İYİ UYGULAMA REHBERİ

Bankacılık Düzenleme ve Denetleme Kurumundan:

OPERASYONEL RİSKİN YÖNETİMİNE İLİŞKİN REHBER

BİRİNCİ KISIM

Amaç ve Kapsam, Tanımlar

Amaç ve Kapsam

1. Bu rehberin amacı, 11.07.2014 tarih ve 29057 sayılı Resmi Gazete'de yayımlanan Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'in "Risk yönetiminin amacı ve risk yönetim sisteminin tesisi" başlıklı 35'inci maddesi çerçevesinde operasyonel riskin yönetimine ilişkin bankalardan beklenen iyi uygulamaları açıklamaktır.
2. Rehber, 19.10.2005 tarih ve 5411 sayılı Bankacılık Kanunu'nun 93'üncü maddesi ve 22.07.2006 tarih ve 26236 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankacılık Düzenleme ve Denetleme Kurumu Tarafından Yapılacak Denetime İlişkin Usul ve Esaslar Hakkında Yönetmelik'in "İyi uygulama rehberleri" başlıklı 7/A maddesine dayanılarak hazırlanmıştır.
3. Etkin ve yeterli bir operasyonel risk yönetiminin bu rehberde yer alan ilkeler doğrultusunda;

    a) Operasyonel risk yönetimi çerçevesinin,
    b) Organizasyon yapısının,
    c) Risk kültürünün,
    d) Strateji, politika ve prosedürlerin,
    e) Operasyonel risk yönetim sürecinin,
    f) İş sürekliliğinin

    banka faaliyetlerinin karmaşıklığı ve büyüklüğü de dikkate alınarak konsolide ve konsolide olmayan yapıya uygun olarak tesis edilmesi beklenmektedir.
4. Bu rehberde yer alan ilkeler, operasyonel risk yönetimi sistemlerinin etkin şekilde tesis edilmesi ve uygulanması amacıyla yol gösterici olarak hazırlanmıştır. Bankalar bu ilkeleri, risk iştahları, risk profilleri ve sermaye yeterlilikleri ile uyumlu olarak dikkate almalıdırlar.
5. Operasyonel risk, geniş bir perspektifte ele alınmalıdır. Bu minvalde bankaların operasyonel risk yönetimi uygulamalarını, banka içi kontrollerdeki aksamalar sonucu hata ve usulsüzlüklerin gözden kaçmasından, banka yönetimi ve personeli tarafından zaman ve koşullara uygun hareket edilmemesinden, banka yönetimindeki hatalardan, bilgi teknolojisi sistemlerindeki hata ve aksamalar ile deprem, yangın, sel gibi felaketlerden kaynaklanabilecek kayıplara kadar oldukça çeşitli faktörleri dikkate alarak geliştirilmeleri beklenmektedir. Ancak yukarıda örnek olarak zikredilen operasyonel risk faktörlerinin tamamen dışında başka faktörlerin de banka veya sektör bazında ortaya çıkabileceği göz önünde bulundurulmalıdır. Bankalar operasyonel risk düzeylerini etkileyen iç ve dış faktörleri sürekli olarak gözden

geçirmelidirler.

Genel sektör uygulamalarında sağlam bir operasyonel risk yönetiminin üçlü savunma hattı yaklaşımı olarak adlandırılan bir metot doğrultusunda teşkil edildiği görülmektedir. Bunlar: (i) Faaliyet kolu yönetimi, (ii) Merkezi operasyonel risk yönetimi fonksiyonu (iii) Bağımsız gözden geçirme.

Bankanın büyüklüğü ve faaliyet yapısı söz konusu üçlü yapının uygulanma düzeyini belirlemektedir. Faaliyet kolu yönetimleri her faaliyet birimi nezdinde bulunan ürün, süreç, faaliyet ve sistemlerden kaynaklanan risklerin tespit edilmesi ve yönetilmesi konusunda sorumluluk üstlenmektedir.

Merkezi operasyonel risk yönetimi fonksiyonu ise faaliyet birimlerinde gerçekleştirilen yönetim sürecinin tamamlayıcısı konumunda olup bağımsızlık düzeyi bankanın büyüklüğüne göre değişmektedir. Küçük bankalarda bağımsızlık; görev ve sorumlulukların ayrıştırılması ile süreç ve fonksiyonların onları icra edenler dışındaki kişiler tarafından gözden geçirilmesi yoluyla sağlanabilir. Büyük bankalarda ise merkezi yapının banka nezdinde bağımsız operasyonel risk yönetim sürecinin teşkili ve geliştirilmesi şeklinde sorumlulukları bulunmaktadır. Bu süreç kapsamında riskin ölçümü, muhtelif banka içi birimlerden raporlar alınması ve risk komitesine ve yönetim kuruluna raporlama yapılması şeklinde yükümlülükler tesis edilir. Bankalarda organizasyon birimi olarak veya faaliyet kolları nezdinde teşkil edilen iç kontrol fonksiyonları da merkezi operasyonel risk yönetiminin önemli bir parçasını oluşturmaktadır.

Üçlü yapının bağımsız gözden geçirme fonksiyonu bu konuda yeterli niteliğe sahip kişiler tarafından banka iç denetim birimi veya banka dışı üçüncü taraflarca yerine getirilebilir.

Basel Komitesinin İleri ölçüm yöntemleri için hazırlamış olduğu Operasyonel Risk-Denetim Rehberinde açıklandığı şekliyle bağımsız gözden geçirme aşağıdaki bileşenleri içermektedir:

Operasyonel Risk Çerçevesinin Yeterliliğine İlişkin Değerlendirme işlemi periyodik biçimde genellikle bankanın iç ve/veya dış denetçileri tarafından gerçekleştirilir. Değerlendirme sürecine banka dışından uygun nitelikleri haiz bağımsız taraflar da katılabilir. Değerlendirme faaliyetinde; genel operasyonel risk çerçevesinin etkinliği ile çerçevenin yönetim kurulu tarafından onaylanan prosedürlerle olan uyum, doğrulama süreçlerinin bağımsızlığı ve bahsi geçen çerçevenin uygulanmasının bankanın mevcut politikaları ile tutarlı bir şekilde yapılıp yapılmadığı tetkik edilir.

Model Doğrulaması, banka tarafından riskin sayısallaştırılması için kullanılan sistemlerin yeterli nitelikte olduğu hususunda güvence verir. Ayrıca doğrulama; mezkûr sistemlerin; girdiler, varsayımlar, süreçler ve çıktılar arasında sağladığı entegrasyonun seviyesi konusunda görüş verir. Bağımsız doğrulama süreci, risk ölçüm sonuçlarının; bankanın operasyonel risk profiline uygun bir sermaye yükümlülüğü hesaplayıp hesaplamadığına dair makul güvence vermelidir. İçsel doğrulamada sayısal hesaplamaya ilişkin

yöntemlerin tetkikinin yanı sıra, veri girişlerinin doğrulaması, operasyonel risk modellerinin metodolojisi ve sistem çıktıları önemlidir.

Güçlü bir risk kültürünün yerleşmiş olması ile söz konusu üçlü savunma fonksiyonu arasında iyi bir iletişim altyapısının kurulması, sağlam bir operasyonel risk yönetimi çerçevesinin en önemli karakteristik özelliğidir.

Tanımlar

6. Bu Rehberde yer alan;

a) Artık risk: Risk azaltımına yönelik olarak gerçekleştirilen risk yönetimi aksiyonlarından ve kontrol uygulamalarından sonra geriye kalan risk düzeyini,

b) İş sürekliliği: Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'in 13 üncü maddesi kapsamında düzenlenen ve bankanın bir kesinti anında faaliyetlerinin sürdürülmesi veya zamanında kurtarılmasını sağlamak üzere operasyonel, finansal, yasal ve itibari olumsuz etkileri en aza indirmeyi amaçlayan uygulamalarını,

c) Kontrol çevresi: Bir bankanın yönetim felsefesi, çalışma tarzı, etik ilkeleri, iç kontrol süreçleri, organizasyon yapısı, politika ve prosedürleri, raporlama yapısı, yetki/onay süreçleri ve görev dağılımı gibi operasyonel risk yönetiminin başarısında etken olan unsur ve uygulamaların tümünü,

ç) Operasyonel risk: Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik'in 3 üncü maddesinde tanımlanan operasyonel riski,

d) Risk iştahı: Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'in 3 üncü maddesinde tanımlanan risk iştahını,

e) Risk kapasitesi: Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'in 3 üncü maddesinde tanımlanan risk kapasitesini,

f) Risk profili: Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'in 3 üncü maddesinde tanımlanan risk profilini,

g) Üst düzey yönetim: Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkında Yönetmelik'in 3 üncü maddesinde tanımlanan üst düzey yönetimi,

ğ) Yasal risk: Yasalara, kurallara uyumsuzluk nedeniyle mahkeme veya karşılıklı anlaşma yoluyla (hakem/tahkim, alacak müzakereleri gibi) sonuçlanan ihtilaflardan yahut bankanın gönüllü eylemlerinden (bir şikayet olmaksızın geri ödemeler veya müşteriye gelecekte sunulacak hizmetlerde indirimler gibi) kaynaklanan gider/zarar riskini,

ifade eder.

İKİNCİ KISIM

Operasyonel Risk Yönetimi Çerçevesi

İlke-1. Her bir bankanın; büyüklüğü, faaliyet yapısı ve finansal ürünlerinin karmaşıklığına uygun kapsam, içerik ve detayda operasyonel risk yönetimi çerçevesi

oluşturması gerekmektedir.

7. Operasyonel risk yönetimi çerçevesi, bankanın maruz kaldığı operasyonel risklerin tutarlı ve kapsamlı bir şekilde tanımlanması, ölçülmesi, değerlendirilmesi, kontrol edilmesi, azaltılması, izlenmesi ve raporlanması süreçlerinin tümünü bünyesinde barındıran üst başlığı ifade etmektedir. Bankalar aşağıda yer verilen ana bileşenleri dikkate alarak operasyonel risk yönetimi çerçevelerini oluştururlar ve bu çerçeveyi hazırlayacakları yazılı dokümanda açıklar.

   - Organizasyon yapısı (yönetim kurulu, üst düzey yönetim, faaliyet kolları, merkezi operasyonel risk yönetimi birimi, iç kontrol ve iç denetim),
   - Bankada yerleşik risk kültürü,
   - Operasyonel risk yönetimi stratejileri, politikaları ve prosedürleri (yazılı iş akış şemaları dâhil olmak üzere) ve
   - Operasyonel risk yönetimi süreci (operasyonel riskin tespit edilmesi, ölçülmesi, değerlendirilmesi, izlenmesi, kontrol edilmesi/azaltılması ve raporlanması süreci).

Operasyonel riskin farklı doğasını yansıtmak üzere, operasyonel riskin 'yönetilmesi' Basel Bankacılık Komitesi tarafından, '**riskin tanımlanması, riskin değerlendirilmesi, riskin izlenmesi ve riskin kontrol edilmesi/azaltılması**' olarak tanımlanmıştır. Bilindiği üzere operasyonel riskin sayısallaştırılması için basitten karmaşığa muhtelif yöntemler bulunmaktadır. Basit yöntemlerde genel kriterlerden (Temel Gösterge Metodunda olduğu gibi) hareketle risk ölçümü yapılmaktadır. İleri yöntemlerde ise teşkil edilecek altyapıya bağlı olarak riskin sayısallaştırılması yapılabilmektedir. Ayrıca bankanın hacminden bağımsız olarak "Skor kart yaklaşımı" başta olmak üzere operasyonel riskin ölçümünde kullanılan muhtelif yaklaşımları ortak bir zeminde ifade etmek üzere "Riskin Sayısallaştırılması/Ölçülmesi" terimi yerine "Riskin Değerlendirilmesi" kavramı kullanılmıştır. Dolayısıyla bu rehberde "Riskin Sayısallaştırılması/Ölçülmesi" ve "Riskin Değerlendirilmesi" kavramları birbirinin yerine ve benzeri anlamları ifade edecek şekilde kullanılmıştır.

ÜÇÜNCÜ KISIM

Organizasyon Yapısı

8. Sağlam bir operasyonel risk yönetimi çerçevesi, farklı alanlardan sorumlu olan muhtelif birimlerin riskin yönetiminde sorumluluk sahibi olmalarını ve tüm personelin görev alanıyla ilgili olarak bankanın maruz kaldığı operasyonel risk düzeyi hakkında bilinçli ve operasyonel riskleri tespit edebilecek yeterliliğe sahip olmalarını (örneğin, mevduat açma işlemlerinden sorumlu personelin ilgili süreçte operasyonel riske yol açabilecek bir hususu tespit etmesi ve bunu bildirmesi) gerektirmektedir. Riskin yönetiminde doğrudan görev alan her bir birimin veya personelin (örneğin, yönetim kurulu veya iç kontrol personeli) yerine getirdiği fonksiyonu ve operasyonel risk yönetimi çerçevesi içindeki yerini iyi anlaması, yetki ve sorumluluklarının farkında olması, hesap verebilirliğinin sağlanması önem arz etmektedir. Banka nezdinde tesis edilecek merkezi bir operasyonel risk yönetimi birimi, yönetim kurulu ve üst düzey yönetimin

sorumluluklarını yerine getirmesine destek olacaktır. Operasyonel risk yönetimi kapsamında görev alması beklenen birimler ve sorumlulukları aşağıda açıklanmıştır.

Yönetim Kurulu

İlke-2. Yönetim kurulu operasyonel risk yönetimi çerçevesinin oluşturulması, onaylanması, düzenli olarak gözden geçirilmesinden sorumludur.

9. Yönetim kurulu; operasyonel risk yönetimine ilişkin banka nezdinde tesis edilen politika, süreç ve sistemlerin tüm karar aşamalarında ve faaliyetlerde etkin bir şekilde uygulanmasına ilişkin gözetimden sorumludur. Örneğin, yeni ürün geliştirme sürecinde üründen kaynaklı ortaya çıkabilecek operasyonel riske ilişkin değerlendirme aşamasının oluşturulması, iç kontrol birimine bağlı personelin görevlerinin icrası sırasında bağımsız hareket edebilmelerinin sağlanması gerekmektedir.

10. Yönetim kurulu banka nezdinde sağlam bir operasyonel risk yönetimi çerçevesinin oluşması amacıyla;

    - Risk kültürünün yerleşmesini sağlayacak tedbirler geliştirmeli, gözetim sorumluluğunu yerine getirebileceği süreçleri oluşturmalı, bankanın strateji ve faaliyetlerinden kaynaklanan riskleri anlamalı ve bankanın tüm risk yönetim sistemine entegre edilmiş kapsamlı dinamik bir kontrol sistemi teşkil etmeli,
    - Üst düzey yönetimi geliştirdiği operasyonel risk yönetimi çerçevesi doğrultusunda somut olarak yönlendirmeli, üst düzey yönetim tarafından hazırlanan prosedür ve politikaların uygunluğunu değerlendirerek onaylamalı ve bunların uygunluğunu belirli aralıklarla gözden geçirmeli,
    - Üst düzey yönetim tarafından politikalara uygun aksiyonların gerekli durumlarda yeterli etkinlikte alınıp alınmadığını kontrol etmeli,
    - Bankanın risk profili ve risk iştahındaki değişimler ile yeni ürün, faaliyet, süreç, sistemler, dış piyasa koşullarındaki dinamikler ve diğer çevresel faktörlerden kaynaklanan operasyonel riski sağlıklı bir şekilde yönettiğinden emin olmak için operasyonel risk yönetim çerçevesini düzenli olarak gözden geçirmeli,
    - Aynı zamanda bağımsız üçüncü taraflarca veya iç denetim tarafından da operasyonel risk yönetimi çerçevesinin gözden geçirilmesini sağlamalıdır.

11. Sağlam bir operasyonel risk yönetimi çerçevesinin oluşturulabilmesinde, banka genelinde operasyonel riskin yönetimine ilişkin görev ve sorumlulukların açıkça tanımlandığı etkin bir kontrol çevresinin (kontrol çevresi; iç kontrol süreçleri, organizasyon yapısı, politika ve prosedürler, raporlama yapısı, yetki/onay süreçleri, etik ilkeler ve görev dağılımı gibi alt unsurlardan oluşmaktadır) tesis edilmesi kritik öneme haiz olup bu husus yönetim kurulunun sorumluluğundadır. Etkin bir kontrol çevresi, merkezi operasyonel risk yönetimi fonksiyonu ile iş kolları ve destek fonksiyonları (iç kontrol ve iç denetim) arasında yeterince ayrıştırılmış, açık ve anlaşılır görev tanımlarının bulunmasını gerektirmektedir.

İlke-3. Yönetim kurulu bankanın operasyonel riske ilişkin genel ve alt unsurlar (faaliyet kolu, ürün, birim vb.) bazında risk iştahı ve kapasitesini, çeşitli eşik değerler, rasyolar ve

limitler bağlamında belirlemeli ve gözden geçirmeli, bu işlevleri yerine getirebilmesi için gerekli sistem ve süreçleri oluşturmalıdır.

12. Yönetim kurulu risk iştahı1 ve kapasitesini belirlerken ve gözden geçirirken; bankanın maruz kaldığı tüm riskleri, riskten kaçınma düzeyini, mevcut finansal koşullarını ve stratejik hedeflerini dikkate almalıdır. Belirlenen genel operasyonel risk iştahı ve kapasitesi, spesifik alt unsurlar için belirlenen risk iştahı ve kapasitesi ile uyumlu ve tutarlı olmalıdır.

13. Yönetim kurulu tesis edilen limit ve eşik değerlere bankanın uyum düzeyini düzenli olarak takip etmelidir. Bu takip süreci, banka dışı çevresel faktörlerin, iş ve faaliyet düzeylerindeki ciddi artışların, kontrol çevresinin kalitesinin, risk yönetim ve azaltım stratejilerindeki etkinliğin, yaşanan operasyonel kayıplar ile limit aşımlarına ilişkin büyüklük ve sıklık düzeylerinin gözden geçirilmesini içermelidir. Diğer taraftan yönetim kurulu belirlenen risk kapasitesindeki aşım düzeylerinin zamanında tespit edilebilmesini sağlamalı ve eş zamanlı düzeltici müdahaleye imkân sağlayacak mekanizmaları kurmalıdır.

14. Yönetim kurulu, operasyonel riskin yönetiminden sorumlu personel ile kredi, piyasa ve diğer risklerin (destek hizmetlerinden kaynaklanan riskler de dâhil) yönetiminden sorumlu personel arasındaki iletişim ve koordinasyonun sağlanmasından ve bu sayede koordinasyonsuzluktan kaynaklanabilecek, bankanın yürüttüğü genel risk yönetimi politikasında oluşabilecek muhtemel sapma ve aşımlardan kaçınılmasından sorumludur.

Üst Düzey Yönetim

İlke-4. Üst düzey yönetim, bankanın risk iştahı ve kapasitesi ile uyumlu olarak tüm faaliyet, iş süreci ve ürünlerde operasyonel risk yönetim çerçevesinin tutarlı ve etkin bir şekilde uygulanmasından ve sürdürülmesinden sorumludur.

15. Üst düzey yönetim, raporlama, takip etme ve uygun görüldüğünde sorunu üst seviyeye taşıma sürecini de içeren etkin sorun çözme süreçleri ve raporlama sistemleri kurmalı ve bu sürecin devamlılığını sağlamalıdır. Bu doğrultuda yönetici bilgi sistemi raporları ile iç veya dış raporlamalara ilişkin yazılan prosedürlerin (dağıtımı ve sıklığı gibi bilgilere yer verilerek) teşkili; raporların doğru ve zamanında, amacına uygun olarak birbiriyle tutarlı, yeterli detayda, ilgili mercilere iletilmesini temin için gerekli tedbirleri almalıdır. Ayrıca operasyonel riske yol açabilecek banka içi suiistimallere ilişkin bilginin ve zayıflıkların kendisine iletilmesini sağlayacak iletişim kanallarını tesis etmelidir.

16. Üst düzey yönetim, yönetim kurulunun ortaya koyduğu operasyonel risk yönetimi çerçevesini, muhtelif faaliyet kolları ve alt birimlerde uygulanabilecek somut politika, prosedür ve süreçlere dönüştürmelidir. Üst düzey yönetim bankada, açık bir yetki-sorumluluk dağılımı ve raporlama hiyerarşisi oluşturmalı ve operasyonel riskin yönetim kurulu tarafından belirlenmiş risk iştahı ve kapasitesine uyumlu olarak yönetilmesini sağlamalıdır.

17. Üst düzey yönetim, banka faaliyetlerinin yeterli deneyim, eğitim ve teknik donanıma sahip olan, gerekli kaynaklara ulaşabilen personel tarafından yürütülmesini sağlamalı ve bu sayede

[1] Bu rehberde "Risk İştahı" kavramı uluslararası literatürde yer verilen "Risk Toleransı" kavramını da ifade edecek şekilde kullanılmıştır.

bankanın personel hatalarından kaynaklı olarak maruz kalacağı potansiyel operasyonel risk düzeyini düşürmelidir.

18. Bankanın muhtelif faaliyetlerinin fiyatlama ve performans ölçümünde operasyonel risk faktörünün uygun biçimde dikkate alınmasının sağlanması üst düzey yönetimin sorumluluğundadır. Zira operasyonel riskin mezkûr kapsamda dikkate alınmaması, bankanın risk iştahı ve kapasitesi ile uyumsuz düzeyde risk almasına neden olabilir.

19. Bilanço kalemlerine ilişkin değerleme uygulamalarında ve risk ölçümü öncesi yapılan değerlemeler hakkında benimsenen yaklaşım, metot ve varsayımların (örneğin, menkul kıymetlerin değerlemesinde hangi verim eğrisinin kullanıldığı) üst düzey yönetim tarafından hazırlanacak bir prosedür kapsamında yazılı hale getirilmesi ve hazırlanan metnin yönetim kuruluna onaylatılması esastır.

Merkezi Operasyonel Risk Yönetimi Fonksiyonu

20. Bankalar tarafından kredi riski ve piyasa riskine benzer şekilde operasyonel riskin yönetiminin bağımsız ve merkezi bir organizasyon tarafından icrası, yaygın bir uygulama haline gelmiştir. Bu organizasyonun temel sorumluluğu, maruz kalınan operasyonel risklerin anlaşılması ve yönetilmesi kapsamında üst düzey yönetime ve risk yönetimi faaliyetlerinin izlenmesi kapsamında yönetim kuruluna yardımcı olmaktır.

21. Her bir banka, kurumsal yapısı, büyüklüğü, karmaşıklığı, risk profili ve faaliyet yapısı ile uyumlu olarak operasyonel riskini yönetebileceği merkezi bir yapı teşkil etmelidir. Bu kapsamda bankaların operasyonel risk yönetimini, özel bir komite, birim veya personel vasıtasıyla icra etmesi mümkündür.

22. Aşağıda ana hatlarıyla açıklanan görevler, bu organizasyon tarafından yerine getirilecektir.

- Konsolide ve konsolide olmayan düzeyde operasyonel risk yönetimi ve kontrolleriyle ilgili politika ve prosedürlerin oluşturulmasında üst düzey yönetime yardımcı olmak,
- Operasyonel risk yönetimi politikalarının, süreçlerinin ve prosedürlerinin banka genelinde tutarlı bir şekilde uygulanmasına yönelik izleme yaparak yönetim kuruluna sunulmak üzere konsolide ve konsolide olmayan bazda raporlar hazırlamak,
- Bankanın konsolide ve konsolide olmayan bazda maruz kaldığı operasyonel risk düzeyine ilişkin ölçümler ve değerlendirmeler yaparak üst düzey yönetimi bilgilendirmek,
- Bankanın operasyonel risk ölçüm ve değerlendirme araçları ile risk raporlama sistemlerini tasarlayarak uygulamaya koymak,
- Bankaca yürütülen genel risk yönetimi faaliyetleriyle operasyonel risk yönetimi uygulamaları arasında koordinasyonu sağlamak,
- Operasyonel risk yönetimi eğitimleri düzenlemek ve faaliyet birimlerine maruz kaldıkları operasyonel riskin yönetimi kapsamında danışmanlık yapmak (örneğin, operasyonel risk yönetimi araçlarının faaliyet birimleri nezdinde kullanımını sağlamak),
- Banka nezdinde denetim gerçekleştiren iç ve dış organizasyonlarla düzenli bilgi alışverişi gerçekleştirmek.

Faaliyet Kolları

23. Operasyonel risk yönetiminde benimsenen üçlü savunma yaklaşımının ilk aşaması faaliyet kolları nezdindeki uygulamalarla başlamaktadır. Bu aşamada her bir faaliyet kolu yönetimi, uhdesinde kullanılan süreç, faaliyet ve sistemlerden kaynaklanan operasyonel risklerin tespit edilmesi, üst düzey yönetimin bilgilendirilmesi ve uygun aksiyonların alınmasını sağlama konularında sorumluluk sahibidir.

24. Faaliyet kolu yöneticileri, kendilerine bağlı birimlerin, operasyonel riske yönelik üst düzey yönetim tarafından belirlenen politika, prosedür ve iş akış süreçlerine uyumlu faaliyet göstermelerini sağlamakla ve gerektiği ölçüde alt düzey ilave politika ve prosedürleri oluşturmakla sorumludurlar.

İç Kontrol

25. Operasyonel risk yönetimine ilişkin iyi uygulamalar arasında her bir faaliyet kolunda riskin yönetiminde özel olarak sürekli görev yapan, icrai birimden bağımsız personel istihdam edilmesi bulunmaktadır. Bu personel genellikle çift taraflı raporlama yükümlülüğünü taşımaktadır. Diğer bir ifadeyle bulundukları iş birimiyle doğrudan raporlama ilişkisine sahip olmakla birlikte aynı zamanda kontrol sonuçlarını ve tespit edilen sorunları merkezi iç kontrol birimine ve risk yönetimi birimine de iletebilmektedirler. Böylelikle uygulanan politikalar ve kullanılan araçlar arasında tutarlılığın sağlanması mümkün olmakta ve özellikle iç kontrol biriminin icracı birimlerden bağımsızlığı sağlanmaktadır. Söz konusu personelin sorumlulukları arasında, görevli olduğu faaliyet koluna ilişkin risk göstergelerinin geliştirilmesi, tetikleyici seviyelerin belirlenmesi ve yönetim kurulu ile üst düzey yönetime yapılacak raporların hazırlanması da bulunabilir. Öngörülen çalışma modelinde yeterli etkinliğin sağlanması adına faaliyet kollarında görevli personele sorumluluklarını yerine getirebilecek yeterli kaynak ve yetki verilmelidir.

Operasyonel Risk ile İlgili Diğer Fonksiyonlar

26. Yukarıda belirtilen kişi/birimlerin yanı sıra bankaların genel operasyonel risk düzeyine doğrudan ve/veya dolaylı etki edebilecek faktörlere ilişkin sorumluluk taşıyan faaliyet birimleri de bulunmaktadır. Bunlar, mevzuat-uyum, insan kaynakları, bilgi teknolojileri ve muhasebe/finansal raporlama gibi operasyonel riskin muhtelif boyutlarıyla ilgili olanlar veya riske dolaylı olarak yol açan alanlarda sorumluluk taşıyan birimlerdir. Bahse konu birimler bir taraftan kendi faaliyet alanlarındaki operasyonel riskin yönetiminden mesul iken diğer taraftan uygun ve gerekli olduğu ölçüde diğer birimlere maruz kaldıkları operasyonel risk türleri, düzeyi ve yönetimi hakkında bilgi ve destek sağlarlar. Örneğin, kredi tahsis sürecinde işlemin muhasebeleştirilmesinden sorumlu personel tarafından gerçekleştirilen hatalı muhasebe işleminin yol açtığı operasyonel riskin tespit edilmesinde, bankanın muhasebe birimi sorumluluk sahibi olabilir.

İç Denetimin Rolü

27. İç denetim, banka nezdinde uygulanan operasyonel risk yönetimi çerçevesinin tüm yönleriyle, bağımsız olarak değerlendirilmesinden sorumludur.

28. İç denetim birimleri operasyonel risk yönetimi politika ve prosedürlerinin banka genelinde etkin bir şekilde uygulanıp uygulanmadığını ortaya koyabilmek için yeterli bir yerinde denetim yapısına ve kaynağına sahip olmalıdır. Yönetim kurulu da bu çerçevede iç denetim birimi tarafından tasarlanan denetim programının kapsamının ve sıklığının bankanın maruz kaldığı operasyonel risk düzeyine uygun olmasını sağlamakla sorumludur. Denetim sürecinde tanımlanan ve raporlanan her bir operasyonel risk konusu bankanın üst düzey yönetimi tarafından zamanında ve etkili bir şekilde ele alınmalı ve uygun olduğu ölçüde yönetim kurulunun dikkatine sunulmalıdır.

DÖRDÜNCÜ KISIM

Risk Kültürü

İlke-5. Bankalar teşkil ettikleri operasyonel risk yönetimi çerçevesi vasıtasıyla banka genelinde yerleşik bir risk kültürünün oluşmasını sağlamalıdır. Yönetim kurulu ve üst düzey yönetim, bu yükümlülüğün yerine getirilmesinde öncü rol üstlenmeli, mezkûr amaca yönelik olarak bankanın taşıdığı operasyonel riskin temel unsurlarının farkında olmalı ve bu riski yönetilmesi gereken ayrı bir risk kategorisi olarak görmelidirler.

29. Bu kapsamda belirlenecek politikalar, süreçler ve sistemler, verilecek meslek içi eğitimler, oluşturulacak etkin iç kontrol mekanizmaları bankada risk yönetimi bakış açısına sahip güçlü bir kurumsal kültürün tesis edilmesini, tüm birim ve faaliyetlere operasyonel risk yönetim kültürünün entegre edilmesini sağlayacaktır. Nitekim risk yönetim kültürünün yerleşik olduğu bir bankada, potansiyel aksaklıkların daha az yaşanması veya ortaya çıktıklarında bu aksaklıklara karşı daha etkin müdahale edilmesi imkânı bulunacaktır.

30. Yönetim kurulu tarafından bir bankada davranış ve mesleki ahlak kuralları ile ücretlendirme politikalarının belirlenmesi önem arz etmektedir. Bu kurallar personelden beklenen sorumlulukların net bir biçimde ortaya konulmasını sağlayarak gerekli durumlarda bu sorumluluklara ilişkin hesap verilebilir bir iş ortamı oluşturacak, diğer taraftan muhtemel çıkar çatışmalarını önleyecektir. Üst düzey yönetimin mezkûr kurallara güçlü ve tutarlı bir şekilde destek vermesi, düzenlemelerden beklenen faydanın elde edilmesinde kritik öneme haizdir. Banka nezdinde uygulanan ücretlendirme süreci; bankanın risk iştahı, risk kapasitesi, finansal hedefleri ve uzun vadeli stratejileri ile uyumlu olmalı, özellikle risk-ödül dengesi iyi kurulmalıdır.

31. Banka nezdindeki kritik faaliyetlerin, risk yönetimi ve kontrol uygulamalarının yeterli teknik özelliğe sahip, deneyimli personel tarafından yerine getirilmesi ve bu personelin gerekli kaynaklara rahatça ulaşabilir kılınması, risk kültürünün yerleşmesinde önemli bir aşamayı oluşturmaktadır.

32. Üst düzey yönetim ayrıca banka içerisinde farklı hiyerarşik seviyelerde çalışan tüm personelin asgari bir operasyonel risk eğitimi almasını sağlamalıdır. Personele verilecek eğitimler belirlenirken ilgili personele ilişkin öncelikler ile personelin görev ve sorumlulukları dikkate alınmalıdır.

33. Banka içerisinde personelin, operasyonel riske ilişkin problemleri rahatça ve negatif tepkilerden kaynaklanabilecek tedirginlik yaşamadan ifade edebileceği bir iletişim kanalı oluşturulmalıdır.

34. Operasyonel riske ilişkin politika ve prosedürlerin ilgili banka personeline duyurulması amacıyla banka bilgi işlem sisteminde veya intranet portalında gerekli altyapı kurulmalı ve sürekli olarak ilgili personelin kullanımına açık tutulmalıdır

BEŞİNCİ KISIM

Strateji, Politika ve Prosedürler

35. Bir bankada risk yönetimi süreci, bankanın genel stratejilerini ve uzun vadeli hedeflerini belirlemesiyle başlar. Zira strateji ve hedefler belirlendikten sonra maruz kalınacak riskler ve bu risklere yönelik izlenecek stratejiler ortaya konabilecektir. Operasyonel risk de bu süreçten vareste değildir. Dolayısıyla bankanın genel strateji ve hedeflerini oluşturduktan sonra operasyonel riske yönelik izleyecekleri stratejileri ve tüm bu stratejilere uygun bir operasyonel risk yönetimi çerçevesini geliştirmeleri önem arz etmektedir. Ayrıca bankanın risk iştahı ve bu iştahın nasıl yönetileceğine ilişkin temel unsurlar operasyonel risk yönetim çerçevesi içerisinde yazılı bir şekilde belirlenmiş olmalıdır.

36. Banka içerisindeki her bir faaliyet kolunun yöneticileri, kendi alanındaki faaliyetlerden kaynaklanan risklerin yönetiminde ilk aşamadaki sorumlulardır. Bundan dolayı, her bir faaliyet kolunun[2] kendi alanına özgü ve bankanın operasyonel risk çerçevesiyle uyumlu olan ilave politika ve prosedürleri oluşturması beklenmektedir. Prosedürler bünyesinde yazılı iş akış şemalarının oluşturulması büyük bir öneme sahiptir. Söz konusu şemaların biçim ve içeriği konusunda standart bir format bulunmamakla birlikte, okuyucular tarafından kolayca anlaşılabilmesini sağlayacak detay ve üslupta hazırlanması gerekmektedir.

Bir bankanın genel stratejisi ile operasyonel riske yönelik strateji, politika ve prosedürlerinin belirlenmesine ilişkin bir örneğe aşağıda yer verilmiştir.

Yönetim kurulu tarafından bankanın genel stratejisi 3 yıllık perspektifte her yıl aktifin %20 büyümesi şeklinde belirlenmiştir. Yapılan hesaplamaya göre banka bu hedefe ulaşma sürecinde yıllık ortalama %13'lük bir SYSR'ye sahip olacaktır. Dolayısıyla bankanın risk iştahı minimum %13'lük bir SYSR seviyesine denk gelmektedir. Yönetim kurulu aynı zamanda operasyonel risk için bulundurulması gereken sermaye yükümlülüğünün, toplam yükümlülüğün %15'ini aşmamasına da karar vermiş ve bunun için genel müdürlüğe talimat vermiştir (buraya kadar anlatılanlar tipik bir genel strateji ve operasyonel riske yönelik strateji oluşturma süreci örneğidir).

Genel müdürlük belirlenen stratejiye uygun olarak, operasyonel risk tespit edilen seviyeyi geçmemesi için riske yönelik politikalar geliştirmiş ve bu politikalar arasında örneğin kredi kartı tahsis sürecinde müşterinin kredibilitesinin yanlış

[2] Kurumsal finansman, perakende bankacılık vs. gibi ana faaliyet kolları kastedilmektedir.

değerlendirilmesinden kaynaklanabilecek maddi kayıplar için sigorta yapmaya karar vermiştir (bankanın ileri ölçüm yöntemine göre sermaye gereksinimi hesapladığı varsayılmıştır).

Oluşturulan strateji ve politikalara uygun olarak ilgili genel müdür yardımcısı tarafından teşkil edilen kredi kartı tahsis prosedüründe, bankanın her bir kredi kartı tahsis işlemi için x, y veya z şirketlerinden herhangi birinden sigorta hizmeti alınması yönünde talimat bulunmaktadır (x, y ve z sigorta şirketlerinin, bankanın satın alma sorumlusu birim tarafından yapılan değerlendirme ve imzalanan sözleşmelere göre daha önceden belirlendiği varsayılmıştır).

37. Operasyonel risk yönetimi çerçevesi altında oluşturulan politika ve prosedürlerde asgari olarak aşağıdaki unsurlara yer verilmelidir.
    - Yaşanan veya yaşanması muhtemel iç ve dış olaylardan hareketle bankaya özgü operasyonel risk tipleri (riskin tanımlanmasında, derecelendirilmesinde ve risk yönetimi amaçlarına ulaşmada tutarlılığı sağlamak üzere operasyonel risk terimleri için ortak bir sınıflandırma ve tanımlama sistematiği geliştirilmelidir. Zira bankanın maruz kaldığı operasyonel risk ve kayıp tiplerini yeterli kapsam ve içerikte somut olarak tanımlayamaması ve sınıflandıramaması, riskin sayısallaştırılmasını ve yönetilmesini engelleyecek temel bir unsurdur.),
    - Operasyonel riskin bileşenlerinden olan; yeni müşteri, ürün ve bilgi yönetimi sistemlerinin onaylanması, destek hizmeti kullanımı, iş sürekliliği planları, kriz yönetimi ve kara para aklama gibi konulara yönelik kurallar,
    - Riskin yönetimi kapsamında uygulanan raporlama sürecinin ve ilgili taraflara düşen sorumlulukların açıkça belirlendiği organizasyon yapısı (örneğin, rapor kontrolü yapacak yetkililer, imza ve gönderim prosedürlerinin belirlenmiş olması, bu kapsamda değerlendirilecektir),
    - Riskin ölçümü ve değerlendirilmesi için kullanılan yöntemler ve bu yöntemlerin nasıl kullanıldıkları,
    - Bankanın strateji dokümanında yer alan operasyonel risk iştahı ve kapasitesi çerçevesinde, doğrudan veya dolaylı olarak maruz kalabileceği operasyonel riske ilişkin limitler, onaylanmış risk azaltım yöntemleri ve ilgili diğer hususlar,
    - Bankanın maruz kaldığı operasyonel riske yönelik limit takip süreci,
    - İzleme ve raporlama sürecinde kullanılan yönetim bilişim sistemi altyapısı,
    - Bağımsız tarafların operasyonel riske ilişkin değerlendirme ve denetim yapmalarını sağlayacak süreçler (istenilen formatta ve esneklikte bilgi üretebilecek sistemin varlığı, mümkün olduğunca "kara kutu" yaklaşımından kaçınılması, arşivleme ve yedeklemeye yeterli önemin verilmesi bahsi geçen sürecin temel unsurları arasında yer almaktadır),
    - Bankanın operasyonel risk profilinin önemli ölçüde değiştiği durumlarda politikaların gözden geçirilmesi veya güncellenmesi süreci (örneğin, sektörün ortalama %10 büyüme gösterdiği bir dönemde, bankanın %20 büyüme kaydetmesi).

Basel Komitesi operasyonel riski; yetersiz veya başarısız dâhili süreçler, insanlar ve sistemlerden veya harici olaylardan kaynaklanan kayıp riski olarak tanımlamıştır. Bahsi geçen tanımdan hareketle operasyonel riske neden olan ana risk faktörleri dört grup halinde izleyen sayfadaki tabloda örneklendirilmiştir.

Ana Risk Faktörleri	**Örnekler**
Süreçler	• Yetersiz ve uygun olmayan politika, prosedür ve rehberler, • İletişimin yapılamaması ya da iletişimde yaşanan aksaklıklar • Hatalı veri girişi • Yetersiz mutabakat • Yetersiz hukuki dokümantasyon • Kontrol noktalarındaki yetersizlikler • Yasal olarak ayrılması gereken karşılıkların ayrılmaması ya da eksik ayrılması veya karşılık ayırma sürecinin etkin olmaması • Değişim yönetimi süreçlerinde yaşanan aksaklıklar • Yetersiz yedekleme faaliyeti ile etkin olmayan aksiyon planları
Personel	• Rehber, politika ve prosedürlere uyulmaması • Yetkisiz işlem ve görevi ihmal • Ceza hukuku uyarınca konusu suç olan banka içi eylemler • Görev ve sorumluluk alanlarının ve çifte kontrol mekanizmasının oluşturulmasındaki eksiklikler, tecrübesiz personel çalıştırılması • Personel hatası ve dikkatsizliği, görev ve sorumlulukların açıkça tanımlanmaması
Sistem	• Bilgi işlem sisteminde yer alan donanım, ağ ve sunucuların işlerliklerinin sürdürülememesi
Harici Olaylar	• Ceza hukuku uyarınca konusu suç olan banka dışı eylemler • Hizmet sağlayıcıların kötü performans göstermesi • İnsan kaynaklı olarak yaşanan felaketler • Doğal felaketler • Politik ve yasal faktörler

ALTINCI KISIM

Operasyonel Risk Yönetim Süreci

İlke-6. Bankalar; ürünleri, faaliyetleri, süreçleri ve sistemleri dolayısıyla maruz kaldıkları operasyonel riski düzenli olarak tespit edebilecekleri, ölçebilecekleri, değerlendirebilecekleri, izleyebilecekleri ve kontrol edebilecekleri bir risk yönetim sürecine ve yeterli araçlara sahip olmalıdırlar.

Riskin Tespit Edilmesi, Ölçülmesi ve Değerlendirilmesi

İlke-7. Üst düzey yönetim tüm önemli ürün, aktivite, süreç ve sistemlerdeki operasyonel risklerin tespit edilmesi ve değerlendirilmesinden sorumludur.

38. Her bir banka, operasyonel risk profilini en doğru şekilde ortaya koymak ve bu sayede sahip olduğu kaynakları optimal şekilde risk yönetimine tahsis edebilmek amacıyla, öncelikle maruz kaldığı muhtelif operasyonel risk tiplerini mümkün olan en somut çerçevede tespit etmeli ve mezkûr risk tiplerine karşı kırılganlık düzeyini değerlendirmelidir. Etkin tespit, ölçme ve değerlendirme süreçleri, riskin yönetiminde müteakip aşamaları oluşturan izleme ve kontrol süreçlerinden beklenen sonuçların elde edilmesinde hayati öneme haizdir.

39. Operasyonel riskin tespit edilmesi sürecinde, banka faaliyetlerini olumsuz etkileyecek içsel ve dışsal faktörlerin yeterli kapsam ve içerikte dikkate alınması önemlidir. Bahse konu faktörlerden bazıları örnek olarak aşağıda sıralanmıştır.

- Bankanın yönetim yapısı, risk kültürü, insan kaynakları yönetiminde benimsediği yaklaşımlar ve uygulamaları, organizasyonel değişiklikler ve personel devir hızı,
- Bankanın müşteri, ürün ve hizmet profili, hizmet dağıtım kanallarının yapısı, işlem yoğunluğu ve işlemlerindeki karmaşıklık düzeyi,
- Bankanın müşterilerine sunduğu her bir ürün ve hizmete ilişkin teşkil edilen iş akışları ve bunların uygulanması süreci,
- Politik, yasal, teknolojik ve/veya ekonomik değişimlerin, bankanın faaliyet gösterdiği iş çevresi, sektörün eğilimleri, rekabet düzeyi ve piyasa yapısı üzerindeki etkileri.

40. Risklerin tespit edilmesini müteakip banka, tespit ettiği risklerin ölçülmesi ve değerlendirmeye tabi tutulması kapsamında uygun olan yaklaşımları belirlemeli, risklerin nedenlerini de dikkate alarak gerçekleşme olasılıklarını tahmin etmeli ve bunların bankanın mevcut faaliyet hacmi, yapısı ve hedefleri üzerindeki potansiyel etkilerini değerlendirmelidir.

41. Operasyonel riskin tespit edilmesi, ölçülmesi ve değerlendirilmesinde bankanın kullanabileceği araçlardan bazıları şunlardır:

(a) Denetim bulguları: İç ve dış denetimlerde elde edilen bulgular, esas olarak banka faaliyetlerindeki kontrol zafiyetlerine ve güvenlik açıklarına odaklanmakla birlikte maruz kalınan operasyonel risk düzeyinin belirlenmesi sürecinde önemli girdilerdir.

(b) İçsel kayıp verilerinin toplanması ve analizi: Operasyonel kayıp verileri bir bankanın iç kontrol sürecinin etkinliğinin ve maruz kaldığı operasyonel risk düzeyinin belirlenmesinde anlamlı girdiler sağlamaktadır. Kayıp olaylarının analiz edilmesi ise bu kayıpların nedenleri hakkında bilgi vererek örneğin, kontrol hatalarının olay bazındaki bir hatadan mı, yoksa sistematik bir hatadan mı kaynaklandığının anlaşılmasını sağlamaktadır.

(c) Dışsal verilerin toplanması ve analizi: Dışsal veriler; bankanın dışındaki kuruluşlarda gerçekleşen brüt operasyonel kayıp tutarları, kayıp yaşanan tarihler, tazmin tutarları (sigorta, personelden tahsil vb.) ve kayıpların nedenlerinden oluşmaktadır. Dışsal veri kayıpları, içsel veri kayıpları ile karşılaştırılarak bankanın kontrol çevresindeki muhtemel zayıflıkların tespit

edilmesinde ya da daha önce tanımlanamayan risk faktörlerinin tespit edilmesinde kullanılabilir.

(d) Risk Değerlendirmesi: Bir bankanın operasyonel riske ilişkin öz değerlendirmesi; faaliyet süreçleri ile faaliyetlerden kaynaklanan potansiyel tehditler ve bu tehditlere karşı banka nezdindeki zayıf noktaların değerlendirilmesini, ayrıca söz konusu tehditlerin ve zayıf noktaların banka üzerindeki muhtemel olumsuz etkilerinin analizini içermektedir. Bankanın ayrıca risk kontrol sürecini (risk kontrol süreci temelde, faaliyet kollarının bizzat gerçekleştirdiği kontroller ve iç kontrol biriminin kontrol uygulamalarından müteşekkildir) de değerlendirmesi gerekmektedir. Bu kapsamda banka, kontrol öncesi risk düzeyini değerlendirir, kontrol çevresinin etkinliğini gözden geçirir ve artık riskleri (kontrol sonrası geriye kalan risk faktörlerini) belirler. Artık riskler bankaca ağırlıklandırılabilir ve bu amaçla skor kartlar kullanılabilir. Bu sistem, değerlendirme sonuçlarının metrik sisteme aktarılmasını sağlayarak, kontrol çevresine ilişkin bir derecelendirme imkânı sunacaktır.

(e) İş Süreçleri Haritası: İş süreçleri haritası; banka faaliyetlerinin mümkün olan en genel sınıflamadan başlayarak her bir ürün/hizmetin üretilme sürecini ayrıntılı biçimde ve iş akış şemalarındaki bağlantı noktalarıyla bir arada gösteren yapıdır. Bu kapsamda banka örneğin, kurumsal finansman faaliyetini (birinci seviyede yer alan diğer bir ana faaliyete örnek perakende bankacılıktır) birinci seviye ayrımda belirledikten sonra bu ana faaliyete bağlı olan; satın alma-birleşmeler, menkul kıymetleştirme, menkul kıymet ihracına aracılık vb. alt faaliyetleri tanımlar. Her bir alt faaliyetin uhdesinde yer alan iş ve işlemlerin icra edilme yöntemlerini gösteren iş akış şemaları da bu haritanın tamamlayıcı unsurudur. Bankanın söz konusu haritaları, belirleyecekleri kurallar çerçevesinde yazılım desteği kullanarak ilgili personelin bilgisine sunmaları uygulamadan beklenen faydayı artıracaktır. İş süreçleri haritası sayesinde banka, münferit riskleri ve birbiriyle ilişkili riskleri belirlemeyi, diğer taraftan kontrol ve risk yönetimi fonksiyonlarındaki zayıflıkları ortaya çıkarmayı amaçlamaktadır. Harita sayesinde banka, iş süreçlerindeki ve diğer organizasyonel faaliyetlerindeki temel aşamaları ortak zeminde görebilecek ve bu sayede banka süreçlerinde yer alan temel risk noktalarını belirleyebilecektir. Bu yöntem ayrıca, bankanın müteakip dönemlerde alacağı yönetim aksiyonlarında önceliklerinin belirlenmesine de yardımcı olmaktadır.

(f) Risk ve Performans Göstergeleri: Risk ve performans göstergeleri bankanın maruz kaldığı risk faktörlerinin analizini sağlayan risk ölçü birimi ve/veya istatistikleridir. Göstergelerde yer alan sayısal büyüklükler ve bu büyüklüklerin zaman içinde gösterdiği değişimler operasyonel risklerin tespit edilmesi ve değerlendirilmesi sürecinde oldukça faydalıdır (örneğin, bankanın operasyonel etkinlik düzeyine ilişkin veriler, mutabakat hataları, personel devir hızı, sistem kesintileri, işlem hacimleri ve hata sayıları, denetim skorları, denetim dışı kalan faaliyet alanlarının sayısı/oranı, limit aşımları). Risk göstergeleri, temel risklere ilişkin muhtemel etkenlerin izlenmesinde kullanılır. Performans göstergeleri ise operasyonel zayıflık, hata ve kayıplar yaşanan iş süreçlerinin mevcut durumu hakkında anlamlı bilgiler sağlar. Her iki gösterge, risk seviyelerinin eşik/limitlere yaklaştığı veya aştığı ve acil risk azaltımı gerektiren tetikleyici seviyelerde bir uyarı mekanizması işlevi görürler.

(g) Senaryo analizleri: Banka, faaliyet kollarında görev yapan uzmanların ve risk yöneticilerinin görüşlerini alarak muhtemel operasyonel risk olaylarının tespit edilmesi ve bu olayların muhtemel sonuçlarının değerlendirilmesi amacıyla senaryo analizleri geliştirmelidir. Analizler, potansiyel risk faktörlerinin, ilave kontrollerin ya da risk azaltımına olan gereksinimin belirlenmesinde etkili bir araçtır. Senaryo analizlerinin sübjektif olma özelliği göz önünde bulundurularak, analiz sürecinde etkinliğin, tutarlılığının ve objektifliğin sağlanması amacıyla banka tarafından ilave tedbirler alınması uygun olacaktır. Bankanın risk yönetimi uygulamalarında yer vereceği senaryo analizlerine ilişkin kapsamlı açıklamalar "Bankaların Sermaye ve Likidite Planlamasında Kullanacakları Stres Testlerine İlişkin Rehber"de yer almaktadır.

(h) Risk Ölçümü: Banka, risk değerlendirme araçlarının (içsel kayıp verileri, denetim bulguları, senaryo analizleri vb.) çıktılarını, operasyonel risk ölçümü yapılan modelde girdi olarak kullanmak suretiyle maruz kaldıkları operasyonel risk düzeyini sayısallaştırılabilir. Modelin sonuçları bankanın ekonomik sermayesinin hesaplanması sürecinde ve risk-getiri ilişkisine göre faaliyet kolları bazında yapılacak değerlendirmelerde kullanılabilir.

Riskin sayısallaştırılması için gelişmiş hesaplama yöntemini benimseyen bankanın operasyonel kayıp olayları ile ilgili tam ve doğru tarihsel veriyi toplaması ve operasyonel kayıp oluşturan potansiyel kaynakları belirlemesi gerekir. Kayıp olaylarına ilişkin bankaca tesis edilen veri tabanı; ampirik analizlerde, model kurulmasında ve birbiriyle ilişkili kayıp olaylarının sayısallaştırılmasında kullanılabilir.

(i) Karşılaştırmalı analizler: Bu tür analizler bankanın risk profiline ilişkin kapsamlı bir değerlendirme yapmak üzere muhtelif değerlendirme araçlarından elde edilen sonuçların karşılaştırılması temeline dayanır. Örneğin, senaryo analizinde kullanılan verilerin, içsel ve dışsal verilerle karşılaştırılması sayesinde bankanın maruz kalabileceği riskin büyüklüğü daha iyi görülebilir.

Riskin İzlenmesi ve Raporlanması

İlke-8: Bankalar operasyonel risk profillerini ve maruz kaldıkları kayıpları düzenli olarak izlemek amacıyla süreç ve sistem tesis etmelidir.

42. Bu süreç, bankanın maruz kaldığı her türlü operasyonel risk tipine yönelik nitel ve nicel değerlendirmeleri, alınan düzeltici önlemlerin ve risk azaltımı kapsamındaki aksiyonların kalitesinin ve uygunluğunun değerlendirilmesini, yeterli oranda kontrol noktasının etkin olarak devrede olup olmadığının (örneğin, mevcut kontrol seviyesinin banka nezdinde önemli kayıplar ortaya çıkmadan önce problemlerin tespitine imkân sağlayıp sağlamadığı) gözden geçirilmesi uygulamalarını içermelidir. Tesis edilen süreç aynı zamanda bankanın ölçeğine, risk profiline ve faaliyet yapısına uygun olmalıdır.

43. Riskin izlenmesi kapsamında banka, operasyonel risk doğuran faktörlere yönelik olarak erken uyarı mahiyetinde risk göstergeleri geliştirmelidir. Bu göstergeler, bankanın maruz kalabileceği kayıp olaylarına ilişkin tahmini bilgiler vererek ve riskin muhtemel kaynaklarını açıklayarak, bankanın önemli kayıplara maruz kalmadan önce gerekli aksiyonları almasına imkân

verecektir. Göstergelerin tespitinde bankanın muhtelif faaliyet türlerinden ve kontrol süreçlerinden oluşan ve bankanın tüm faaliyetlerini kapsayıcı bir havuzdan yararlanılır. Göstergeler, banka nezdindeki muhtelif faaliyet kolları tarafından düzenli olarak izlenir. Temel göstergeler şeklinde tesis edilen hedef ve limitler veya tetikleyici seviyeler, izleme sürecinde bankanın operasyonel risk düzeyindeki artışa yönelik bir erken uyarı vazifesi görerek, riskin yönetimindeki kötüleşmenin ve ortaya çıkması muhtemel problemlerin banka üst düzey yönetimi ile müzakere edilmesine imkân verecektir (suiistimalleri önleyici erken uyarı mekanizmalarına verilebilecek diğer uygulama örnekleri; günlük yapılan merkezi hesap kontrolleri, geçici hesaplara yönelik özel kontroller, belirli bir kişiye aynı gün açılan birden fazla krediye yönelik kontroller vb.).

44. Operasyonel riskin izlenmesi süreci, rutin banka faaliyetlerine entegre edilmeli ve bu kapsamda her bir faaliyet kolunun operasyonel risk oluşturma potansiyeli değerlendirilmeli, mezkûr değerlendirme sürecinde faaliyet gösterilen iş çevresindeki değişikliklerin sıklığı ve özellikleri de dikkate alınmalıdır.

45. Operasyonel riskin izlenmesi kapsamında banka yönetim kuruluna sunulmak üzere rapor hazırlanmalı ve hazırlanan raporda, mümkün olduğunca banka içi finansal ve operasyonel işlemlere ait veriler, bankanın yasal ve banka içi düzenlemelere uyum seviyesi ve karar alma süreçlerinde dikkate alınması gereken dış piyasa koşulları hakkında bilgiler yer almalıdır. Bu türden bir raporlamanın temel amacı, banka yönetimine bankanın operasyonel risk profilini ve doğurduğu etkileri yeterli kapsam ve içerikte anlaşılmasını sağlayacak muhtelif bilgiler sunulmasıdır. Bu raporlarda banka yönetim kurulunun, üst düzey yönetimin ve ilgili faaliyet kollarının özellikle bilgi sahibi olmasını amaçlayan hususlar aşağıda sıralanmıştır.

- Bankanın karşı karşıya olduğu mevcut veya potansiyel kritik operasyonel riskler (örneğin, temel risk göstergelerinin doğrudan veya trend analizi yoluyla işaret ettiği olumsuz değişimler, denetim veya uyum raporlarında yer verilen değerlendirmeler),
- Önemli düzeyde risk doğuran olaylar, veri kaybı yaşanan tecrübeler, bunların nedenleri ve gerekli görülen iyileştirici önlemler,
- Risk azaltım ve risk transfer stratejileri,
- Alınan önlemlerin seviyesi ve/veya etkinlik düzeyi,
- Yeni ürünlerden kaynaklanan operasyonel riske ilişkin bilgiler,
- Zayıf alanların tanımlanması,
- Operasyonel risk tutarlarının faaliyet kolları arasındaki dağılımı, yönü ve geçişmeleri,
- İstisnai raporlamalar (bankada risk iştahı, risk kapasitesi ve risk politikalarından bilinçli veya bilinçli olmayan sapmalar, operasyonel riske ve kayıp düzeylerine yönelik önceden tanımlanmış limit ve eşiklerde gerçekleşen veya gerçekleşmesi olası ihlaller),
- Önem arz eden banka dışı olaylar ve bunların banka ve bankanın operasyonel risk sermayesi üzerindeki muhtemel etkileri.

Bir bankada risk izleme sürecinin tüm sonuçları, iç kontrol, iç denetim ve/veya risk yönetimi birimi tarafından tespit edilen bulgular, bağımsız dış denetçiler ve denetim otoritesi tarafından hazırlanan raporlar mümkün olduğu ölçüde hazırlanan operasyonel risk yönetim/izleme raporunda yer almalıdır.

Banka yönetim kuruluna sunulacak söz konusu raporlamanın teşkili sürecinde kullanılmak üzere, üst düzey yönetim tarafından, faaliyet kolları, destek birimleri, operasyonel risk yönetimi birimi ve iç denetim birimi gibi riskin oluşumu ve yönetimi kapsamında pay sahibi olan birimlerden düzenli olarak raporlar alınacaktır. Banka üst düzey yönetimi, operasyonel risk yönetimine ilişkin kendisine sunulan raporların zamanında ve düzenli olarak alınmasından ve bu raporlar sayesinde ilgili yönetim kadrolarının kendi faaliyet alanlarını izlemesinden ve ayrıca raporlarda yer alan kritik öneme haiz hususların yönetim kurulu seviyesinde müzakere edilmesinden sorumludur.

46. Raporlamaya ilişkin sıklık veya zamanlama, ihtiyaçlara göre planlanmalı, strese tabi koşullarda da ilave raporlama yapma imkânı sağlanmalıdır. Raporlama sıklığı belirlenirken bankanın hacmi, faaliyet yapısındaki karmaşıklık, riskin yapısal özellikleri ve faaliyet ortamındaki değişim sıklığı göz önünde bulundurulmalıdır. Ancak her halükarda raporlamaların, bankanın faaliyet hacmi, yapısı ve/veya karmaşıklığına göre asgari 3 aylık veya 6 aylık dönemlerde mutat olarak yapılması esastır.

47. Bankanın halihazırdaki raporlama ve veri toplama süreçleri, mevcut risk yönetim performansının iyileştirilmesi ve risk yönetimi politika, prosedür ve uygulamalarının geliştirilmesi amacıyla düzenli olarak gözden geçirilmeli, bu kapsamda iyi uygulamalar takip edilmelidir.

48. Banka üst düzey yönetimi, operasyonel riskin yönetimine ilişkin raporlamaların kapsamlı, doğru, tutarlı ve kullanılabilir olmasını sağlamalıdır. Bu minvalde raporların uygun kapsam ve hacimde olmasına dikkat edilmeli, verilerin yetersiz ya da aşırı düzeyde olmaları nedeniyle etkin karar alma imkânının ortadan kalkmasına sebebiyet verilmemelidir. Alınan raporların amaca matuf ve güvenilir olmasını sağlamak üzere üst düzey yönetim, bankada tesis edilen raporlama sisteminin zamanlama tablosuna uyumunu, tam ve doğru bilgi sağlayıp sağlamadığını, farklı birimlerce hazırlanan raporlarda aynı başlıkta yer alan bilgilerin tutarlılığını, raporların ilgili mercilere zamanında ulaşmasını, banka ölçeği ve risk profiline uygunluğunu ve yapılan iç kontrol faaliyetlerine ilişkin istatistikleri düzenli olarak gözden geçirmelidir.

Riskin Kontrolü ve Azaltımı

İlke-9: Bankalar; hazırlayacakları politika, prosedür ve sistemlerden yararlanarak, iç kontrol, risk azaltım ve/veya transfer stratejilerinin uygulandığı güçlü bir operasyonel risk kontrol ve azaltım süreci teşkil etmek zorundadırlar.

49. Banka nezdinde yerine getirilen iç kontrol uygulamaları, banka operasyonlarının verimli ve etkili olmasına, personel hatalarının minimize edilmesine, varlıkların güvence altında tutulmasına, güvenilir finansal raporların üretilmesine, meri kanun ve alt düzenlemelere uyum gösterilmesine imkân sağlamalıdır.

50. Tesis edilen kontrol süreçleri, banka politikalarına uyum düzeyini arttırmaya yönelik muhtelif uygulamaları (örneğin, herhangi bir iş sürecinde yapılan işlemler ile bahse konu iş sürecine ilişkin prosedürde öngörülen işlemler arasındaki uyumsuzlukları konu eden farklılık raporları)

içermelidir. Politikalara uyum düzeyinin değerlendirilmesi kapsamında aşağıdaki unsurların dikkate alınması yararlı olacaktır.

- Belirlenen hedeflere yönelik işleyen sürecin, banka üst düzey yönetimi tarafından sürekli olarak takip edilmesi,
- Uyum sağlanmamış noktalara ilişkin olarak alınan tedbir ve çözümler üzerinden kaydedilen gelişmelerin düzenli olarak üst düzey yönetim tarafından gözden geçirilmesi,
- İlgili yönetim seviyelerinde hesap verilebilirliğin sağlanması amacıyla gerekli yetkilendirme ve onaylama süreçlerinin belirli aralıklarla gözden geçirilmesi,
- Eşik değerler ve limitlerdeki istisnai uygulamaların veya politikalardaki diğer bilinçli/bilinçsiz sapmaların izlenmesine yönelik etkin bir raporlama sürecinin tesis edilmesi.

51. Etkin bir kontrol çevresi, banka içinde görev ve sorumluluk dağılımının mümkün olduğu ölçüde ayrıştırılmasını ve çapraz kontrol noktalarının tesis edilmesini gerektirir. Zira personel arasında çatışmaya neden olan veya kontrol (veya diğer benzer önlemler) süreci bulunmayan görevlendirmeler, bankada kayıpların, hataların ve yasal olmayan aksiyonların gizlenmesine sebep olacaktır. Bu nedenle, menfaat çatışmasına yol açabilecek potansiyel noktaların tespit edilmesi, minimize edilmesi ve bağımsız izleme/kontrol süreçlerine tabi kılınması önem arz etmektedir.

52. Banka risk yönetimi kontrol altyapısını; aktif büyümesine ve faaliyet yapısındaki genişlemeye ve artan karmaşıklık düzeyine (örneğin, yeni ürün, iştirak-şube ağı, yabancı piyasalara giriş) paralel şekilde geliştirmek ve genişletmekle mükelleftir.

53. Bir banka nezdindeki operasyonel risk kontrolü uygulamaları genel itibarıyla aşağıdaki unsurlardan oluşmaktadır.

- Personel arasındaki menfaat çatışmalarını, kayıpların-hataların gizlenmesini ve personelin diğer yasal olmayan davranışlara girmesini engelleyici nitelikte etkin görev dağılımı ve açık bir biçimde tasarlanmış yetkilendirme ve onay süreçleri,
- Belirlenen risk eşik değerlerine ve limitlere bağlılığın yakından izlenmesi ve ihlallerin araştırılması,
- Banka varlıklarının ve veri tabanlarının kullanımına ilişkin etkin bir yetkilendirme ve güvenlik süreci,
- Tüm seviyelerdeki banka faaliyetlerinde uzmanlaşmanın sağlanması ve sürdürülmesine yönelik olarak, uygun personel seçimi ve eğitim imkânlarının geliştirilmesi (aynı kıdemdeki ve benzer faaliyetleri yürüten personelin eşit sürelerde benzer konularda eğitim almalarının sağlanması da mezkûr kapsamda dikkate alınmalıdır),
- Bankada yürütülen faaliyetlere ilişkin hazırlanan eğitim dokümanlarının çalışanların kolay ulaşımına imkân verecek şekilde bilgi işlem sistemi bünyesinde bulundurulması ve bunların düzenli biçimde güncellenmesi
- Beklentilerin önemli ölçüde dışında gelir/fayda sağlayan faaliyet birimi ve ürünlerin önceden tespit edilmesine yönelik süreçler (örneğin, bankanın düşük risk ve düşük getiri oranı şeklinde gerçekleşmesini beklediği bir işlemden bankanın yüksek gelir elde etmesi

durumunda söz konusu gelirin herhangi bir usulsüzlük sonucu elde edilip edilmediği ya da iç kontrol zafiyetinden kaynaklanıp kaynaklanmadığı araştırılmalıdır),

- Banka işlemlerinin ve muhasebe hesaplarının düzenli olarak mutabakatının sağlanması,
- İzin, hastalık vb. durumlardan dolayı görevini belirli bir süre yerine getiremeyecek personele ait sorumlulukların sekteye uğramasına engel olacak nitelikte bir izin ve vekâlet politikası.

54. Banka maruz kaldığı operasyonel riskleri tanımladıktan sonra öncelikle söz konusu risklere yönelik takip edeceği stratejileri belirler. Bu süreçte her bir banka maruz kaldığı riskleri; öngördüğü politika ve prosedürleri uygulayarak kontrol etme, risk azaltım tekniklerini kullanarak azaltma, başka bir sektöre veya alana transfer etme, alternatif risk türlerini tercih etme (örneğin, yasal risk veya karşı taraf riski) veya mevcut haliyle taşıma seçenekleri arasından kendisine ve duruma uygun olanı belirlemelidir. Kontrolü ve azaltımı mümkün olmayan riskler için bankanın, riskleri kabul edip etmeyeceği, bahse konu iş kolundaki faaliyet düzeyini azaltıp azaltmayacağı veya faaliyeti tamamen sonlandırıp sonlandırmayacağı değerlendirilmelidir.

55. Banka sigorta gibi risk azaltım tekniklerinden faydalanmak suretiyle maruz kaldığı riskleri üçüncü taraflara transfer edebilir. Bununla birlikte risk azaltımında kullanılan araçların banka tarafından operasyonel risk kontrollerinin yerine kullanılması doğru bir yaklaşım değildir.

Dikkate Alınması Gereken Özel Hususlar

56. Banka, aşağıda yer verilen faktörlere yönelik özel nitelikli politika ve prosedürlere sahip olmalıdır.

- **Yeni ürün ve faaliyetler**

57. Operasyonel risk düzeyi bankanın yeni faaliyet türlerine giriştiği veya yeni ürünler geliştirdiği dönemlerde ve özellikle mezkûr faaliyet ve ürünlerin bankanın temel faaliyet yapısına yabancı olduğu durumlarda belirgin olarak yükselmektedir. Dolayısıyla banka; yeni ürün/faaliyet onaylama süreçlerini belirli standartlar altında yazılı politika ve prosedürlere dayandırmalı, ürün ve faaliyete ilişkin görev ve sorumlulukları açık bir biçimde tanımlamalıdırlar. Hazırlanan politika ve prosedürlerin temel amacı, yeni bir girişimin veya mevcut faaliyet yapısındaki değişikliğin kontrollü bir şekilde uygulamaya geçirilmesi ve ilgili iş kolları ve destek birimlerinin uygulama sürecine hazır hale getirilmesidir.

58. Bankanın yeni ürün, faaliyet, süreç ve sistemler dolayısıyla maruz kalacağı muhtemel risk türleri ve düzeyleri özel olarak değerlendirilmeli ve bunlar yapılacak söz konusu değerlendirme sonrası hayata geçirilmelidir. Mezkûr değerlendirme ve onaylama süreci asgari olarak aşağıdaki hususları açıklığa kavuşturmalıdır.

- Yeni ürün, hizmet ve faaliyetin doğuracağı muhtemel riskler nelerdir?
- Yeni ürünlerin değerlemesi yapılırken ortaya çıkabilecek zorluklar nelerdir ve ekonominin stres dönemlerinde söz konusu değerlemeler nasıl değişecektir?
- Bankanın mevcut operasyonel risk profili, risk iştahı ve risk kapasitesinde ne tür değişiklikler yaratacaktır?

- Uygun olan kontrol ve risk yönetim süreçleri ile risk azaltım stratejileri nelerdir?
- Kontrol sonrası ortaya çıkacak artık riskler nelerdir?
- İlgili eşik değer ve limitlerde değişiklik yapılmalı mıdır?
- Yeni ürün ve faaliyetlerden kaynaklanacak risklerin ölçümünde, izlenmesinde ve yönetiminde kullanılacak prosedürler ve ölçüm yöntemleri nelerdir?

▪ **Bankanın bilgi teknolojileri kapasitesinin, sistemlerinin, tesislerinin ve ekipmanlarının güvenliği ve değişimleri**

59. Bilgi teknolojileri (BT) imkânlarının yaygın kullanımı, bankanın etkin bir kontrol çevresine sahip olmasına önemli katkılar sağlamaktadır. Zira otomatize edilmiş süreçler manuel süreçlere göre hata riskini büyük ölçüde minimize etmektedir. Buna karşılık ürünlerin sunumunda, faaliyet ve süreçlerde ya da hizmet dağıtım kanallarında kullanılan teknolojik altyapılar aynı zamanda bankanın stratejik, operasyonel, itibar vb. risk türlerine ve maddi kayıplara maruz kalmasına da sebep olmaktadır. Bu nedenle bankanın; tesis edeceği teknoloji riski yönetimi ve altyapıya ait risk yönetimi programlarını takip ederek teknoloji kullanımından ve otomatize edilmiş süreçlerden doğan risk faktörlerini tespit etmesi, ölçmesi, izlemesi ve çeşitli araçlar kullanarak yönetmesi gerekmektedir. Teknoloji riski, operasyonel risk yönetimine benzer yaklaşımlarla yönetilir ve temel olarak aşağıdaki unsurları ihtiva etmelidir.

- Alınan destek hizmetleri de dâhil olmak üzere bankanın teknolojik altyapısının, mevcut faaliyet yapısı ve hedefleri ile uyumlu gelişme göstermesini sağlayacak yönetim ve kontrol uygulamaları,
- Riskin yönetimi ve kontrolüne destek sağlamak üzere risk iştahının, kapasitesinin ve performans beklentilerinin oluşturulması,
- Risklerin tespit edilmesi ve değerlendirilmesine imkân sağlayan politika ve prosedürlerin belirlenmesi,
- Politika ve prosedürler kapsamında etkin bir kontrol çevresinin oluşturulması ve risk transfer-azaltım stratejilerinin ortaya konulması gereken durumlarda uygulamaya sokulması,
- Belirlenen eşik değerler ve limitlere uyum düzeyinin izlenmesi.

60. Teknoloji riski yönetimi kapsamında hazırlanacak politika ve prosedürler temel olarak, bankanın BT altyapısı dolayısıyla maruz kaldığı riskin yeterli düzeyde BT kontrolleri, güvenlik yönetimi, sistem geliştirme ve değişim yönetimi, bilgi işlem süreci, iletişim ağları ve teknoloji hizmet sağlayıcıları üzerinden yönetimini amaçlamaktadır.

61. Banka üst düzey yönetimi, bankanın normal şartlar altındaki faaliyet düzeyinin yanı sıra stresli piyasa koşulları altında da faaliyetlerinde aksamaya yol açmayacak, diğer taraftan mevcut ve uzun vadeli faaliyet planlaması için yeterli kapasiteyi haiz bir teknoloji altyapısına sahip olmasını sağlamakla yükümlüdür. Bu altyapı, gerekli verilerin sağlanmasına, sistem entegrasyonuna, güvenliğine, sisteme zamanında ulaşılabilirliğe, kapsamlı risk yönetimine ve yetkili üçüncü taraflarca talep edilen bilgilerin esnek bir biçimde istenilen şekil ve içerikte sunulabilmesine imkân sağlamalıdır. Ayrıca, operasyonel risklerin düzenli olarak BT bağımsız denetimleri vasıtasıyla üçüncü taraflarca ele alınması riskin yönetiminde oldukça önem arz etmektedir.

62. Banka birleşme ve satın alma süreçlerinde ortaya çıkan; parçalı, aralarında bağlantı bulunmayan, maliyet düşürmeye yönelik olan ya da yetersiz yatırımlar şeklindeki teknolojik altyapılar dolayısıyla önemli düzeyde operasyonel riske maruz kalmaktadır. Operasyonel riske neden olan faktörler temel olarak, konsolide edilen kuruluşlar ve/veya faaliyet alanlarından gerekli bilgilerin toplanmasını ve analiz edilmesini zorlaştırarak, riskin muhtelif boyutlarıyla ele alınmasını engelleyecek, diğer taraftan özellikle yüksek büyüme dönemlerinde risklerin yönetimi ve izlenmesini sekteye uğratacaktır. Bu nedenle banka yönetimleri, uygun seviyede sermaye tahsis ederek özellikle birleşme işlemleri tamamlanmadan veya yüksek büyüme stratejileri uygulamaya konmadan ve yeni ürünler müşterilere sunulmadan önce sağlam teknoloji altyapılarını bankada işler hale getirmelidirler.

- **Alternatif Dağıtım Kanalları**

63. Alternatif dağıtım kanallarından (ATM, internet bankacılığı, cep bankacılığı vs.) kaynaklı risklerin yönetimi, bankanın teknoloji riski yönetiminin ayrılmaz bir parçasını oluşturmaktadır. Bu kapsamda, müşterilerin yetkilendirilmesi, bilgilerin gizlilik ve bütünlüğü, uygulamaların güvenliği, internet altyapısı, güvenliğin izlenmesi ile müşteri hesaplarına yetkisiz girişlerin (örneğin, sahte e-posta ve internet adreslerinin kullanımı yoluyla) önlenmesini konu alan müşteri güvenliği uygulamaları ve riskin yönetimini amaçlayan diğer münhasır kontroller yer almaktadır.

- **Destek Hizmetleri**

64. Bankaların, mevduat veya katılım fonu kabulü, nakdî, gayrinakdî her cins ve surette kredi verme ve mevzuatta kredi olarak sayılan işlemler dışında kalan faaliyetlerini banka adına gerçekleştiren; ya da reklamının yapılması hariç olmak üzere mevduat veya katılım fonu kabulü dışındaki faaliyetlerinden herhangi birinin pazarlanması da dâhil gerçekleştirilmesinde bankalara yardımcı nitelikte hizmet veren kuruluşlar destek hizmeti kuruluşu kabul edilmektedir. Bu türden bir hizmet alımı bankalar açısından önemli olan maliyet avantajı, uzman desteği, ürün yelpazesinin genişlemesi veya hizmetlerin iyileştirilmesi konularında avantaj sağlamasıyla birlikte banka yönetimlerinin dikkate alması gereken bir takım riskler doğurmaktadır. Destek hizmetlerinden kaynaklanan risklerin yönetimi, öngörülen hizmetin banka için taşıdığı kritik önem, servis sağlayıcı hakkında yapılacak durum değerlendirmesi, hizmete ilişkin kontrol imkânları ve acil durum eylem planı gibi unsurlar üzerinden kapsamlı risk değerlendirmelerini içermektedir. Yönetim kurulu ve üst düzey yönetim, destek hizmeti anlaşmalarının yarattığı riskleri anlama ve bu risklerin yönetimine yönelik etkin politika ve prosedürler geliştirmekle sorumludurlar. Destek hizmeti alımı politikaları ve risk yönetimi uygulamaları temel olarak aşağıdaki unsurları ihtiva etmelidir.

- Hangi tür banka faaliyetlerinin ne şekilde destek hizmeti alımına konu edilebileceğini belirleyen politika ve prosedürler,
- Potansiyel hizmet sağlayıcıların seçimine yönelik değerlendirme çalışmasında takip edilecek süreç,

- Destek hizmeti alım anlaşmalarının sağlıklı bir şekilde oluşturulması (anlaşmalarda sahiplik, bilgilerin güvenilirliği, sır koruma yükümlülüğü, sorumluluklar, fesih hakları vb. hususların açık ve anlaşılır olarak ortaya konması gereklidir),
- Destek hizmeti alımından doğan risklerin ve hizmet sağlayıcıların izlenmesine yönelik uygulamalar (örneğin, hizmet sağlayıcının yükümlülüklerini yerine getirebilmesi açısından önemli olan finansal durumunun düzenli olarak takip edilmesi),
- Kritik öneme haiz destek hizmetlerinde yaşanabilecek aksama ihtimaline karşılık uygulanabilir ve test edilmiş bir acil durum eylem planının geliştirilmesi,
- Hizmet sağlayıcı kuruluş ve bankanın sorumluluklarının net bir biçimde belirlendiği yeterli kapsam ve içeriğe sahip yeknesak kontrat ve/veya hizmet alımı anlaşmalarının hazırlanması ve bu hususun temini için hukuk biriminden görüş alınması

65. Bankanın destek hizmeti alımından kaynaklı riskleri yeterli ölçüde yönetemediği, ancak hizmet alımının durdurulmasının da makul bir seçenek olarak görülemeyeceği durumlarda banka üst düzey yönetimi, kontrol zafiyetlerini ortadan kaldırmak amacıyla maruz kaldığı riskleri üçüncü bir tarafa transfer edebilir (sigorta vb. araçlar vasıtasıyla). Yönetim kurulu bu durumda bankanın finansal gücünü dikkate alarak yönetebileceği maksimum kayıp tutarlarını belirler ve bankanın risk ve sigorta yönetimi programını uygulamaya geçirir. Söz konusu programın sonuçları düzenli aralıklarla gözden geçirilmelidir. Ancak bu uygulamalar, banka yönetim kurulu üyelerine ve yöneticilerine yönelik mevzuatta getirilen sorumlulukları ortadan kaldırmaz.

- **Kara paranın aklanması**

66. Banka, kara paranın aklanması ve terörün finansmanı ile mücadele kapsamında müşterini tanı, mevzuat uyum, yasal otoritelerle işbirliği ve sürekli personel eğitimleri vb. hususlarda politika, prosedür ve kontroller geliştirmelidir.

- **Uygun Müşteri Seçimi**

67. Banka, karmaşık yapıdaki yüksek risk içeren belirli ürünleri satacağı müşteri tiplerini tanımlamalı, bu ve benzer hususların yer aldığı politika ve prosedürlere sahip olmalıdır. Hedef müşteri kitlesinin tanımlanmasında, bu müşterilerin satın alacakları ürünlerden kaynaklanan riskleri anlayabilecek ve taşıyabilecek kapasiteye sahip olmaları, bankanın dikkate alması gereken temel kriterdir.

- **Yurtdışı şubeler ve iştirakler**

68. Yurtdışı şube ve iştiraklerin ana bankacılık sistemleri ve faaliyet süreçleri bankanın risk profilini önemli ölçüde etkileyebilmektedir. Bu nedenle banka, şube ve iştiraklerde mevcut olan sistemleri kendi ana sistemine mümkün olan en üst seviyede entegre etmeli ve faaliyet süreçlerini yeterli kapsam ve içerikte dokümante etmeli, meydana gelen değişimlerin etkilerini anlamalı ve yurtdışı operasyonları üzerinde uygun kontrol mekanizmalarını geliştirmelidir.

- **Dış Dokümantasyon**

69. Dış dokümantasyon, bankalar tarafından düzenlenerek müşterilere, üçüncü taraflara veya herhangi bir karşı tarafa sunulan ve bankaya hak/yükümlülük getiren dokümanları (örneğin kontratlar, işlem beyanları veya reklam broşürleri) ifade etmektedir. Bu dokümanlarda yer alan bilgilerin eksik veya yanlış olması yasal riske ve/veya operasyonel riske yol açmaktadır. Bu nedenle bankanın dış dokümantasyonu yayımlamadan önce gözden geçirdiği yazılı bir kontrol sürecine sahip olması önem arz etmektedir. Bu kontrol sürecinde bankanın hukuk biriminin yazılı görüş vermesi en önemli aşamayı oluşturmaktadır. Yayımlanması planlanan dokümanların bahse konu gözden geçirme sürecinde temel olarak aşağıdaki unsurlar bazında kontrol edilmesi uygun olacaktır.

- Yasal mükellefiyetlere uygunluk,
- Dokümanlarda kullanılan standart ve standart olmayan terimlerin kapsamı,
- Dokümanların yayımlandığı kanallar,
- Onay mekanizmasının uygunluğu,
- Sözleşmenin bankaca hazırlanan standart sözleşme tiplerine uygunluğu.

YEDİNCİ KISIM

İş Sürekliliği

İlke-10. Bankaların sürekli olarak faaliyetlerine devam edebilmesine ve ayrıca önemli iş kesintilerinin ortaya çıktığı dönemlerde maruz kalacakları kayıpları sınırlamaya yönelik bir iş sürekliliği planına sahip olmaları zorunludur.

70. Banka, faaliyetlerine zarar verici nitelikteki olaylara sürekli olarak maruz kalmaktadır. Bu olaylardan bazıları bankanın sorumluluklarından bir kısmını veya tamamını yerine getirememesine neden olabilmektedir. Banka hizmet binalarına, iletişim-bilgi teknoloji altyapısına zarar veren veya bunlara ulaşımı olanaksız kılan kazalar veya bankanın insan kaynaklarını olumsuz etkileyen olaylar banka bazında önemli finansal kayıpların yaşanmasına ya da finansal sistemin topyekûn zarar görmesine de yol açabilir. Bu türden olaylara karşı her banka kendi büyüklüğü, faaliyet yapısı ve iş süreçlerinin karmaşıklığını dikkate alarak bir iş sürekliliği planı oluşturmak zorundadır. Bu planlar bankanın hazırlıksız ve savunmasız kalabileceği farklı türden makul ve mantıklı senaryolara göre geliştirilmiş muhtelif müdahale programlarını ortaya koymalıdır.

71. İş sürekliliği yönetimi kapsamında her bir banka; iş etki analizine, sistem ve veri kurtarma stratejilerine, iş sürekliliği yönetiminin muhtelif açılardan test edilmesine, acil durumlardaki görev, yetki ve sorumluluk dağılımının açık ve anlaşılır biçimde ortaya konulmasına, iş sürekliliği planında yer alan uygulamalarla ilgili eğitimlere, farkındalığın arttırılmasını sağlayacak programlar ile iletişim ve kriz yönetimi programlarına yer vermelidir. Banka mezkûr süreçte öncelikle kritik faaliyetlerini, konsolide ve konsolide olmayan bazda bağımlı olduğu banka içi ve dışı hizmet çeşitlerini (örneğin, elektrik-su gibi kamu hizmetleri, mal tedarikleri, üçüncü taraflardan sağlanan destek hizmetleri) ve bunlara ilişkin uygun esneklik seviyelerini belirlemelidir. Bankaca oluşturulan olumsuz durum senaryoları, finansal,

operasyonel ve itibari etkileri açısından değerlendirilmeli, ortaya çıkan risk değerlendirmeleri bankanın kurtarma öncelikleri ve hedefleri için temel oluşturmalıdır. İş sürekliliği planları bankada acil durum stratejilerini, kurtarma-yeniden başlama prosedürlerini, yönetimin, personelin, yasal otoritenin, müşterilerin, hizmet sağlayıcıların ve gerekli olan durumlarda sivil otoritenin (meslek kuruluşları) bilgilendirilmesine yönelik iletişim planlarını içermelidir.

Banka, acil durum stratejilerinin mevcut faaliyetler, riskler, tehditler, esneklik gereksinimleri ve kurtarma öncelikleri ile uyumlu/tutarlı olup olmadığını kontrol etmek üzere iş sürekliliği planını düzenli olarak gözden geçirmelidir. Acil durum eylem planının personel tarafından eksiksiz bir şekilde uygulanabilmesini sağlamak üzere, eğitim ve farkındalık programları uygulanmalıdır. Bu doğrultuda kurtarma öncelikleri ile zaman kısıtının uyum gösterip göstermediğinin kontrol edilmesi amacıyla planlar periyodik olarak test edilmelidir. Ayrıca bankanın uygun zaman aralıklarında kritik öneme sahip hizmet sağlayıcıları ile birlikte afet kurtarma ve iş sürekliliği planlarını da test etmesi gerekmektedir. Test sonuçları eş zamanlı olarak üst düzey yönetim ve yönetim kuruluna raporlanmalıdır.