespit edildiği sistemden sorumlu sistem yöneticisine en kritik güvenlik açıklarını öncelikli olarak listeleyecek şekilde raporlama yapılır.

(4) Banka, tüm masaüstü, dizüstü ve iş istasyonu makineleri ile sunucularını, sürekli bir şekilde izleyerek üzerindeki zararlı yazılımları tespit edecek etkin araçlar kullanmakla yükümlüdür. Bankanın tüm masaüstü, dizüstü ve iş istasyonu makineleri ile sunucuları, bu makinelere taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanır. Bunun yanında bu tür harici cihazların makinelere bağlanacağı bağlantı arayüzlerinin ön tanımlı olarak kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan kullanıcılarla sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır.

(5) Banka, e-posta sunucusuna gelen ve giden tüm e-postaları tarayarak zararlı yazılım barındıran ya da bankanın iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren tüm e-postaları engelleyecek çözümler kullanır.

Sızma testleri ve güvenlik tatbikatları

MADDE 17- (1) Banka, bilgi sistemleri aracılığıyla sunduğu hizmetlerin tasarımı, geliştirilmesi, uygulanması veya yürütülmesinde görevi bulunmayan bağımsız ekiplere yılda en az bir defa sızma testi yaptırır.

(2) Banka, bilgi güvenliği organizasyonu ve Kurumsal SOME ekiplerinin etkinliğini test etmek üzere yılda en az bir defa güvenlik tatbikatı gerçekleştirir.

Siber istihbarat paylaşımı ve dolandırıcılıkla mücadele

MADDE 18- (1) Banka, Kurumun belirleyeceği usul ve esaslar çerçevesinde, tespit ettiği ya da haber aldığı yeni siber tehditler, zararlı yazılımlar, siber olaylar ya da bankacılık sektöründe ortaya çıkan yeni dolandırıcılık yöntemleri hakkında bilgilendirmeleri yapmakla yükümlüdür. Dolandırıcılıkla mücadele ve erken müdahaleyi sağlamak amacıyla banka, gerek Kurumun gerekse soruşturma ve kovuşturma makamlarının 7/24 esasına göre irtibat kurabilecekleri ve mevduat hesaplarına bloke koydurmaya yönelik yetkisi bulunan irtibat görevlisi atar ve bu irtibat görevlisinin güncel iletişim bilgileri her yıl ve güncellendikçe Kuruma iletilir.

Fiziksel güvenlik kontrolleri

MADDE 19- (1) Kritik bilgi sistemleri, uygun güvenlik engelleri ve giriş kontrollerine sahip veri merkezleri, sistem odaları, ağ ekipman odaları gibi güvenli alanlarda barındırılır. Bu alanlara erişim, sadece erişim yetkisine sahip olması gereken personelle sınırlandırılır, erişim hakları düzenli olarak gözden geçirilir ve güncellenir.

(2) Bankalar, veri merkezlerinin yerlerini seçerken doğal riskleri ve çevresel tehditleri göz

önünde bulundurur. Binaların, barındırdıkları bilgi işlem tesislerinin varlığını açık edecek işaretler ve bilgiler bulundurmaması sağlanır.

(3) Banka, veri merkezlerinin çalışmasını olumsuz etkileyebilecek elektrik kesintisi, yangın, duman, sıcaklık, su, toz ve nem gibi çevresel koşulları izleyecek sistem ve sensörler kullanır, bunların bakımlarını düzenli olarak yapar. Bu destek sistemi ve sensörlerin ilgili veri merkezlerinin bütünüyle devre dışı kalmalarına neden olabilecek tek bir arıza noktası içermemesi sağlanır.

(4) Veri merkezi personeli dışında kalan herhangi bir banka personeli, ziyaretçi, dış hizmet sağlayıcı ya da yüklenici firma personelinin veri merkezlerine ve kritik bilgi sistemlerine erişimleri onay mekanizmasına tabi tutulur, bunların erişim sonrası faaliyetleri yakından izlenir ve veri merkezindeki çalışmaları boyunca mutlaka kendilerine refakat edilir. Bu çerçevede, veri merkezlerine ve sistem odalarına yapılan erişim talepleri ve onayları ile bu erişimler kapsamında gerçekleştirilen işlemler ve giriş çıkışlar için iz kaydı tutulur. Bu alanlar için kör nokta barındırmayacak ve en az bir yıl süreyle kayıt saklayacak şekilde kamera kayıt sistemleri kullanılır.

Siber güvenlik farkındalığını artırma

MADDE 20- (1) Banka genelinde siber güvenlik farkındalık seviyesini artırmak için kapsamlı bir siber güvenlik farkındalığı eğitim programı oluşturulur. Eğitim programı, bilgi güvenliği politikaları ve standartları ile birlikte, bilgi güvenliği konusundaki bireysel sorumlulukların neler olabileceği ve bilgi varlıklarını korumak için alınması gereken önlemler hakkında bilgi içerir ve bu eğitimler yoluyla bankanın BT kaynaklarına ve sistemlerine erişimi olan herkesin bu kaynakların kullanımı ile ilgili mevzuat ve yönergeler hakkında bilgi sahibi olması sağlanır.

(2) Siber güvenlik farkındalığı eğitim programı Bilgi Güvenliği Komitesi tarafından onaylanır ve programın içeriği yılda en az bir defa yeni teknolojiler ve ortaya çıkan yeni riskler dikkate alınarak gözden geçirilir ve güncellenir. Bankanın BT kaynaklarına ve sistemlerine erişimi olan tüm yeni ve mevcut personelin ve ilgili olduğu alanlar doğrultusunda yükleniciler ile dış hizmet sağlayıcıların bu eğitimlerden geçmesi ve eğitim programı güncellendikçe söz konusu kişilerin güncellenen kısımlarla ilgili tekrar eğitim alması sağlanır.

(3) Banka, siber güvenlik farkındalığını artırmak üzere eğitim programının haricinde aşağıdaki faaliyetlerin de mümkün mertebe yapılmasını sağlar:

a) Siber güvenlik ile ilgili periyodik olarak kurum içi bülten hazırlanması,

b) Banka çalışanlarına periyodik olarak bilgi güvenliğiyle ilgili hatırlatma e-postaları gönderilmesi,

c) Varsa banka iç portalında siber güvenlik ile ilgili bir bölüm oluşturulması,

ç) Çalışanların kişisel işlerinde kullandıkları parolaları, bankanın iş süreçlerinde kullanmamaları gerektiği konusunda bilinçlendirilmesi,

d) Siber güvenlikle ilgili ekran koruyucuların ve arka plan resimlerinin hazırlanması,

e) Bankanın yemekhane, toplantı odaları gibi ortak kullanılan bölgelerine bilgi güvenliğiyle ilgili posterler asılması,

f) Çalışanlara yönelik düzenli olarak siber güvenlik farkındalığını ölçecek anketlerin yapılması

(4) Banka yukarıdaki farkındalık artırıcı çalışmaların etkinliğini doğrulamak ve geliştirilmesi gereken eksiklikleri tespit etmek amacıyla gerekli çalışmaları yapar. Ayrıca, çalışanların şüpheli bir e-postadan bir bağlantıyı tıklayıp tıklamayacağını veya telefonla arayan kişiyi doğrulamak için uygun prosedürleri izlemeden telefonda hassas veriler paylaşıp paylaşmayacağını sınamak gibi gerekli sosyal mühendislik senaryoları üzerinden çalışanlara yönelik periyodik testler gerçekleştirir ve bu testlerden geçemeyen çalışanlara yönelik ilave hedefli eğitimler verilmesini sağlar.

DÖRDÜNCÜ BÖLÜM
Sistem Geliştirme ve Değişiklik Yönetimi

Bilgi mimarisinin tanımlanması

MADDE 21- (1) Banka, bilgi sistemleri yoluyla işlenecek ve saklanacak verilerin bütünlüğünü ve tutarlılığını sağlayacak, veri tekrarını en aza indirecek bir kurumsal bilgi mimarisi modelini esas alır.

(2) Banka, bilgi mimarisi modelinin bir parçası olarak veri söz dizimi kurallarını belirler ve bu söz dizimi kuralları doğrultusunda verilerin uyması gereken standart yapıları tarif eden veri sözlüğünü oluşturarak yazılım geliştirme ve veritabanları yönetimi süreçlerinde bu veri sözlüğünün kullanılmasını sağlar.

(3) Bilgi mimarisi modeli, veri söz dizimi kuralları ve veri sözlüğünün merkezi olarak takibi ve yönetilmesi için ilgili sorumluluklar atanır, uygulamalarda veya veritabanlarında meydana gelecek mimariyi etkileyen değişiklikler için bu sorumluların onayı alınır ve söz konusu değişikliklerin bilgi mimarisi modeline yansıtılarak güncellenmesi sağlanır.

Proje yönetimi

MADDE 22- (1) Banka, yürüteceği tüm BS projelerinin doğru önceliklendirilmesini ve koordinasyonunu sağlamak ve bu projeler yoluyla edinilecek ya da geliştirilecek bilgi sistemlerinin zamanında ve gerekli işlevsellik düzeyine sahip olacak şekilde teslim edilmesini sağlamak üzere bir proje yönetim süreci uygular. Proje yönetim süreci, projelerin büyüklük, karmaşıklık ve riskliliklerine göre uygun bir yönetim yapısı tesis edilmesini sağlar.

(2) Hangi kapsamdaki işlerin proje olarak sınıflandırılacağına ve bunların önceliklendirilmesine ilişkin somut kriterler tanımlanır ve bu kriterler çerçevesinde proje talepleri ele alınarak projelerin işletilmesi ve gözetimi gerçekleştirilir.

(3) Süreç, asgari olarak rol ve sorumlulukların belirlenmesi, zaman ve kaynak planlamasının yapılması, proje kapsamında gerçekleştirilecek faaliyet detaylarının tanımlanması, proje aşama ve çıktılarının tanımlanması, anahtar bağımlılıkların belirlenmesi, kalite temin, risk değerlendirmesi ve onay adımlarını içerir. Bankada, hazırlanan proje planlarında, projenin her aşamasında oluşturulacak çıktılar ve ulaşılması gereken kilometre taşları açıkça belirtilir.

(4) Banka, proje planlarında belirtilen kilometre taşlarına ulaşılmasını ve teslimin zamanında gerçekleştirilmesini sağlamak ve proje risklerini yönetmek üzere, proje ilerleyişini takip eder ve gerektiğinde BS Yönlendirme Komitesine, projelerin gidişatı ve karşılaşılan sorunlara ilişkin bilgilendirme yapılmasını sağlar.

(5) Büyük ve önemli projelerde, risk analizleri sürekli bir şekilde yapılır, risk analiz sonuçlarına uygun önlemler alınır ve iç sistemlerden sorumlu birimlerin ve BS güvenlik fonksiyonunun görüşleri alınır.

(6) Banka, üretim ortamına aktarılacak projelerle ilgili olarak bir eğitim planı hazırlar. Bu planda, eğitim ihtiyaçları, yapılacak eğitimlere ilişkin takvim ve sorumluluklar belirlenir. Eğitim materyalleri ve dokümanlarının eğitim ihtiyacını karşılayacak nitelikte olması ve eğitim sonrası ilgili personelin eğitimlerle ve üretime aktarılan uygulamalarla ilgili görüş ve önerileri alınarak bunların dikkate alınması sağlanır.

Sistem geliştirme, taşıma ve kurulum

MADDE 23- (1) Banka, bilgi sistemlerinin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesinde, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Bu kapsamda sistem ve uygulamaların

geliştirilme süreci, kaynak kodlarının tek bir kişi tarafından hazırlanıp derlenerek geliştirme, test ve üretim ortamları arasında taşınmasına imkân vermeyecek şekilde görevler ayrılığı prensibine uygun olarak işletilir.

(2) Yalnızca geçerli bir iş ihtiyacı ve zorunluluk halinde ve sadece onay mekanizmasından geçmek suretiyle, yazılım geliştirmeden sorumlu personelin üretim ortamına erişimine izin verilebilir. Ancak böyle durumlarda dahi söz konusun personelin üretim ortamında gerçekleştirdiği tüm işlemler takip edilir ve kayıt altına alınır. Banka üretim ortamına erişmede kullanılan tüm yöntemleri kayıt altına alarak yazılı hale getirir ve bunların yönetim kurulu ya da yönetim kurulunun bu yönde yetkisini devrettiği üst düzey yöneticilerce onaylanmasını sağlar.

(3) Bankanın yazılım geliştirme sürecinde, talebin alınması, analiz, tasarım, geliştirme, test, kurulum ve bakım gibi yazılım geliştirme yaşam döngüsünde bulunan aşamalar ve bu aşamalara ilişkin geçiş koşulları, dokümantasyon gereksinimleri ve kodlama standartları yazılı olarak belirlenir ve yazılım geliştirme süreci kapsamındaki işlerin kalitesinden, bankanın yazılım geliştirme yaşam döngüsüne, mevzuat gereksinimleri ile banka içi politikalara ve kodlama standartlarına uyumun sağlanıp sağlanmadığından ve sürecin dokümantasyon gereksinimlerinin takibinden sorumlu olan bir birim tesis edilir. Söz konusu birim dışarıdan tedarik edilen uygulamalar için de kalite güvencesinin sağlanmasından ve bu uygulamaların mevzuat gereksinimleri ile banka içi politikalara ve bankanın kodlama standartlarına uygun olmasının sağlanmasından sorumludur.

(4) Yazılım kalitesini artırmak ve güvenlik açıklarını en aza indirmek amacıyla bilgi güvenliği, yazılım geliştirme yaşam döngüsünün her aşamasında dikkatle ele alınır. Yazılım geliştirme veya tedarik sürecinin başından itibaren, iş gereksinimlerinin ve yazılımdan beklenen fonksiyonel gereksinimlerin neler olduğunun belirlenmesinin yanında, yetkilendirme ve erişim, kimlik doğrulama, veri bütünlüğü, iz kayıtları, istisnai durum yönetimi gibi güvenlikle ilgili gereksinimlerinin neler olduğu da belirlenir ve bankanın güvenlik standartlarına, politikalarına ve mevzuat gerekliliklerine ilişkin uyum durumu kontrol edilir.

(5) Banka içinde geliştirilen veya dışarıdan tedarik edilen internete açık tüm uygulamalar, kurulumları yapılmadan önce ve bu uygulamalarda yapılan güncellemeler sonrası düzenli olarak yinelenen bir temelde, güvenlik açıkları barındırıp barındırmadıkları bakımından taranır.

(6) Tedarikçinin iş dışı kalması durumunda kaynak kodun kullanılabilirliğini sağlamak amacıyla, tüm kritik uygulamalar için kaynak kodun en başından tedarikçiden temin edilmesi sağlanır ya da üçüncü tarafların da katılımıyla bir yazılım emanet sözleşmesi yapılır. Ürün güncellemelerinin ve program düzeltmelerinin de emanet sözleşmesi kapsamında yer alması sağlanır.

(7) Banka, tüm yazılım geliştirme personelinin, kullandıkları yazılım geliştirme ortamları özelinde güvenli kod geliştirme eğitimlerini almasını sağlar.

(8) Yazılım geliştirme yaşam döngüsünün tüm aşamaları boyunca iş birimi ve ilgili diğer paydaşların uygun bir şekilde sürece katılımı sağlanır ve her aşamadan diğerine geçişle ilgili onayları alınır.

(9) Analiz, tasarım ve geliştirme aşamalarında yeni veri tanımı yapılan ya da mevcut veri tanımlarında değişiklik yapan işler bilgi mimarisi ile veri sözlüğü açısından tutarlığı değerlendirilerek gerekli güncellemelerin yapılması sağlanır.

(10) Yazılım kodlarının geliştirme, test ve üretim ortamları arasında taşınması esnasında bunların içine yetkilendirilmemiş ya da zararlı kod parçalarının eklenmesini engellemek üzere versiyonlama ve sürüm kontrollerine dayanan bütünlük kontrolleri gerçekleştirilir, aynı zamanda ortamlar arasındaki geçişlerde ilgili kullanıcı ya da uygulama sahiplerinin onayları alınır.

(11) Test ortamının işletim sistemi, veritabanı yönetim sistemi, entegre olunan uygulamalar ve sistemler itibarıyla üretim ortamını temsil etmesi ve test verilerinin sayı ve

nitelikçe üretim ortamında gerçekleşecek operasyonu temsil etmesi ve hassas verilerden arındırılması sağlanır.

Uygulama kontrolleri

MADDE 24- (1) Bankada geliştirilen ya da dışarıdan tedarik edilen tüm uygulamalar, ilgili oldukları bankacılık faaliyetlerini ve iş süreçlerini banka içi politikalara ve mevzuat gereksinimlerine uygun olarak yürütmek ve bu uygulamalara girilen, bu uygulamalar tarafından değiştirilen, işlenen veya üretilen tüm verilerin doğruluğunu, tamlığını, güvenilirliğini, gizliliğini ve bütünlüğünü sağlamak üzere sistemsel veya manüel kontroller barındırır. Bu kontroller, uygulamaya girdi teşkil edecek verilerin tanımlanması; türü, tipi, formatı ve büyüklüğünün kontrol edilmesi; kaynağının doğrulanması; uygulamanın işlediği verilerin bütünlük ve güvenilirliğinin sağlanması; verilere erişimin görevler ayrılığı prensibine uygun olarak yetkilendirilmesi; gerekli olduğu durumlarda girişçi-onaycı yapısının tesis edilmesi; uygulamanın çıktısı olan verilerin gizliliğinin, bütünlüğünün, mutabakatının ve sadece gerekli taraflara dağıtımının sağlanması gibi fonksiyonları yerine getirir. Banka, söz konusu uygulama kontrollerinin mümkün mertebe sistemsel kontroller olmasına ve manüel yordamlarla yürütülmemesine dikkat eder, uygulamaların kurulumundan önce banka içi politikalara ve mevzuat gereksinimlerine uyduklarından emin olmak için barındırdıkları kontrolleri test eder ve test sonuçlarını kayıt altına alır.

(2) Sermaye yeterliliğinin, riske maruz değerin, risk ağırlıklı varlıkların, takibe dönüşüm oranının, takibe aktarılacak varlıkların yaşlandırmalarının, sigortaya tabi mevduat tutarının, yabancı para bakiyelerinin, yeniden değerlenecek ve piyasa değeri kaydedilecek bilanço kalemlerinin ve genel olarak bilançonun hesaplanması gibi mevzuattan kaynaklanan yükümlülükleri ve finansal tabloları doğrudan etkileyebilecek kritik finansal hesaplamalar ve risk yönetim fonksiyonları, uygun sistemsel uygulamalar vasıtasıyla otomatik olarak gerçekleştirilir ve bunlar için manüel ya da elektronik çizelge uygulamaları gibi yarı otomatik yöntemlerin kullanılmaması sağlanır.

Değişiklik yönetimi

MADDE 25- (1) Banka, meydana gelen değişiklikler sebebiyle gerçekleşebilecek hata ve sorunların sayısını ve etkisini en aza indirecek, değişikliklerin etkili, hızlı ve kontrollü bir şekilde gerçekleştirilmesini ve değişiklikler sırasında yapılan işlemlerin değişiklik sonrasında da denetlenebilir olmasını sağlayacak etkin bir değişiklik yönetimi süreci tesis eder. Bu süreç kapsamında, ağ altyapısı, donanım, işletim sistemleri, yazılım gibi bilgi sistemleri öğeleri ile sistem, servis, uygulama konfigürasyonu ve parametrelerinde yapılacak her türlü değişikliğin bir değişiklik talep yönetimi süreci çerçevesinde başlatılması, değişiklik talebinin geçerli bir iş ihtiyacına dayalı olması, ve görevler ayrılığı prensibine uygun olarak yetkilendirilmesi, test edilmesi, gerçekleştirilmesi, kaydedilmesi ve dokümantasyonu sağlanır. Bu kapsamdaki tüm değişikliklerin kimlik doğrulaması uygun tekniklerle gerçekleştirilmiş yetkili kullanıcılar tarafından yapılması, bunlar için yeterli iz kaydı tutulması ve tutulan iz kayıtlarının düzenli olarak gözden geçirilmesi esastır.

(2) Banka, bilgi sistemi yazılım bileşenlerinin ilk versiyonlarından itibaren kaydını tutar ve bilgi sistemi bileşenlerinde meydana gelen tüm değişiklikleri, meydana geldiği sırayla ve değişimin gerçekleştiği tarihle birlikte kaydederek belgelendirir.

(3) Değişiklik yönetimi süreci, talep yönetimi, risk değerlendirmesi, yetkili merci onayı, yapılan değişikliğin uygulanması, test edilmesi ve doğrulanması gibi adımlar içerir. Bu kapsamda,

a) Değişiklik taleplerinin belgelendirilmesi, sadece yetkili kişilerden gelen değişiklik taleplerinin kabul edilmesi, bunlara ilişkin bir risk ve etki analizi yapılması, gelen taleplerin

sınıflandırılması ve önceliklendirilmesi sağlanır.

b) Uygulanacak değişikliklerin bir güvenlik zafiyetine neden olmadığından emin olmak için, teknik birim ya da BS güvenlik fonksiyonunun yardımıyla, kaynak kod incelemesi de dahil olmak üzere mümkün olduğunca yüksek güvence verecek inceleme faaliyetleri gerçekleştirilir.

c) Uygulanacak değişiklikler uygun test planları doğrultusunda test edilir ve değiştirilen modüllerin üretim ortamına aktarılmasından önce kullanıcı onayları alınır.

ç) Uygulanacak değişiklikler üretim ortamına aktarılmadan önce hem iş birimi hem de teknik birimin onayından geçer ve bu onayların alınması sonrasında değişiklik komitesi gibi uygun bir otorite tarafından da onaylanarak üretim ortamına aktarılır.

d) Değişiklikler ile bağlantılı riskleri en aza indirmek için değişiklikten önce, değişiklikten etkilenecek sistem veya uygulamaların yedekleri alınır, üretim ortamına aktarım sırasında veya sonrasında bir sorunla karşılaşıldığında sistem ya da uygulamaların eski bir versiyonuna dönebilmek için bir geri alma planı oluşturulur.

e) Değişiklikler gerçekleştirildikten sonra, operasyonel prosedürler, konfigürasyon bilgileri, uygulama dokümantasyonu, yardım ekranı ve eğitim materyalleri gibi ilgili sistem ve kullanıcı dokümanları ve prosedürlerinde de değişiklikleri yansıtacak gerekli güncellemeler yapılır.

(4) Acil durum değişiklikleri de kaydedilir ve önceki yazılım sürümleri ve verilerin ulaşılabilir olması bakımından gerekli yedekler alınır. Değişikliklerin doğru olması ve üretim ortamı üzerinde istenmeyen bir etkisinin olmaması için acil durum değişiklikleri bağımsız bir personel tarafından gözden geçirilir, daha sonra normal kabul testleri ve değişiklik yönetimi prosedürleri ile uygun düzeltmeler yapılır, alınamamış kullanıcı ve yetkili birim onayları varsa bu onayların acil durum değişikliklerinin uygulanması sonrası mümkün olan en kısa sürede alınması ve belgelenmesi sağlanır.

BEŞİNCİ BÖLÜM
Bilgi Sistemleri Sürekliliği ve Erişilebilirlik Yönetimi

BT operasyon yönetimi

MADDE 26- (1) Banka, BS servislerinin tanımlanmış hizmet seviyelerine uygun olarak sunulmasını sağlamak üzere BT altyapısının günlük yönetim ve bakımını yerine getiren bir BT operasyon yönetimi fonksiyonu işletir. Bu çerçevede, BS strateji planındaki hedefler ve iş gereksinimleriyle uyumlu olacak şekilde iş birimlerinin de katılımı ve onayıyla bu servislere ilişkin hizmet seviyeleri tanımlanır.

(2) Banka, BT operasyonel olaylarına derhal müdahale etmek, teknoloji ile ilgili tüm sorunlarda kullanıcılara destek sağlamak, araştırılması ve çözümü için sorunları ilgili BT birimlerine aktarmak, rapor edilen sorunların düzeltilmesine kadar tüm olayların kaydını tutmak, analiz etmek ve takip etmek üzere bir yardım masası fonksiyonu ve problem yönetim sistemi tesis eder.

(3) Banka, bilgi sistemlerinin performansının sürekli olarak izlenmesini ve beklenmedik durumların zamanında raporlanmasını sağlamak için bir performans izleme süreci uygular. Performans izleme süreci, sistem performansını etkilemeden önce sorunların tanımlanmasını ve düzeltilmesini sağlayacak bir erken uyarı fonksiyonu içerir, planlanan iş hedefleri doğrultusunda yönelimi belirleyerek kapasite planı için ihtiyaç duyulan bilgileri sağlar ve iş yükü tahminlerinin hazırlanmasına yardımcı olur.

(4) Banka, BS strateji planında belirtilen mevcut ve gelecekteki iş gereksinimlerini tanımlanan hizmet seviyelerine ve iş yükü tahminlerine uygun olarak karşılayabilecek BT

kapasitesinin mevcut olmasını sağlamak üzere kapasite yönetimi ve planlaması yapar. Bu kapsamda banka, kapasite planının sürekli bir şekilde bakımını ve güncellenmesini sağlar ve BS servislerinin performansını, mutabık kalınan hizmet seviyelerindeki performans hedeflerini karşılayacak veya aşacak şekilde yönetir, kapasite ile ilgili olayların ve problemlerin teşhisi ve çözümünü sağlar.

(5) Banka, ay sonu, resmi tatil sonrası, maaş ödemesi yapılan günler gibi müşterilerin yoğun olarak işlem yaptığı günlerde tekrar eden sistem performansı azalması, kapasitenin yetmemesi, teknik arızalarla karşılaşılması gibi sorunların belirli bir desen takip ettiğini tespit edecek yöntemler kullanmakla ve bu sorunların kök nedenlerini tespit ederek çözüme kavuşturulmasını sağlamakla yükümlüdür.

Erişilebilirlik yönetimi ve yedekleme

MADDE 27- (1) Banka, herhangi bir donanım veya yazılım bileşeninin beklendiği gibi çalışmadığı durumlarda, tüm sistemin veya bankacılık faaliyetlerinin önemli bir bölümünün çalışamaz hale gelmesini önlemek adına kritik donanım ve sistemler için yedekli çalışma ya da hazırda bekleme düzenleri kurmakla yükümlüdür. Hangi donanım ve sistemlerin kritik olduğuna, 26 ncı maddede belirtilen BS servisleri ve bunların bağlı olduğu hizmet seviyelerine ve 8 inci maddede belirtilen bilgi varlıklarının erişilebilirlik gereksinimlerine göre karar verilir.

(2) Banka, verilerin erişilebilirliğini sağlamak adına 8 inci maddede belirtilen her bir verinin erişilebilirlik gereksinimlerine uygun yedekleme düzenini tesis etmekle yükümlüdür. Bu kapsamda,

a) 8 inci maddedeki erişilebilirlik gereksinimlerine uygun olacak şekilde her bir sistemin otomatik olarak yedeklenmesi sağlanır.

b) Bir sistemin alınan yedeğinden geri yüklenebilmesi için, işletim sistemi, uygulama yazılımı ve veriler gibi sistemin çalışmasını sağlayan bileşenler yedekleme prosedürüne dahil edilir.

c) Yedeklemenin düzgün bir şekilde çalıştığından emin olmak için, veri geri yükleme işlemleri gerçekleştirerek yedekleme ortamındaki veriler düzenli olarak test edilir.

ç) Yedeklerin saklanırken ya da taşınırken, uygun şifreleme teknikleri ve fiziksel güvenlik kontrolleri yoluyla korunması sağlanır.

(3) Banka, ağ ve iletişim altyapısından kaynaklanabilecek kesintilere karşı uygun alternatif iletişim kanalları oluşturmakla yükümlüdür.

(4) Banka, hangi sistem, sunucu ve veri yedeklerinin, hangi sıklıkta ve hangi yöntemlerle alındığını ve bu yedeklerin hangi ortam ve konumlarda tutulduğunu, güncel durumu yansıtacak şekilde kayıt altına almakla yükümlüdür.

(5) Banka, soruşturma veya kovuşturma yürüten adli merciler ile Kurumdan gelen veri taleplerini alır almaz bu verilerin bir kopyasını alarak yedeklemekle ya da aslını talep yerine getirilene kadar idame ettirmekle yükümlüdür. Banka aynı zamanda söz konusu verileri, talepte bulunan mercilerin kolaylıkla inceleyebileceği bilinen formatlara dönüştürerek tevdi etmekle veya talepte bulunan mercilere bu verilerle birlikte verilerin incelenmesini mümkün kılan uygulama ve araçları temin etmekle de yükümlüdür. Banka, bu fıkra kapsamında kendisine iletilen veri taleplerini geç işleme almasından dolayı mevzuattaki veri saklama sürelerinin geçmiş olduğunu ve bu sebepten verilerin erişilemez olduğunu ileri süremez. Banka bu fıkra kapsamında kendisinden talep edilen verilere ilişkin almış olduğu kopyaları veya ilave yedekleri en az üç yıl süreyle saklar.

Bilgi sistemleri sürekliliğinin sağlanması

MADDE 28– (1) Bankacılık faaliyetlerini yürütmede kullanılan BS servislerinin sürekliliğini sağlamak üzere iş sürekliliği yönetimi ve planının bir parçası olan bilgi sistemleri süreklilik yönetimi süreci ve Yönetim Kurulu onaylı bir bilgi sistemleri süreklilik planı hazırlanır, süreç sorumlusu atanır ve BS Süreklilik Komitesi tesis edilir. BS Süreklilik

Komitesi, bankanın insan kaynakları, hukuk, iş birimleri, BS güvenlik fonksiyonu ve ilgili BS birimlerinin temsilcilerinden oluşur ve bilgi sistemleri süreklilik yönetimi süreci sorumlusu bu komiteye başkanlık eder. BS Süreklilik Komitesi meydana gelen siber olaylarla ilgili bütün faktörleri göz önünde bulundurarak kriz durumu olduğunu ilan etmekle, planın devreye alınmasına karar vermekle ve diğer kurtarma, süreklilik ve müdahale ekipleriyle koordinasyonu sağlamakla yükümlüdür.

(2) Bilgi sistemleri süreklilik yönetimi sürecinin ulusal veya uluslararası bir standart ya da en iyi uygulamaları temel alması esastır. Bu süreç kapsamında banka aşağıdaki faaliyetleri yerine getirir:

a) İş etki analizi, risk değerlendirmesi, risk yönetimi, izleme ve test faaliyetlerini içeren bir bilgi sistemleri süreklilik yönetim süreci tesis etmek,

b) İş birimlerinin de katılımıyla gerçekleştirilen iş etki analizi ve önceliklendirilen iş hedefleri çerçevesinde bilgi sistemleri süreklilik planını geliştirmek ve kurtarma için gerekli olan kritik işlemleri belirlemek,

c) Bilgi sistemleri süreklilik planının uygulanabilir olmasını ve bakımını sağlamak,

ç) Yılda en az bir defa, denetimler ve risk analiz çalışmaları sonucu tespit edilen bulgular ve testlerden öğrenilen derslere göre veya iş süreçlerini ya da bilgi sistemleri sürekliliğini etkileyen değişikliklerden sonra planın gözden geçirilerek güncellenmesini sağlamak,

d) Bilgi sistemleri süreklilik planının ilgili diğer planlarla ve mevzuat gereksinimleriyle uyumlu olmasını sağlamak,

e) Yaşanan acil durum ve felaketlerden kaynaklanan yasal konuları ele almak ve halkla ilişkiler ve basın ile olan iletişimi yürütmek,

f) İlgili ekiplere ve çalışanlara plan kapsamında eğitim verilmesini ve farkındalığın artırılmasını sağlamak.

(3) Planın hazırlanması sürecinde, bilgi varlıklarının ve tutulan verilerin önem düzeyi değerlendirilerek iş etki analizi çerçevesinde her bir BS servisi için kabul edilebilir kesinti süreleri ile kabul edilebilir veri kayıpları belirlenir ve belirlenen bu limitler doğrultusunda servisin tekrar erişime açılabilmesine imkân tanıyacak kurtarma prosedürleri geliştirilir. Banka, felaket durumunun sona ermesi sonrası ikincil merkezden birincil merkeze geri dönüşün sağlanmasına yönelik prosedürleri de hazırlar.

(4) Plan kapsamında ikincil merkez tesis edilir. Veri ve sistem yedeklerinin ikincil merkezde kullanıma hazır bulundurulması sağlanır. İkincil merkezin coğrafi olarak, deprem, yangın, patlama, sel, su baskını, heyelan, elektrik ve iletişim hattı kesintisi gibi sebeplerden kaynaklanacak zararlar açısından birincil merkez ile aynı risklere maruz olmaması esastır. Bankanın, ikincil merkezini birincil merkezi ile aynı veya komşu il sınırları içerisinde tesis etmesi halinde, belirtilen riskler açısından ikincil merkezin birincil merkez ile aynı statüde olmadığını gösteren, akademik kuruluşlarca da onaylanan bilimsel bir rapor hazırlaması şarttır.

(5) Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan tüm personelin, her yıl sorumlulukları ile orantılı bir detay ve içerikte iş sürekliliği eğitimine tabi tutulması ve plan kapsamındaki görev ve sorumlulukları hakkında bilgilendirilmesi zorunludur.

(6) Birincil sistemlerin tamamen devre dışı kaldığı en kötü felaket senaryolarında dahi bankanın en geç yirmi dört saat içerisinde faaliyetlerini yeniden sürdürebiliyor olması esastır. Bu çerçevede planın etkinliğini ve güncelliğini temin etmek üzere yılda en az bir defa gerçek bir felaket senaryosunun simülasyonunu sağlamaya ve birincil merkezi tamamen kapatarak ikincil merkez üzerinden faaliyetleri sürdürmeye yönelik testler yapılır. Testlere varsa dış hizmet sağlayıcılar da dahil edilir, test sonuçları üst yönetime raporlanır ve bu sonuçlara göre plan güncellenir.

(7) Planın yürütülmesinden sorumlu kritik kişiler ile plan kapsamında sorumluluğu bulunan tüm personelin ve dış hizmet sağlayıcıların iletişim bilgilerinin geçerliliği ve bu kişilerin göreve hazır olarak ulaşılabilir olduğu, iletişim zinciri testleri ile yılda en az iki defa

test edilir. Söz konusu iletişim bilgileri ile planın ve ilgili kurtarma veya geri dönüş prosedürlerinin güncel kopyalarının, yalnızca bilmesi gereken kişilerin erişebileceği şekilde sürekli olarak erişime açık tutulması ve gereken konumlarda kopyalarının bulundurulması sağlanır.

(8) Banka, birincil merkezdeki sistem, sunucu, ağ cihazı ve diğer BT bileşenlerinde yapılan güncellemelerin, yama yüklemelerinin ve konfigürasyon değişikliklerinin, söz konusu bileşenlerin ikincil merkezdeki yedeklerinde de aynı şekilde uygulanmasını sağlar, ikincil merkeze kopyalanan veri ve sistem yedeklerinin birincil merkez ile aynı olduğunu garanti edecek bütünlük kontrollerini gerçekleştirir.

(9) Banka, ikincil merkez kapsamına aldığı BS servisleri, sunucu, sistem, uygulama ve verilerin listesi ile ikincil merkez kapsamına almadığı BS servisleri, sunucu, sistem, uygulama ve verilerin listesini güncel durumu yansıtacak şekilde yazılı hale getirir.

(10) Birincil veya ikincil merkez için dış hizmet alınması ya da başka kuruluşlarla paylaşılan bir veri merkezinde barındırılması halinde, veri merkezlerinin bulunduğu konumda veya bölgesel olarak yaşanacak gerçek bir felaket anında birincil ve ikincil merkezdeki çalışma ortamının ve dış hizmet sağlayıcıların bankaya ayıracağı kaynağın, bankanın iş sürekliliğini sağlamayı garanti edecek nitelikte olması esastır.

ALTINCI BÖLÜM
Bilgi Sistemlerine ilişkin Dış Hizmet Alımı

Bilgi sistemlerine ilişkin dış hizmet alımı sürecinin yönetimi

MADDE 29– (1) Banka üst yönetimi, bilgi sistemlerine ilişkin dış hizmet alımlarıyla ilgili olarak alınacak hizmetlerin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve dış hizmet sağlayıcı ile ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak yeterli bir gözetim mekanizması tesis eder. Bu kapsamda;

a) Bilgi sistemlerine ilişkin alınacak dış hizmetin doğuracağı risklerin tüm yönleriyle değerlendirilmesi,

b) Dış hizmet sağlayıcının seçiminde gerekli özenin gösterilmesi,

c) Hizmet alınan tüm dış hizmet sağlayıcılar ile bunların hizmet alanları, iletişim bilgileri ve hizmetlerin sonlanma tarihlerinin yazılı hale getirilmesi,

ç) Dış hizmet alımına konu edilen hizmetlerin erişilebilirliğinin, performansının, kalitesinin, taahhüt edilen hizmet seviyelerine uyulup uyulmadığının, bu hizmetler kapsamında gerçekleşen güvenlik ihlali olaylarının, dış hizmet sağlayıcının gizlilik, bütünlük ve erişilebilirlik ile ilgili güvenlik kontrollerinin, operasyonel ve finansal durumunun yükümlülüklerinin yerine getirmeye uygun olup olmadığının ve sözleşme şartlarına uygunluğunun sürekli bir şekilde takip edilmesi,

d) Dış hizmet alımı kapsamındaki tüm sistem ve süreçlerin bankanın kendi risk yönetimi, güvenlik ve müşteri mahremiyeti politikalarına uygun olması,

e) Dış hizmet alımı kapsamında banka verilerinin dış hizmet sağlayıcıya aktarılmasının gerekli olduğu durumlarda, dış hizmet sağlayıcının güvenlik konusundaki prensip ve uygulamalarının en az bankanın uyguladığı düzeyde olması ve dış hizmet sağlayıcı tarafından sır kapsamındaki verilerin gizliliğinin ve güvenliğinin korunması için gerekli tedbirlerin alınması,

f) Dış hizmet alımı kapsamındaki faaliyetlerin banka bünyesinde gerçekleştirilmesi durumunda hangi denetimlere tabi tutulması öngörülüyorsa, herhangi bir kapsam daraltılmasına gidilmeden dış hizmet sağlayıcının da aynı denetimlere tabi tutulması,

g) Dış hizmet alımına ilişkin hususların banka iş süreklilik planı göz önünde

bulundurularak düzenlenmesi ve gerekli önlemlerin alınması,

ğ) Dış hizmet alımının, planlananın dışında sonlanması veya kesintiye uğraması durumlarına ilişkin risklerin yönetilmesine uygun bir çıkış stratejisinin belirlenmesi

sağlanır.

(2) Dış hizmet alımına ilişkin koşul, kapsam ve her türlü diğer tanımlama, ilgili dış hizmet sağlayıcı tarafından da imzalanmış olacak şekilde sözleşmeye bağlanır. Sözleşme, asgari olarak aşağıdaki hususları içerir;

a) Hizmet seviyelerine ilişkin tanımlamalar,

b) Hizmetin sonlanma koşulları,

c) Bankanın iş sürekliğinin sekteye uğramasını engellemek üzere dış hizmet sağlayıcının alması gereken önlemlere ilişkin hükümler,

ç) Bankanın güvenlik politikası dâhilinde hassasiyet arz eden konulara ilişkin gereklilikler ve gerek hizmet sırasında gerek hizmetin sonlanması halinde dış hizmet sağlayıcının banka ve müşterileri hakkında öğrendiği bilgiler hususunda gizliliğe riayet etmesini sağlayacak hükümler,

d) Dış hizmet sağlayıcı bünyesinde gerçekleşen güvenlik ihlali veya veri sızıntısı gibi olayların derhal bankaya bildirilmesini sağlayacak hükümler,

e) Sözleşmeye konu ürün ve hizmetlerin sahipliği ve fikri mülkiyet haklarına ilişkin hükümler,

f) Sözleşmede dış hizmet sağlayıcı için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler,

g) Dış hizmet alımının, planlananın dışında sonlanmasından veya kesintiye uğramasından kaynaklanacak risklerin yönetilmesine ilişkin hükümler,

ğ) Alınan hizmetin sonlanması halinde, banka ve müşteri verilerinin uygun bir şekilde bankaya teslim edilmesini ve imha edilmesini sağlayacak hükümler,

h) Bankanın tabi olduğu mevzuat hükümlerinin alınan hizmet çerçevesinde dış hizmet sağlayıcılar için de uygulanmasını sağlayacak hükümler,

ı) 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,

i) Banka ile bağımsız denetçisinin, dış hizmet alınan konuyla ilgili olarak dış hizmet sağlayıcıdan her türlü bilgi ve belgeyi talep etme yetkisinin bulunduğuna ilişkin hükümler.

(3) Banka, ikinci fıkra kapsamındaki sözleşmeye dair yükümlülükleri uygulatma imkanının bulunmadığı standart sözleşmeler çerçevesinde yürütülen dış hizmet modelleri ile kritik servis ve hizmetleri edinemez ve kritik iş akışlarını bu tür dış hizmet modelleri yoluyla yürütemez.

(4) Banka, sunmakta olduğu bankacılık hizmetlerine yönelik reklam hizmeti aldığı arama motoru, sosyal medya platformu gibi sağlayıcılarla yapacağı sözleşmelerde, bu sağlayıcıların banka adına verilen sahte reklamları engellemekle ve banka adına yayınladıkları sahte reklamlar dolayısıyla meydana gelen zararları karşılamakla yükümlü olduklarına dair hükümleri ekletmek zorundadır. Aksi takdirde söz konusu hükümlerin eklenmediği sözleşmeler çerçevesinde bahsi geçen sağlayıcılardan reklam hizmeti alınamaz.

(5) Banka, güvenlik politikasının tanımladığı ilkeler doğrultusunda, dış hizmet alımından kaynaklanan riskleri kontrol altında tutmak üzere gerekli organizasyonel değişiklikleri yapar, idari prosedürleri tanımlar ve alınan dış hizmete ilişkin olarak, dış hizmet sağlayıcıyla ilişkileri yürütecek, yeterli bilgi ve tecrübeye sahip bir sorumlu atar.

(6) Dış hizmet sağlayıcıya verilen erişim hakkı tipleri özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır; buna göre, eğer

gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim tipi, erişilen verinin değeri, dış hizmet sağlayıcı tarafından yürütülmekte olan kontroller ve bu erişimin banka bilgilerinin güvenliği üzerindeki etkileri dikkate alınır.

(7) Banka, dış hizmet alımlarında 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 kuruluşa ve kullanıcılarına ait gizli bilgilerin korunmasına yönelik tedbirlerin alınmasını sağlamak bankanın sorumluluğundadır.

(8) Bu Yönetmelik kapsamında belirtilen BS iç kontrol ve iç denetim faaliyetleri dış hizmet alımına konu edilemez ve bankanın kendi personelince ve bankanın kendisi tarafından yerine getirilir.

(9) Bankanın bilgi sistemlerinin bir bütün olarak veya kısmen dış hizmet alımına konu edilebilmesi ancak;

a) Bankacılık mevzuatının gerektirdiği bankacılık faaliyet ve yükümlülükleri bakımından bankanın bilgi sistemleri üzerinde yönetim, içerik, tasarım, erişim, kontrol, denetim, güncelleme, bilgi ve/veya rapor alma gibi konularla alakalı hususlarda herhangi bir sınırlama olmaksızın karar alma gücünün ve hakim rolün bankada bulunması,

b) Dış hizmet alımına konu edilen bilgi sistemleri ile ilgili yönetsel tüm detaylara bankanın vakıf olması,

c) Bankanın veritabanlarına ve verilerine erişim yetkilerinin kritik bilgi olsun olmasın mutlaka bankanın kendi vereceği izinler doğrultusunda gerçekleştirilmesini sağlayacak bir yetkilendirme mekanizması tesis edilmesi ve bankanın kullanmakta olduğu uygulamaların tamamının yetkilendirmesini ve iz kayıtlarının gözden geçirilmesi gibi iç kontrol faaliyetlerini bizzat bankanın kendisinin yapması,

ç) Yazılıma ilişkin fikri mülkiyet hakları saklı olmak üzere, alınan dış hizmet kapsamında oluşan tüm hesap, kayıt ve işlemlere ait her türlü bilgi ve belgenin mülkiyetinin bankaya ait olması,

şartıyla mümkündür.

(10) Kritik bilgi sistemleri ve güvenlik kapsamında alınacak ürün ve hizmetlerin Türkiye'de üretilmesi veya üreticilerinin ar-ge merkezlerinin Türkiye'de bulunması tercih edilmelidir. Ayrıca bu tür sağlayıcıların ve üreticilerin Türkiye'de müdahale ekiplerinin bulunması şarttır. Kurum, bankaların kullanacağı güvenlik ürünleri ve diğer BT unsurları hakkında ilave şartlar belirlemeye yetkilidir.

(11) Bu maddede yer alan diğer hükümler saklı kalmak kaydıyla banka, bir dış hizmet olarak bulut bilişim hizmetlerini de kullanabilir. Ancak birincil veya ikincil sistemler kapsamına giren bir hizmetin bulut bilişim yöntemiyle alınması, bu dış hizmetin sadece bankalara hizmet vermek üzere tesis edilmiş ve bankaların tabi olduğu mevzuat hükümlerine uygun olan bulut hizmet modelleriyle alınması halinde mümkündür. Bu şekilde alınacak bulut hizmeti, tek bir bankaya tahsis edilmiş donanım ve yazılım kaynakları üzerinden özel bulut hizmet modeliyle alınabileceği gibi birden fazla banka arasında donanım ve yazılım kaynaklarının fiziken paylaşıldığı ancak mantıksal olarak her bankaya ayrı kaynaklar atayan ve sadece bankalara hizmet veren topluluk bulutu hizmet modeliyle de alınabilir. Ana bankacılık uygulaması, kredi ve kredi kartı uygulamaları ile ödeme hizmeti gibi faaliyet konularında topluluk bulutu hizmet modeliyle dış hizmet alınabilmesi Kurulun iznine tabidir.

YEDİNCİ BÖLÜM
BS İç Kontrol ve İç Denetim Faaliyetleri

BS iç kontrol ve uyum fonksiyonu

MADDE 30- (1) Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğunu sürekli bir şekilde kontrol etmek üzere bankanın iç kontrol birimi altında bir BS iç kontrol ve uyum fonksiyonu oluşturulur ve hiyerarşik olarak arada başka bir pozisyon bulunmadan iç kontrol birimi yöneticisine doğrudan bağlı olacak şekilde bir BS iç kontrol ve uyum sorumlusu atanır.

(2) BS iç kontrol ve uyum sorumlusunun BS iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya siber güvenlik alanlarının herhangi birinde ya da birkaçında fiilen en az yedi yıllık mesleki tecrübesinin bulunması şarttır. BS iç kontrol fonksiyonunda görev alacak personelin de, söz konusu alanlarda öğrenim durumları itibarıyla veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

(3) BS iç kontrol ve uyum fonksiyonu aşağıdaki faaliyetleri yerine getirir:

a) Kontroller sonucunda belirlenen eksikliklerin giderilmesi ve aksiyon alınması amacıyla ilgili birimlere ve üst yönetime bildirimde bulunulması,

b) Kontroller sonucunda gerekli olduğu anlaşılan süreçsel veya sistemsel iyileştirme önerilerinin ilgili birimlere ve üst yönetime bildirilmesi,

c) Talep halinde bankanın ürünleri ve süreçlerinde planlanan değişiklikler, yenilikler veya banka içi politika, prosedür ve süreç dokümanları hakkında görüş oluşturulması,

ç) Görev alanına giren süreçlerle ilgili proje ve çalışma gruplarına, kurul ve komitelere katılım sağlanması ve ilgili toplantılarda riski en aza indirmeye yönelik öneriler getirilmesi,

d) Bilgi teknolojileri yönetimi ve dış hizmet alımından kaynaklı risklerin sürekli bir şekilde takibinin sağlanmasına yönelik üst yönetim, denetim komitesi ve iç kontrol birimi yöneticisine periyodik olarak raporlama yapılması,

e) Bir sonraki yıl yapılacak planlı incelemeleri gösterecek şekilde her yıl BS iç kontrol inceleme planları oluşturulması ve bunların banka denetim komitesinin onayından geçirilmesi,

(4) BS iç kontrol faaliyetleri kapsamında yapılan periyodik tüm kontroller kayıt altına alınır ve yapılan kontrollere ilişkin çalışma kanıtları saklanır.

BS iç denetim fonksiyonu

MADDE 31- (1) Banka ve bankanın dış hizmet sağlayıcıları nezdindeki BS yönetimine ilişkin faaliyetler, bu faaliyetleri destekleyen süreçler ve tesis edilen BS kontrollerinin mevzuata ve banka içi politika, prosedür ve standartlara uyumlu olduğu ve BS'ye ilişkin iç kontrol ve risk yönetimi faaliyetlerinin etkinliği ve yeterliliği hususunda yönetim kuruluna güvence sağlamak üzere bankanın iç denetim birimi altında bir BS iç denetim fonksiyonu oluşturulur, hiyerarşik olarak arada başka bir pozisyon bulunmadan iç denetim birimi yöneticisine doğrudan bağlı olacak şekilde bir BS iç denetim sorumlusu atanır ve tüm BS iç denetim faaliyetleri bu kişinin sorumluluğunda yürütülür.

(2) BS iç denetim sorumlusunun BS iç kontrol, BS denetimi, BS yönetişimi ve kontrollerinin tesisi veya siber güvenlik alanlarının herhangi birinde ya da birkaçında fiilen en az yedi yıllık mesleki tecrübesinin bulunması şarttır. BS iç denetim fonksiyonunda görev alacak personelin de, söz konusu alanlarda öğrenim durumları itibariyle veya aldıkları sertifikalarla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

(3) BS iç denetimlerinin kapsamının tüm kritik BS servisleri, süreçleri ve kritik varlıkları içerecek ve bunlara ilişkin güvence verecek derinlikte ve detayda olması esastır. Bu çerçevede her yıl, bir sonraki yıl için denetlenebilir BS alanlarından oluşan bir BS denetim planı oluşturularak banka denetim komitesinin onayından geçirilir.

(4) BS iç denetim fonksiyonu tarafından gerçekleştirilecek denetimler, 13/1/2010 tarihli ve 27461 sayılı Resmî Gazete'de yayımlanan Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Banka Bilgi Sistemleri ve Bankacılık Süreçlerinin Denetimi Hakkında Yönetmeliğin, Bilgi Sistemleri ve Bankacılık Süreçleri Denetimine İlişkin Esaslar başlıklı beşinci bölümü ile Bilgi Sistemleri ve Bankacılık Süreçleri Denetimi Metodolojisi başlıklı altıncı bölümünde belirlenen usul ve esaslar çerçevesinde gerçekleştirilir.

(5) Bankanın BS iç denetimlerinin sıklığı ve denetim döngülerinin; BS servislerinin, süreçlerinin ve varlıklarının kritikliği ve riski ile orantılı olması sağlanır. Bu Yönetmelikte yer alan hükümlerin tamamının banka tarafından yerine getirildiği konusunda güvence vermek üzere yapılacak BS iç denetimleri için denetim döngüsü en çok iki yıl olarak belirlenebilir. Tüm kritik BS servisleri, süreçleri ve kritik varlıkları da en çok iki yılda bir BS iç denetimine tabi tutulur.

(6) BS iç denetim fonksiyonu tarafından gerçekleştirilecek BS denetimleri için denetim rehberleri ve kontrol listeleri hazırlanarak yazılı hale getirilir ve günün teknolojisine uygun olacak şekilde düzenli olarak gözden geçirilerek güncellenir. Yapılan denetimlere ilişkin çalışma kanıtları saklanır.

Bulguların takibi ve güvence sağlanması

MADDE 32- (1) Banka denetim komitesi, BS iç kontrol, BS iç denetim ve diğer bilgi sistemleri denetim çalışmaları sonucu tespit edilen bulguların ele alınması konusuna yeterli zaman ayırır, bu çalışmalar sonucu tespit edilen kritik konuları bizzat gözden geçirir ve gerekli önlemlerin alınması konusunda üst yönetime rehberlik eder. Bu çerçevede, banka denetim komitesi üyelerinin kompozisyonu, BS iç kontrol ve BS iç denetim raporlarını ve bulgularını uygun bir şekilde değerlendirebilecek mesleki tecrübe ve bilgi birikimine sahip olacak şekilde oluşturulur.

(2) Banka, BS iç kontrol, BS iç denetim ve diğer bilgi sitemleri denetim çalışmaları sonucu tespit edilen bulguların aksiyon planına bağlanarak takip edilmesini sağlar.

(3) BS iç kontrol ve iç denetim birimi, tespit ettiği bulguların giderilmesine yönelik olarak denetlenen ilgili birim tarafından alınabilecek önlemler ve aksiyonlara yönelik önerilerde bulunur ya da denetlenen ilgili birimin bu yönde almayı planladığı aksiyonlar konusunda mutabık kalır. Uygulaması tamamlanan ve kapatılabilir duruma gelen öneri ve aksiyonlara ilişkin nihai karar, kanıt dokümanlarının, bulgunun sahibi olan BS iç kontrol ya da BS iç denetim fonksiyonu tarafından incelenmesi neticesinde verilir.

(4) Bulguların kapatılmasına yönelik olarak aksiyon planında hedef tamamlanma tarihi atanamayan, aşılan, bir seneyi aşacak şekilde uzatılan veya iptal edilen bulgular denetim komitesine düzenli olarak raporlanır ve bu bulgular denetim komitesinde kritik konular olarak ele alınır.

(5) BS iç kontrol ve iç denetim fonksiyonları tarafından gerçekleştirilen çalışmalar sonucunda, bankanın BS kontrollerinin ve iç kontrollerinin incelenmesi ve bağımsız denetim kuruluşları tarafından gerçekleştirilen çalışmalardan bağımsız olarak bu kontroller hakkında bütün önemli kontrol eksikliklerini ortaya koymak üzere bir değerlendirme yapılması ve bu kapsamda:

a) Bankanın BS kontrollerinde ve iç kontrollerinde, İSEDES Yönetmeliğinin "İç Kontrol Sistemi" başlıklı İkinci Kısmı ile bu Yönetmelikte belirtilen usul ve esaslar açısından etkinlik, yeterlilik veya uyumluluğa engel teşkil edecek herhangi bir önemli kontrol eksikliğinin bulunmadığı,

b) 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 bir durumun ya da yöneticiler ile iç kontrol sisteminde kritik görevleri bulunan diğer görevlilerin dâhil olduğu bir suistimal ya da yolsuzluğun bulunmadığı,

c) Tespit edilen bulgular arasında (a) ve (b) bentleri kapsamına giren hususlar varsa, bunların hepsinin banka denetim komitesine ve yönetim kuruluna raporlandığı

hususlarında güvence sağlanması esastır.

Personelin eğitilmesi ve kaynak tahsisi

MADDE 33- (1) BS iç kontrol ve BS iç denetim faaliyetlerinin layıkıyla yerine getirilmesini sağlamak üzere, yeterli nitelik ve sayıda personel istihdam edilmesi ve söz konusu fonksiyonlara banka tarafından yeterli kaynağın tahsis edilmesi esastır. Bu kapsamda, BS iç kontrol ve iç denetim fonksiyonlarında görev alacak tüm personelin, yılda en az yirmi saat, üç yılda en az yüz yirmi saat olmak üzere BS iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya siber güvenlik alanlarında eğitim almaları sağlanır.

(2) BS iç kontrol ve BS iç denetim faaliyetlerinin karşılıklı iş birliği ve bilgilendirmeye dayalı olarak koordineli bir şekilde yürütülmesi, önemlilik arz eden sistem, süreç ve alanların zamanında ve öncelikli olarak değerlendirilmesini sağlayacak şekilde iç kontrol ve iç denetim faaliyetlerinin planlanması, personel ve iş gücü kaynağının ilgili iç kontrol ve iç denetim görevlerine buna göre atanması esastır.

ÜÇÜNCÜ KISIM
Elektronik Bankacılık Hizmetleri

BİRİNCİ BÖLÜM
Ortak Hükümler

Kimlik doğrulama ve işlem güvenliği

MADDE 34– (1) Bu Yönetmelikte aksi belirtilmedikçe, müşteri bilgilerinin görüntülenmesi gibi finansal sonuç doğurmayan işlemler de dahil olmak üzere tüm elektronik bankacılık hizmetleri için bankaların müşterilerine birbirinden bağımsız en az iki bileşenden oluşan bir kimlik doğrulama mekanizması uygulaması ve bu bileşenlerin kimlik doğrulama sürecinde kullanılmaları esnasında barındırdıkları kimlik doğrulama verilerinin gizliliğini sağlayacak önlemleri alması esastır. Bu iki bileşen; müşterinin "bildiği", "sahip olduğu" veya "biyometrik bir karakteristiği olan" unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Bileşenlerin bağımsız olması, bir bileşenin ele geçirilmesinin diğer bileşenin güvenliğini tehlikeye atmamasını ifade eder. Müşterinin sahip olduğu bileşenin müşteriye özgü olması ve kopyalanıp taklit edilememesi, biyometrik bir kimlik doğrulama bileşeninin kullanıldığı durumlar haricinde bileşenlerden en az birinin tek kullanımlık olması ve bu tek kullanımlık bileşen için gerekli olan en kısa geçerlilik süresinin belirlenmesi esastır.

(2) Kimlik doğrulamada T.C. Kimlik Kartının kart PIN'i ile birlikte kullanılması veya 15/01/2004 tarihli ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde düzenlenen güvenli elektronik imzanın kullanılması hallerinde birinci fıkranın gerekleri yerine getirilmiş sayılır.

(3) Kurum, elektronik bankacılık dağıtım kanalları üzerinden gerçekleştirilebilen işlemler bazında, birinci fıkranın uygulanmasına ilişkin istisna veya ilave güvenlik önlemleri tanımlamaya veya ilave usul ve esaslar belirlemeye yetkilidir. Ancak birinci fıkraya uygun olmayacak şekilde iki bileşenli kimlik doğrulama kullanılmaksızın gerçekleştirilen her türlü işlem için, gerçekleştirilen işlemlerin müşteri tarafından yapıldığını ispat etme yükümlülüğü

bankaya aittir.

(4) Kullanıcılara uygulanacak kimlik doğrulama mekanizmasında kullanılacak parola, tek kullanımlık parola cihazı, şifreleme gizli anahtarı, akıllı kart ve işlem doğrulama kodu gibi bileşenlerin üretim aşamalarından başlayarak kullanıcıya ulaştırılmasına kadar geçen sürecin tamamı boyunca güvenliği sağlanır.

(5) Kimlik doğrulamada kullanılacak şifreleme anahtarları; bu anahtarların ele geçirilme ihtimallerini en aza indiren, gizliliğini sağlayan, değiştirilmesini ve bozulmasını önleyecek yöntemler barındıracak şekilde müşteri kullanımına sunulur.

(6) Banka mobil bankacılık uygulamasını yükleyerek aktifleştirmiş olan müşterilerine, oturum açma ya da oturumun devamında herhangi bir işlemin doğrulanması için hiçbir şekilde SMS OTP gönderemez ve bunu bir kimlik doğrulama unsuru olarak kullanamaz. Mobil bankacılık uygulamasının ilk kurulumu, aktifleştirilmesi ya da yeniden aktifleştirilmesi aşamalarında SMS OTP gönderilmesi bu fıkra hükmüne aykırılık teşkil etmez.

(7) Banka, SIM kart değişikliği gerçekleştirmiş veya numara taşıma yoluyla elektronik haberleşme işletmecisini değiştirmiş müşterilerine, söz konusu değişiklikler müşteri tarafından banka şubesi kanalıyla yüz yüze yapılan görüşme ile veya birinci fıkraya uygun olarak gerçekleştirilecek uzaktan kimlik doğrulama yöntemleriyle teyit edilmediği müddetçe, değişikliğin yapıldığı tarihten itibaren 90 gün boyunca elektronik bankacılık hizmetleri de dahil olmak üzere hiçbir işlem için SMS OTP gönderemez ve ilgili elektronik bankacılık hizmetleri sunulurken SMS OTP söz konusu müşteriler için bir kimlik doğrulama unsuru olarak kullanılamaz. Bu fıkraya göre uzaktan kimlik doğrulama yoluyla alınacak müşteri teyidinde SMS OTP ya da müşterinin SIM kartına dayalı bir bilgi, bir kimlik doğrulama unsuru olarak kullanılamaz.

(8) Altıncı fıkranın uygulanması kapsamında bankanın, müşterilerine SMS OTP göndermeden önce SIM kart değişikliği sorgusunu yapması ve sorgulama fonksiyonunun aktif durumda olmasını sağlamak için kısa mesaj hizmeti veren tüm elektronik haberleşme işletmecileri ile gerekli anlaşmaları yapmış olması, müşterinin elektronik haberleşme işletmecisi değişikliği yapması durumunda müşterinin aktif operatörünün tespit edilmesini müteakip SIM kart değişikliği sorgusunun yinelenmesi, SIM kart değişikliği yapıldığı bilgisinin minimum 90 gün geçmişe dönük tutulması ve bu 90 günlük süre zarfında SIM kart ya da elektronik haberleşme işletmecisinin değiştirilmesi halinde müşteri tarafından değişiklik teyit edilene kadar SMS OTP gönderilmemesi gereken 90 günlük sayacın yeniden başlatılması esastır.

(9) Müşterilere kimlik ya da işlem doğrulama amacıyla kullandırılacak tek kullanımlık parolalar, tahmin edilmesi zor olacak şekilde yeterli uzunlukta harf ve/veya rakamlardan oluşmalı, tahmin edilmesine imkân vermeyecek şekilde rastgele, değişken ve eşsiz olarak üretilmeli ve belirli bir süre için geçerli olmalıdır.

(10) Müşterinin anne kızlık soyadı, T.C. Kimlik No'su, nüfus cüzdanı veya T.C. kimlik kartları üzerinde yer alan bilgiler elektronik bankacılık hizmetlerinin sunulması esnasında hiçbir aşamada kimlik ya da işlem doğrulama amacıyla kullanılamaz. Bankanın kimlik doğrulamada müşterinin bildiği unsur olarak bir güvenlik sorusu kullanmak istemesi durumunda, bu güvenlik sorusunun nüfus cüzdanı veya T.C. kimlik kartları üzerinde yer alan bilgilerden birine ilişkin olmaması ve cevabının müşterinin kendisi tarafından belirleniyor olması gerekir.

(11) Bir kimlik doğrulama bileşeninin bir müşteri ile ilk defa ilişkilendirilmesi uzaktan gerçekleştirilecekse, söz konusu ilişkilendirme güvenli yöntemlerle ve birinci fıkraya uygun olarak en az iki bileşenli kimlik doğrulama gerçekleştirilerek yapılmalıdır. Ancak, 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu kapsamındaki kartlar ve diğer ön ödemeli kartlara ait PIN, ilgili elektronik bankacılık dağıtım kanalının aktifleştirilmesinden ve ilk parolanın alınmasından sonra birinci fıkrada belirtilen "müşterinin bildiği" kimlik doğrulama unsuru

olarak kullanılamaz. Elektronik bankacılık dağıtım kanalının aktifleştirilmesinden ve ilk parolanın alınmasından sonra parolanın unutulması veya yanlış girilmesinden dolayı sıfırlanması gereken hallerde, yeni parolanın uzaktan belirlenmesi için birinci fıkraya uygun olarak en az iki bileşenli kimlik doğrulama gerçekleştirilmesi şartıyla yukarıda belirtilen PIN bilgisi müşterinin bildiği unsur olarak kullanılabilir.

(12) Banka elektronik bankacılık dağıtım kanallarından gerçekleştirilebilecek işlemler için müşterilerine, varsayılan ve müşteri tarafından güncellenebilecek erişim kısıtlamaları, günlük işlem limitleri, güvenli alıcılar listesi gibi ek güvenlik önlemleri sunar. Söz konusu güvenlik önlemlerinin tanımlanması, güncellenmesi veya değiştirilmesinin birinci fıkraya uygun olan bir kimlik doğrulama sonrasında gerçekleştirilmesi esastır. Banka kendi risk değerlendirmesi çerçevesinde söz konusu güvenlik önlemlerinde yapılacak değişiklikler için birinci fıkraya ilave güvenlik önlemleri belirleyebilir.

(13) Banka elektronik bankacılık dağıtım kanallarından sunmakta olduğu herhangi bir işlemin tersinin gerçekleştirilmesi orijinal işleme göre eşit ya da daha az riskliyse, orijinal işlemin tersi olan bu işlemlerin de aynı elektronik dağıtım kanalından gerçekleştirilmesini sağlamak zorundadır.

(14) Bankanın elektronik bankacılık hizmetlerinde kullanmak üzere müşterilerine sunduğu her türlü yazılım ya da mobil uygulamanın kaynağının, ilgili banka olduğunun doğrulanabiliyor olması sağlanır. Banka bu yazılım ya da mobil uygulamaların, müşteri güvenliğini tehlikeye sokacak herhangi bir kod içermemesini sağlamakla, güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri yayınlamakla yükümlüdür. Banka, akıllı telefonlar gibi birden fazla kimlik doğrulama bileşeninin bankaya iletilmesinde kullanılan çok amaçlı mobil cihazların kullanıldığı hallerde, söz konusu cihazlar üzerinde çalışan bankacılık uygulamalarının kullandığı hassas verilerin, hem aynı mobil cihaz üzerindeki diğer uygulamalar ve çalışmakta olan işlemler tarafından erişilemez olmasını hem de bu mobil cihazların kaybolması ya da çalınması halinde bunlar üzerindeki hassas verilerin yetkisiz kişilerce erişilemez olmasını sağlamak amacıyla ve söz konusu cihazların ele geçirilmesi, güvenilirliğinin bozulması, işletim sistemi yazılımının kırılması veya değiştirilmesi gibi hallerden kaynaklanacak risklerin azaltılması amacıyla günün teknolojisine uygun kontroller tesis etmekle ve gerekli önlemleri almakla yükümlüdür.

İnkâr edilemezlik ve sorumluluk atama

MADDE 35– (1) Banka, sunmakta olduğu elektronik bankacılık hizmetleri kapsamında gerçekleştirilen işlemlerde hem banka hem de müşteri için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanır. Kullanılan tekniğin oluşturduğu iz kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte olması sağlanır.

İşlemlerin takibi

MADDE 36- (1) Banka, elektronik bankacılık hizmetleri kapsamında gerçekleşen sıra dışı ve şüpheli işlemleri tespit etmek ve sahtekarlık ya da dolandırıcılık amaçlı işlemleri önlemek için işlem takip mekanizmaları kurar. İşlem takip mekanizması kapsamında asgari olarak aşağıdaki risk unsurları takip edilir:

a) Finansal sonuç doğuran işlemlere yönelik bilinen dolandırıcılık yöntemleri,

b) Gerçekleştirilen her bir bankacılık işleminin tutarı ve bu tutarlara göre müşterinin normal dışı bir ödeme, fon transferi ya da davranış deseni gösterip göstermediği,

c) Müşterinin konum bilgisini de kullanarak normal dışı bir işlem gerçekleştirip gerçekleştirmediği ya da müşterinin ödeme yaptığı veya fon transfer ettiği tarafların riskli bir konumda bulunup bulunmadığı,

ç) Kaybolmuş, çalınmış ya da yetkisiz kişilerce ele geçirilmiş kimlik doğrulama unsurlarının listesi,

d) Her bir kimlik doğrulama oturumuna yönelik olarak zararlı yazılımların bulaşmış

olabileceğini gösteren belirtiler.

(2) Banka, şüpheli veya yüksek riskli işlemleri filtreleyerek değerlendirir ve bu filtrelere takılan müşterileri daha yakından takip eder. Şüpheli ya da yüksek riskli işlemlerin gerçekleştirildiğinin tespit edilmesi halinde banka, telefon ya da kısa mesaj gibi uygun yöntemlerle müşterilerin en kısa sürede uyarılmasını sağlar.

Hizmet kalitesinin sağlanması

MADDE 37- (1) Banka sunmakta olduğu elektronik bankacılık hizmetleri için, her bir dağıtım kanalı bazında, Kurumun belirleyeceği usul ve esaslara göre taahhüt edilen ve gerçekleşen MTBF, MTTR ve süreklilik yüzdesi değerlerini raporlar.

Müşterilerin bilgilendirilmesi

MADDE 38- (1) Banka tarafından sunulan elektronik bankacılık hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir. Buna ek olarak bankanın söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik benimsediği güvenlik prensipleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterinin dikkatine sunulur. Bu çerçevede, bu Yönetmelik kapsamında belirtilen müşterilerin bilgilendirmesine yönelik her türlü bilgi ve açıklama, bankanın gerek kendi internet sitesinde gerek internet bankacılığı hizmetini verdiği internet sitesinde, müşteri erişimine daima açık tutulur ve erişilen bu sitelerin bankaya ait olduğunu gösterecek teknikler kullanılır. Söz konusu bilgi ve açıklamaların açık ve anlaşılır olması sağlanır, verildiği internet sitesinde dikkat çekici bir yere yerleştirilir ve ilgili elektronik bankacılık hizmetinden yararlanmaya başlamadan önce müşterilerin en az bir kere okumasını garanti edecek şekilde yönlendirmeler ve sistemsel kısıtlamalar uygulanır. Hizmetlerden yararlanmaya başladıktan sonra müşterilerin dikkatine sunulması gereken önemli güvenlik uyarıları ve duyurular için de müşterilerin bu uyarı ve duyuruları okumasını sağlayacak teknikler kullanılır.

(2) Birinci fıkra kapsamında, banka kendi internet sitesinde veya internet bankacılığı hizmetini verdiği internet sitesinde:

a) Bankanın kimliği, ticaret unvanı, genel müdürlük adresi, kanuni statüsü, bankanın denetiminden sorumlu olan Bankacılık Düzenleme ve Denetleme Kurumuna ilişkin iletişim bilgileri, mevduatların sigortalanma koşul ve kapsamına,

b) Elektronik bankacılık hizmetlerinin kullanımının taşıdığı riskler, bu risklerden korunmak için müşterilerin kullanması gereken yöntemler, müşteri farkındalığını artıracak yönlendirici güvenlik kılavuzları ile bu hizmetlerden yararlanacak müşterilerin sorumluluk ve haklarına,

c) Bankanın hangi elektronik bankacılık hizmetlerini verdiği, bu hizmetlerin ve bu hizmetler dahilinde gerçekleştirilebilecek bankacılık işlemlerinin hangi gün ve saatlerde erişime açık olduğu ve hizmetlere ilişkin diğer koşullara,

ç) Elektronik bankacılık hizmetlerinde iki saatten daha uzun süreli bir kesinti öngörülen planlı bakım, değişiklik ya da siber olay gibi durumlarda müşterilerin önceden bilgilendirilmesini sağlayacak duyurulara,

d) Hassas verilerin ya da kişisel verilerin sızmasına ya da ifşasına yol açan bir siber olayın yaşanması halinde müşterilerin bilgilendirilmesini sağlayacak duyurulara,

e) Verilen hizmetlerle ilgili olarak müşterilerin herhangi bir sorunla ya da dolandırıcılık vakasıyla karşılaşması durumunda neler yapması gerektiğine ilişkin yönlendirici bilgilere

yer verilir.

(3) Elektronik bankacılık hizmetlerinden dolayı müşterilerin yaşayabileceği sorunları ve şikayetlerini iletebileceği ve takip edebileceği mekanizmalar oluşturulur. Bu kapsamda oluşturulacak şikayet birimleri veya çağrı merkezlerinde müşteriyi karşılayacak menülerde ilgili elektronik bankacılık hizmetine ilişkin yaşanan dolandırıcılık vakalarının iletilmesi

işleminin ana menüde ve ilk sıralarda müşterinin dikkatine sunulması ve bu kapsamda bankaya ulaştırılan bildirimlerin en kısa sürede giderilmesine yönelik gerekli çalışmaların yapılması sağlanır.

(4) Banka tarafından sunulan elektronik bankacılık hizmetlerinde, müşterilerin yanlış işlem yapma ihtimalini en aza indirecek kontrollerin bulunması, müşterilerin başlattıkları işlemlere ilişkin ödemekle yükümlü oldukları her türlü tutar, komisyon ve ücret bilgilerinin işlem anında açıkça müşteri bilgisine sunulması ve müşterinin bunları onaylaması halinde söz konusu işlemlerin gerçekleştirilmesi temin edilir.

(5) Banka, müşteri talebi olmadan herhangi bir elektronik bankacılık hizmetini ilgili müşterinin kullanımına açamaz. Müşteri, herhangi bir elektronik bankacılık hizmetine erişimini kapatmışsa veya kapattırmışsa, müşterinin yeni bir talebi olmadan ilgili hizmet kullanıma açılamaz.

(6) Banka, yapacağı pazarlama faaliyetleri, reklâmlar veya yayınlarda, müşterilerine sunmakta olduğu herhangi bir elektronik bankacılık hizmetinin mutlak manada güvenli olduğu veya bu hizmetlerde hiçbir güvenlik riskinin bulunmadığı izlenimini ve bilgisini verecek ifadeler kullanmaktan kaçınır.

(7) Bankanın sunduğu elektronik bankacılık hizmetleri için bu Yönetmelik kapsamında yapılması gereken bilgilendirmelerin, hizmetin verildiği platformdan ya da müşterinin hizmeti alırken kullandığı cihazdan kaynaklanan nedenlerle bilgilendirme olanakları açısından yetersiz kalması durumunda, müşterinin söz konusu bilgilere farklı kanallar üzerinden ulaşması için gerekli yönlendirmeler yapılır.

(8) Bankanın elektronik ortamda müşterilerine ileteceği hassas veri ve kişisel veri içeren her türlü ekstre, dekont, hesap özeti gibi bilgiler yalnızca güvenli iletişim kanalları üzerinden müşterilere gönderilebilir.

İKİNCİ BÖLÜM
İnternet Bankacılığı

İnternet bankacılığında kimlik doğrulama ve işlem güvenliği

MADDE 39- (1) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek kimlik doğrulama işleminin çevrimdışı olarak lokalde değil banka nezdinde çevrimiçi gerçekleşmesi ve müşterinin bildiği unsurun, mobil bankacılık uygulaması ya da internet tarayıcısı tarafından hatırlanarak veya bu unsurun başka lokal kimlik doğrulama yöntemlerine bağlanarak otomatik olarak gönderilmemesi gerekmektedir. Bu çerçevede, müşterinin bildiği unsurun müşteri tarafından girilmesi zorunlu tutulur ve 34 üncü maddenin ikinci fıkrası hükmü saklı kalmak kaydıyla bu unsur lokalde değil banka nezdinde çevrimiçi doğrulanır.

(2) İnternet bankacılığı dağıtım kanalında kimlik doğrulama işlemi gerçekleştirilirken, müşteri tarafından ilk kimlik doğrulama bileşeni girildikten veya bankaya gönderildikten sonra ve internet bankacılığı oturumu açılmadan önce, müşteri tarafından 34 üncü maddenin birinci fıkrasına göre iki bileşenli bir kimlik doğrulama ile önceden belirlenmiş olan bir karşılama mesajının, müşteriye gösterilmesi sağlanır.

(3) İnternet bankacılığı dağıtım kanalında 34 üncü maddenin birinci fıkrasına göre gerçekleştirilecek her bir kimlik doğrulama işlemi için aynı zamanda, müşteriye atanmış bir şifreleme gizli anahtarı ile imzalanacak şekilde tek kullanımlık bir kimlik doğrulama kodu üretilir. Söz konusu kimlik doğrulama kodu aracılığıyla 34 üncü maddenin birinci fıkrasında belirtilen kimlik doğrulama unsurlarından hiçbiri hakkında bilgi edinilememesi, bilinen bir kimlik doğrulama kodu ile geçerli başka kimlik doğrulama kodlarının türetilememesi, kimlik

doğrulama kodlarının taklit edilememesi sağlanır. Finansal sonuç doğuran işlemler için kimlik doğrulama kodlarının, işlemi gerçekleştirirken müşterinin onayladığı tutar ve alıcı bilgisine göre spesifik olması, tutar veya fonun aktarılacağı alıcı bilgisindeki herhangi bir değişiklik halinde bu bilgilere göre oluşturulmuş ilgili kimlik doğrulama kodunun da geçersiz hale gelmesi temin edilir. Kurumsal internet bankacılığı müşterileri için yığın halinde birden fazla alıcı için toplu işlem gerçekleştirilmesine izin verilen fon transferi gibi işlemlerde, üretilecek kimlik doğrulama kodunun ilgili yığın işlem toplam tutarı ve alıcılar için spesifik olması gerekir.

(4) İnternet bankacılığında müşterinin gerçekleştirdiği finansal sonuç doğuran işlemler için kimlik doğrulama kodunun oluşturulması, iletilmesi ve kullanılması da dahil olmak üzere kimlik doğrulama sürecinin her aşamasında, tutar ve alıcı bilgisi gibi müşteriye gösterilen ve onayına sunulan tüm bilgilerin gizliliği, güvenilirliği ve bütünlüğünü sağlamaya yönelik ve internet bankacılığı oturumu esnasındaki veri iletişiminin yetkisiz kişilere yönlendirilmesi riskine karşı gerekli önlemlerin alınması sağlanır.

(5) Kimlik doğrulama kodunun üretilmesinde hata meydana gelmesi ya da üretilememesi halinde, kimlik doğrulma teşebbüsünde bulunan kişi tarafından söz konusu hatanın hangi kimlik doğrulama unsurundan kaynaklandığının anlaşılamamasını sağlayacak önlemler alınır.

(6) Belirli bir süre içinde gerçekleştirilebilecek hatalı kimlik doğrulama teşebbüslerinin beşi geçmemesi ve belirlenen maksimum deneme sayısı sonrasında ilgili müşterinin internet bankacılığı erişiminin geçici veya kalıcı olarak bloke edilmesi sağlanır. Erişimin kalıcı olarak bloke edilmesi halinde, uygun yöntemler ile müşterinin bu durumdan haberdar edilmesi ve müşteri tarafından blokajın kaldırılmasına yönelik güvenli bir prosedürün işletilmesi esastır.

ÜÇÜNCÜ BÖLÜM
Mobil Bankacılık

Mobil bankacılıkta kimlik doğrulama ve işlem güvenliği

MADDE 40- (1) Mobil bankacılık uygulamasına tanımlanan uygulama PIN'inin şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması halinde, söz konusu uygulama PIN'i çevrimiçi doğrulanan müşterinin bildiği bir kimlik doğrulama bileşeni olarak kabul edilir. Benzer şekilde, müşteriye ait biyometrik bir kimlik doğrulama bileşeninin mobil bankacılık uygulamasında tanımlı bir şifreleme anahtarına erişmek üzere kullanılması ve bu şifreleme anahtarı yoluyla müşteriyle ilintili eşsiz bir bilginin banka nezdinde çevrimiçi olarak doğrulanması ve bu eşsiz bilginin yanında müşterinin bildiği veya sahip olduğu ilave bir unsurun banka nezdinde doğrulanması halinde 34 üncü maddenin birinci fıkrasına uygun olarak iki bileşenli kimlik doğrulama gerekliliği yerine getirilmiş kabul edilir.

(2) Mobil bankacılık uygulamasının yüklü olduğu cihazın ve/veya mobil bankacılık uygulamasının müşteriye bağlanmış olan müşterinin sahip olduğu bir kimlik doğrulama unsuru olarak kullanılması şartıyla ve bu mobil bankacılık uygulamasının yalnızca 37 nci maddenin sekizinci fıkrasında belirtilen güvenli iletişim kanalı amacıyla kullanılması veya müşterinin yalnızca mobil bankacılık uygulaması aracılığıyla müşteri ve hesap bilgilerini görüntülemek istemesi ya da daha önce tanımlanmış güvenli alıcılar listesine para transfer etmek veya ödeme yapmak istemesi halinde ilave bir kimlik doğrulama unsuruna gerek kalmadan tek bileşen ile yapılacak kimlik doğrulama 34 üncü maddenin birinci fıkrasına aykırılık olarak kabul edilmez. Bir müşterinin aynı bankadaki diğer mevduat veya özel cari hesap veya katılma hesaplarının ya da daha önce iki bileşenli bir kimlik doğrulama yoluyla oluşturulmuş tekrar eden aynı tutarlı ödeme veya fon transferi talimatlarının alıcılarının da güvenli alıcılar listesinde olduğu kabul edilir. Müşterinin bu fıkrada belirtilen müşteri ve hesap bilgilerini görüntülemek üzere ilk defa oturum açması halinde ya da 34 üncü maddenin birinci fıkrasına göre iki bileşenle kimlik

doğrulama gerçekleştirerek açtığı son oturumun üzerinden 90 günden daha fazla bir süre geçmiş olması halinde, iki bileşenli kimlik doğrulamaya tabi tutulması esastır.

DÖRDÜNCÜ BÖLÜM
Telefon Bankacılığı

Telefon bankacılığında kimlik doğrulama, işlem güvenliği ve hizmet kalitesi

MADDE 41- (1) Müşteri 34 üncü maddenin birinci fıkrasına uygun olarak bir kimlik doğrulama gerçekleştirmediği müddetçe, telefon bankacılığında hizmet vermek üzere müşteriyi karşılayan müşteri temsilcisinin veya görevli kişinin, müşteriye ilişkin bilgileri görememesi veya müşteriye ilişkin işlem menüsünün aktif olmaması sağlanır. Müşterinin kimlik doğrulaması gerçekleştikten sonra söz konusu müşteri temsilcisi veya görevlinin yalnızca bilmesi gerektiği kadar müşteri bilgisine erişebilmesi ve maskeleme gibi metotlarla müşteri bilgilerinin gizlenmesi sağlanır.

(2) Müşteri için sadece sistem üzerinden bağlantı kurduğu müşteri temsilcisi veya görevli kişi işlem yapar, başka bir kişi işlem yapamaz. Müşteri temsilcisi veya görevli kişi tarafından açılacak oturum telefon bağlantısı kurulmasına bağlıdır. Telefon bağlantısı olmaksızın ya da bağlantının sonlanması halinde müşteriye ilişkin herhangi bir işlem gerçekleştirilemez.

(3) Müşterinin telefon bankacılığı kanalıyla, elektronik bankacılık dağıtım kanallarının herhangi birinde kullandığı kimlik doğrulama veya iletişim bilgilerinde değişiklik gerçekleştirmek istemesi halinde bu değişikliğin müşteri temsilcisi veya görevli kişinin dahli ve erişimi olmadan otomatik sistemler üzerinden gerçekleştirilmesi sağlanır.

(4) Telefon bankacılığı hizmetlerinin verilmesi sırasında kimlik doğrulama gerçekleştirilirken, müşterinin bildiği kimlik doğrulama unsurları ile tek kullanımlık parola veya işlem doğrulama kodu gibi bileşenlerin, müşteri temsilcisi veya görevli kişinin dahli ve erişimi olmadan otomatik sistemler üzerinden girişinin yapılması sağlanır.

(5) Müşterinin bankada kayıtlı olan telefon numarasından aranması gerektiği durumlarda, söz konusu arama gerçekleştirilmeden önce telefonun başka bir numaraya yönlendirilmemiş olduğuna ilişkin kontroller işletilir.

(6) Telefon bankacılığı hizmetlerinin verilmesi sırasında müşterinin gerçekleştirdiği işlemlere ilişkin alınan ses kayıtları için bu Yönetmelikte iz kayıtları hususunda belirtilen hükümler uygulanır. Bu kapsamda alınan ses kayıtlarının güvenilir delillerin elde edilmesini sağlayacak ve sorumluluk atayacak nitelikte ve kalitede olması esastır.

(7) Banka telefon bankacılığı hizmetlerinin müşterilere sunulmasında görev alan müşteri temsilcileri ve çağrı merkezi görevlileri gibi çalışanlara sosyal mühendislik saldırıları ve bilinen diğer dolandırıcılık yöntemleri konusunda periyodik eğitimler aldırmak ve bu çalışanların güvenlik farkındalıklarını artırıcı çalışmalar yapmakla yükümlüdür.

(8) Banka telefon bankacılığı hizmet kalitesini sağlamak adına asgari olarak aşağıdaki kriterleri yerine getirir:

a) Çağrı merkezinde, aynı anda çalışan çağrı merkezi görevlisi ya da müşteri temsilcisi adetlerine uygun bir hat kapasitesi kullanılır ve hat kapasitesinin yetersiz kalması durumunda bunun yeterli seviyeye getirilmesi sağlanır.

b) Sesli yanıt sisteminin ana ve alt menülerinin, reklamlar, duyurular ve bilgilendirmeler dahil, anons sürelerinin altmışar saniyeyi geçmemesi sağlanır.

c) Ses ile yönlendirme sisteminde müşterinin işlemini söylemeye başlaması için anonsu müteakip iki defa on saniye süre verilmesi, akabinde işlemini yapamayan müşterinin ana menüye aktarılması sağlanır.

ç) Ana menüde veya alt menülerde çağrı merkezi görevlisi veya müşteri temsilcisine

bağlanma seçeneği sunulur.

d) Sesli yanıt sisteminin devreye girmesinden veya herhangi bir işlemin gerçekleştirilmesinden itibaren yüz seksen saniye içerisinde ana menüde, alt menülerde işlemlerini tamamlayamayan müşterilere çağrı merkezi görevlisi ya da müşteri temsilcisine bağlanma seçeneği sunulması sağlanır.

e) Çağrı karşılama hedefinin tutturulması için çağrı merkezi görevlisi veya müşteri temsilcisinin müşteri ile görüşme süresinin sınırlandırılması gibi bir uygulamaya yer verilmemesi sağlanır.

BEŞİNCİ BÖLÜM
Açık Bankacılık Servisleri

Açık bankacılık servislerinde kimlik doğrulama ve işlem güvenliği

MADDE 42– (1) Açık bankacılık servisleri bireysel müşterilere verilemez ve bir internet bankacılığı dağıtım kanalı gibi kullanılamaz.

(2) Açık bankacılık servislerinin kullanılması sırasında, müşteri veya müşteri adına hareket eden taraf ile banka arasındaki tüm iletişimin uçtan uca güvenli iletişim şeklinde olması, banka tarafından telafi edici ek kontroller uygulanması ve müşterinin bağlantı kurabileceği kaynaklara ilişkin ilave kısıtlamalar getirilmesi şartıyla tek bileşen ile yapılacak kimlik doğrulama 34 üncü maddenin birinci fıkrasına aykırılık olarak kabul edilmez.

(3) Açık bankacılık servisleri aracılığıyla sunulabilecek hizmetler ve bu hizmetlere ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

ALTINCI BÖLÜM
ATM Bankacılığı

ATM'lerde kimlik doğrulama ve işlem güvenliği

MADDE 43– (1) Banka, ATM cihazları üzerinde kart kopyalama veya dolandırıcılığını önlemek için bilinen suç aygıtları ve tekniklerine karşı gerekli önlemleri almakla yükümlüdür. Bu kapsamda banka asgari olarak aşağıdaki önlemleri alır.

a) Sahte önyüz, sahte klavye, kart sıkıştırma aparatları, kart kopyalama aparatları, nakit sıkıştırma aparatları, mobil kamera gibi kart okuyucu içerisine, para giriş ve çıkış noktalarına veya ATM'nin diğer birimlerine monte edilebilecek tüm yabancı cihazların ATM'ye takılmasını ve mevcut ATM ekipmanlarının ATM'den çıkarılmasını zorlaştırıcı teknikler ile önleyici veya tespit edici kontroller kullanılır.

b) Yapılacak risk analizleri sonucunda belirlenen periyotlarda ATM cihazları yabancı cisimlerin mevcudiyetine karşı fiziksel olarak kontrol edilir. Kart kopyalama ve kart dolandırıcılığına yönelik cihazların monte edilme ihtimalinin yüksek olduğu tespit edilen ATM'ler için söz konusu kontrol periyotları sıklaştırılır.

(2) ATM üzerine herhangi bir kart kopyalama ve dolandırıcılık amaçlı cismin monte edildiğinin veya ATM cihazının kurcalandığının tespit edilmesi, kart kopyalama ve dolandırıcılığı önlemeye yönelik çözümlerin alarm üretmesi veya bu çözümlerin çalışmadığının algılanması durumlarında; ATM'nin güvenlik amacıyla merkezden devre dışı bırakılabilmesi ve fiziksel olarak kontrol edilmeden ya da kamera görüntüleri incelenerek herhangi bir problemin bulunmadığı hususunda güvence sağlanmadan tekrar hizmete açılmaması temin edilir.

(3) ATM cihazları üzerinde ön tanımlı olarak gelen her türlü parola, ATM cihazının bu

ön tanımlı parolalarını bilen kötü niyetli kişiler tarafından yönetilmesini engellemek amacıyla, kolaylıkla tahmin edilemeyecek şekilde değiştirilir.

(4) ATM cihazları üzerine, zararlı içerikli programların kötü niyetli kişilerce yüklenmesini ve yetkisiz erişimi engelleyecek gerekli tedbirler alınır, uygulamaların ve uygulamalara ilişkin kritik servis ve verilerin bütünlüğü periyodik olarak doğrulanır ATM'ler üzerine güvenlik açıklarını gidermek amacıyla otomatik olarak veya düzenli periyotlar ile gerekli güncellemeler ve yamalar yüklenir. Bu çerçevede, ATM'ler üzerinde çalışan işletim sisteminin gerekli olan en az yetki ve ayrıcalıklara sahip olarak çalışacak şekilde ayarlanmış, gerekli güncellemeleri ve yamaları yüklenerek sıkılaştırılmış, stabil ve günün teknolojisine göre güvenli bir işletim sistemi olması sağlanır. ATM'ler, kaynağını ve bütünlüğünü onaylayamadığı uygulama ve kodları işleme almadan siler.

(5) ATM'lere yetkisiz kişilerin herhangi bir şekilde başka bir elektronik cihaz bağlamasını sağlayacak bütün giriş noktaları erişime kapatılır ve ATM cihazı ile banka arasındaki ağ bağlantısına yetkisiz olarak diğer cihazların bağlanmasını engelleyecek ek güvenlik tedbirleri uygulanır.

(6) ATM cihazları üzerinden gerçekleştirilen işlemler için kullanılan iletişim ağının veri güvenliği, gizliliği ve bütünlüğünü sağlayacak özellikte olması sağlanır. ATM üzerinde saklanan, iletilen, işlenen her türlü verinin gizliliği ve bütünlüğü uygun yöntemlerle korunur. PIN bilgisi, parmak izi bilgisi, kart bilgisi gibi kimlik doğrulamaya ilişkin kritik bilgilerin sayısallaştırılarak sisteme girildiği aşamadan itibaren gizlilik ve bütünlüğü sağlanır.

(7) Banka ATM cihazlarının güvenli kullanımı hususunda müşterilerinde farkındalık yaratacak çalışmalarda bulunur.

(8) Banka şubesinde gerçekleştirildiği takdirde yasal kimlik ibrazı zorunlu tutulan işlemlerin ATM'ler üzerinden yapılmak istenmesi durumunda 34 üncü maddenin birinci fıkrasına uygun olarak kimlik doğrulama uygulanır. İşlem tipi, sayısı ve limiti gibi hususlar dikkate alınarak şüpheli işlem gerçekleştirilmesi ihtimaline karşı gerekli kontrol ve takip mekanizması tesis edilir ve gerekli bildirimler yapılır.

(9) Banka, ATM cihazlarının bulunduğu yerlere müşterinin klavye hareketlerini göremeyecek uygun bir açıyla güvenlik kamerası koyar. Güvenlik kamerası kayıtları en az altı ay süreyle saklanır ve kamera kayıtları için aynı zamanda bu Yönetmelikte iz kayıtları için belirtilen hükümler ve 28 nci maddenin dördüncü fıkrası hükmü uygulanır. Kamera kayıtlarındaki görüntünün delil niteliği teşkil etmesi ve görüntü kalitesinin ATM'deki müşterinin ve yakın çevresindekilerin eşkâllerinin belirlenmesini sağlayabilecek nitelikte olması esastır. Bu bakımdan kamera kaydının alınması ve belirtilen süre boyunca saklanması tek başına yeterli olmamakta, ışık kaynakları ve güneş ışığı gibi arka plan ışıklarının çok fazla olması veya yetersiz olması gibi çevresel etkenler ya da konumlandırma hatalarından dolayı şahısların eşkallerinin belirlenmesini ve görüntü kayıtlarının delil teşkil etmesini olumsuz etkileyecek unsurlara karşı gerekli önlemler alınır. Kameraların saatlerinin güncel ve doğru olması aynı zamanda ATM'de gerçekleştirilen işlem referans numarası, dekont numarası gibi parametrelerin zaman bilgisi ile uyumlu olması sağlanır. Kameranın herhangi bir sebeple görüntü kalitesinin düşmesi, görüntü alımının durması, lensinin dış bir etkenle kapatılması veya devre dışı kalması durumunu tespit edip gerekli aksiyonların alınmasını sağlayacak bir yapı kurulur.

(10) Görüntüleme alanı bakımından ATM'yi de kapsayan ve yukarıdaki fıkrada yer alan koşulları karşılayan bir güvenlik kamerası altyapısının varlığı durumunda ATM'ye özel ayrıca bir güvenlik kamerası kurulmasına gerek yoktur. Kamu güvenlik ve istihbarat kurumlarının faaliyet bölgesinde bulunan ATM'ler için güvenlik kamerası kurulma şartı, ilgili kamu güvenlik ve istihbarat kurumlarından izin alınabilmesi koşuluyla yerine getirilir.

DÖRDÜNCÜ KISIM
Çeşitli ve Son Hükümler

BİRİNCİ BÖLÜM
Çeşitli Hükümler

Birincil ve ikincil sistemler

MADDE 44- (1) Bankaların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.

(2) Birincil sistemlerin kaçıncı yedeği olduğuna bakılmaksızın birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilir ve birinci fıkra hükmüne tabidir.

(3) Bankacılık faaliyetlerinin yürütülmesi veya Kanun ve mevzuatta tanımlanan sorumlulukların yerine getirilmesi amacını taşımayan banka içi mesajlaşma sistemleri, piyasa izleme platformları gibi sistemler birincil sistemler kapsamında değildir. Bankanın kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için aynı zamanda söz konusu sistem veya uygulama üzerinden herhangi bir iş sürecinin yürütülmemesi, hassas veri ya da bankacılık sırrı kapsamına girebilecek verilerin işlenmemesi, iletilmemesi ve saklanmaması gereklidir.

(4) İşlemin doğası gereği, bir bacağı yurt dışında olan bankanın, ödeme veya mesajlaşma sistemleri ile etkileşimin gerekli olduğu bankacılık işlemleri hariç olmak üzere, yurt dışında kurulu bir sistemden herhangi bir onay sürecine tabi olmaksızın bütün bankacılık işlemlerini gerçekleştirebilmesi ve yurt dışı iletişim ağlarıyla tüm bağlantılarının kesildiği durumlarda dahi yurt içinde kurulu bulunan birincil ve ikincil sistemleri aracılığıyla ülke içerisinde bankacılık faaliyetlerini sunmaya devam edebilmesi gereklidir.

(5) Birincil veya ikincil sistemler kapsamında olan bir faaliyet için dış hizmet ya da bulut bilişim hizmeti alınması halinde, dış hizmet sağlayıcının söz konusu hizmete ilişkin faaliyetleri yürütmede kullandığı bilgi sistemleri ve bunların yedekleri de birincil ve ikincil sistemler kapsamında ele alınır ve yurt içinde bulundurulur.

Verilerin mahremiyeti

MADDE 45 – (1) Banka, faaliyetlerinin ifası sırasında ve her türlü dış hizmet alımlarında bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerini, yasalarla açıkça yetkili kılınan merciler dışındaki taraflarla, ancak paylaşım sınırları açıkça belirtilmek ve müşterilerin açık rızaları yazılı şekilde veya kalıcı veri saklayıcısı yoluyla kanıtlanabilir bir biçimde alınmak kaydıyla paylaşabilir. Müşterilere bilgilerini söz konusu taraflarla paylaşıp paylaşmama konusunda seçenek sunulur ve müşterinin böyle bir seçeneğinin bulunduğuna dair bilgilenmesi sağlanır. Ayrıca müşterinin bilgilerini paylaşmaya dair rıza göstermesi verilecek hizmet için bir ön şart haline getirilemez.

(2) Birinci fıkra hükmüne uygun olarak müşterinin açık rızası alınsa bile müşteri bilgilerinin yurt dışıyla paylaşılması veya yurt dışına aktarılması Kurulun iznine tabidir. Doğası gereği yurt dışında kurulu banka, ödeme veya mesajlaşma sistemleri ile etkileşimin gerekli olduğu bankacılık işlemleri bu şarta tabi değildir.

(3) Birinci ve ikinci fıkradaki koşullar haricinde herhangi bir müşteri verisi de dahil olmak üzere, sır kapsamındaki her türlü verinin ve trafik bilgisinin yurt dışı ile paylaşılması yasaktır.

Uzaktan kimlik tespiti ve üçüncü tarafa güven

MADDE 46- (1) Banka, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve alt düzenlemelerinde yer alan yükümlülükler saklı kalmak kaydıyla, müşterinin veya müşteri adına hareket eden kişinin kimliğini tespit etmek amacıyla, halihazırda söz konusu

müşteri veya müşteri adına hareket eden kişi için daha önce kimlik tespitinde bulunmuş başka bir bankadan açık bankacılık servisleri aracılığıyla hizmet alabilir. Bu fıkranın uygulanmasına ilişkin usul ve esasları belirlemeye Kurul yetkilidir.

Mesleki tecrübeye ilişkin alanlar ve süreler

MADDE 47- (1) 28/12/2005 tarihli ve 2005/9859 sayılı Bakanlar Kurulu Kararı ile yürürlüğe konulan mülga Bankacılık Düzenleme ve Denetleme Kurumu Teşkilat Yönetmeliği ile 16/03/2014 tarihli ve 28943 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren Bankacılık Düzenleme ve Denetleme Kurumu Teşkilat Yönetmeliğine göre Kurum tarafından ilgili kuruluşlarda bilgi sistemleri yerinde denetimlerini yapmakla görevli daire başkanlığı bünyesinde görev alan Kurum meslek personeli, bu Yönetmelikte geçen mesleki tecrübeye ilişkin alanlarda çalışmış kabul edilir ve söz konusu meslek personelinin ilgili daire başkanlığı bünyesinde çalıştığı süreler, bu Yönetmelikte geçen mesleki tecrübeye ilişkin alanlarda çalışılmış süreler olarak kabul edilir.

İKİNCİ BÖLÜM
Son Hükümler

Geçiş süreci

GEÇİCİ MADDE 1– (1) Banka, mevcut faaliyet ve sistemlerini, 01/01/2020 tarihine kadar bu Yönetmelik hükümlerine uygun hale getirir.

Yürürlükten kaldırılan tebliğ

MADDE 48– (1) 14/06/2007 tarihli ve 26643 sayılı Resmî Gazete'de yayımlanan Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, bu Yönetmeliğin yürürlük tarihinden itibaren yürürlükten kaldırılır.

Yürürlük

MADDE 49– (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 50– (1) Bu Yönetmelik hükümlerini Bankacılık Düzenleme ve Denetleme Kurumu Başkanı yürütür.