# OPERASYONEL RİSKİN YÖNETİMİNE İLİŞKİN İYİ UYGULAMA REHBERİ

## AMAÇ

Bu Rehberin amacı, 62/2017 sayılı Bankacılık Yasasının 17'nci ve 22'nci maddeleri kapsamında "Operasyonel Riskin Yönetimine" ilişkin bankalardan beklenen iyi uygulamaları, açıklamaktır.

## KAPSAM

Kuzey Kıbrıs Türk Cumhuriyetinde faaliyet gösteren bankalar, bu Rehber kuralları kapsamındadır.

Operasyonel risk yönetim sisteminin, bu Rehberde yer alan ilkeler doğrultusunda ve aşağıda yer alan hususları kapsayacak şekilde tasarlanması ve uygulanması gerekmektedir:

- Üst yönetimin gözetimi,
- Riskin yönetimine ilişkin banka içi politika ve süreçleri,
- Yeterli risk ölçüm, izleme ve kontrol süreçleri ve
- Kontrol faaliyetleri.

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.

Bu Rehberde yer alan hususların banka faaliyetlerinin karmaşıklığı ve büyüklüğü de dikkate alınarak solo ve konsolide yapıya uygun olarak tesis edilmesi beklenmektedir.

## TANIMLAR

Artık Risk; risk azaltmaya yönelik olarak gerçekleştirilen risk yönetimi aksiyonlarından ve kontrol uygulamalarından sonra geriye kalan risk düzeyini anlatır.

Acil ve Beklenmedik Durum Planı; faaliyetlerde ani ve planlanmamış bir kesintiye, iş kaybına veya krize neden olması muhtemel bir durumda risklerin ve sorunların yönetilebilmesi amacıyla alınacak tedbirlerin ve gerçekleştirilecek öncelikli eylemlerin belirlendiği, iş sürekliliği planının bir parçası olan planı anlatır.

İş Sürekliliği Yönetimi; felaket, kriz veya kesinti durumunda etkin önlem alınabilmesi; itibarın, marka değerinin, değer yaratan faaliyetlerin ve paydaşların çıkarlarının korunabilmesi amaçlarıyla belirlenen operasyonların sürekliliğinin temin edilmesi veya hedeflenen zaman diliminde kurtarılabilmesinin sağlanması ve kriz öncesi duruma dönülmesine yönelik, potansiyel risklerin belirlenmesini de içeren politika, standart ve prosedürleri içeren bütünsel yönetim sürecini anlatır.

İş Sürekliliği Planı; iş sürekliliği yönetiminin bir parçası olan ve bir kesinti durumunda bankanın öncelikleriyle uyumlu olarak faaliyetlerin sürdürülmesine ve mevzuata uyum sağlanmasına yönelik politika, standart ve prosedürlerden oluşan yazılı plan veya planlar bütününü anlatır.

Kontrol Çevresi; bir bankanın yönetim felsefesi, çalışma tarzı, etik ilkeleri, iç sistem birimlerinin süreçleri, organizasyon yapısı, politika ve süreçleri, raporlama yapısı, yetki/onay süreçleri ve görev dağılımı gibi operasyonel risk yönetiminin başarısında etken olan unsur ve uygulamaların tümünü anlatır.

Merkez Bankası; Kuzey Kıbrıs Türk Cumhuriyeti Merkez Bankasını anlatır.

Operasyonel Risk; yetersiz veya başarısız iç süreçler, insanlar ve sistemlerden ya da harici olaylardan kaynaklanan ve yasal riski de kapsayan zarar etme olasılığını anlatır.

Risk Çerçevesi; bankayı etkileyebilecek potansiyel olayları tanımlamak, riskleri bankanın kurumsal risk alma profiline uygun olarak yönetmek ve bankanın hedeflerine ulaşması ile ilgili olarak makul bir derecede güvence sağlamak amacı ile oluşturulmuş; bankanın üst yönetimi ve diğer tüm çalışanlar tarafından etkilenen ve stratejilerin belirlenmesinde kullanılan, bankanın tümünde uygulanan sistematik süreci anlatır.

Risk İştahı; bankanın, risk kapasitesini göz önünde bulundurarak hedef ve stratejilerini gerçekleştirmek için toplu olarak ve her bir risk türü itibarıyla taşımaya razı olduğu risk düzeyini anlatır.

Risk Kapasitesi; yasal ve varsa banka tarafından belirlenmiş sınırların aşılmasına yol açmayan azami risk düzeyini anlatır.

Risk Kültürü; risk farkındalığının banka nezdinde var olması, iş yapış şeklinin ve tüm süreçlerin ve organizasyonun bu risk farkındalığını besleyecek şekilde tasarlandığı ortamları anlatır.

Risk Profili; bankanın maruz kaldığı ya da kalmayı beklediği risk türlerini ve risk türü bazındaki risk düzeyini anlatır.

Risk Yönetimi; risklerin tanımlanması, değerlendirilmesi ve etkisinin kabul edilebilir bir seviyede tutulabilmesi için gerekli kontrollerin uygulanması, gözden geçirilmesi ve raporlanmasını sağlayan yönetim sürecini anlatır.

Üst Düzey Yönetim; bankalarda, genel müdür ve genel müdür yardımcıları, şube bankalarında Kuzey Kıbrıs ülke/genel müdürü ve Kuzey Kıbrıs ülke/genel müdür yardımcılarını veya bunlara muadil icrai nitelikte görev yapanları anlatır.

Üst Yönetim; bankalarda yönetim kurulu üyesi, üst düzey yönetici veya bunlara muadil konumlarda yönetici olarak görev yapanları anlatır.

Yasa; 62/2017 sayılı Kuzey Kıbrıs Türk Cumhuriyeti Bankacılık Yasasını anlatır.

Yasal Risk; mevzuata uyumsuzluk veya aykırılık nedeniyle mahkeme veya karşılıklı anlaşma yoluyla sonuçlanan ihtilaflardan yahut bankanın bir şikayet olmaksızın geri ödemeler veya müşteriye gelecekte sunulacak hizmetlerde indirimler gibi gönüllü eylemlerinden kaynaklanan gider/zarar riskini anlatır.

Yönetim Kurulu; bu Rehber amaçları bakımından Kuzey Kıbrıs Türk Cumhuriyetinde kurulu bankalar için yönetim kurulunu, şube bankaları için müdürler kurulunu anlatır.

## BİRİNCİ KISIM
GENEL İLKELER

### 1.1. ÜST YÖNETİMİN GÖZETİMİ

**İlke – 1 Bankalar yönetim kurulu onayı ile yürürlüğe konulan operasyonel riskinin yönetimine ilişkin yazılı strateji, politika ve süreçler oluşturur. Yönetim kurulu, üst düzey yönetimin bu strateji, politika ve süreçlere uygun ve uyumlu olarak riskleri izlemesini ve kontrol altında tutmasını ve operasyonel riskini kontrol etmeye ve değerlendirmeye yönelik yeterli kaynak bulundurmasını sağlar.**

1. Operasyonel risk yönetimi, bankanın maruz kaldığı operasyonel risklerin tutarlı ve kapsamlı bir şekilde tanımlanması, ölçülmesi, değerlendirilmesi, kontrol edilmesi, azaltılması, izlenmesi ve raporlanması süreçlerini kapsamalıdır. Bankalar aşağıdaki ana bileşenleri dikkate alarak operasyonel risk yönetimi sürecinin yazılı süreçlerini oluşturmalıdır.
   -Yönetim kurulu, üst düzey yönetim, birimler, merkezi operasyonel risk yönetimi birimleri, iç sistem birimleri dâhil organizasyon yapısı,
   -Bankada yerleşik risk kültürü,
   -Operasyonel risk yönetimi stratejileri, politikaları ile yazılı süreçleri ve
   -Operasyonel riskin tespit edilmesi, ölçülmesi, değerlendirilmesi, izlenmesi, kontrol edilmesi/azaltılması ve raporlanması sürecini içeren operasyonel risk yönetimi süreci.

2. Bankalar operasyonel riski geniş bir perspektifte ele almalı ve operasyonel risk yönetimi uygulamalarını aşağıda yer alan faktörler gibi faktörleri dikkate alarak geliştirmeli ve operasyonel risk düzeylerini etkileyen iç ve dış faktörleri sürekli olarak gözden geçirmelidir;
   -Banka içi kontrollerdeki aksamalar sonucu hata ve usulsüzlüklerin gözden kaçması,
   -Banka yönetimi ve personeli tarafından zaman ve koşullara uygun hareket edilmemesi,
   -Banka yönetiminde hatalar yapılması,
   -Bilgi işlem sistemlerinde hata ve aksamalar olması,
   -Deprem, yangın, sel gibi felaketlerden kaynaklanabilecek kayıplar oluşması ve
   -Banka veya sektör bazında ortaya çıkabilecek diğer faktörleri içermelidir.

3. Genel sektör uygulamalarında sağlam bir operasyonel risk yönetiminin üçlü savunma hattı yaklaşımı olarak adlandırılan metod doğrultusunda oluşturulduğu görülmektedir. Üçlü savunma hattı aşağıdaki bölümlerden oluşmaktadır;

3.1. Birim Yönetimi; bankanın büyüklüğü ve faaliyet yapısı söz konusu üçlü yapının uygulanma düzeyini belirlemekte olup birim yönetimleri her faaliyet birimi nezdinde bulunan ürün, süreç, faaliyet ve sistemlerden kaynaklanan risklerin tespit edilmesi ve yönetilmesi konusunda sorumluluk üstlenmektedir. Bu aşamada her bir birim yönetimi altındaki süreç, faaliyet ve sistemlerden kaynaklanan operasyonel risklerin tespit edilmesi, üst düzey yönetimin bilgilendirilmesi ve uygun aksiyonların alınmasını sağlama konularında sorumlu ve yükümlüdür. Birim yöneticileri, kendilerine bağlı birimlerin, operasyonel riske yönelik üst düzey yönetim tarafından belirlenen politika ve iş akış süreçlerine uyumlu faaliyet göstermelerini sağlamakla ve gerektiği ölçüde alt düzey için ek politika ve süreçleri oluşturmakla sorumludurlar.

3.2. Merkezi Operasyonel Risk Yönetimi Fonksiyonu; faaliyet birimlerinde gerçekleştirilen yönetim sürecinin tamamlayıcısı konumundadır. Bağımsızlık düzeyi bankanın büyüklüğüne göre değişmekte olup küçük bankalarda görev ve sorumlulukların ayrıştırılması ile süreç ve fonksiyonların onları icra edenler dışındaki kişiler tarafından gözden geçirilmesi, büyük bankalarda ise merkezi yapının banka nezdinde bağımsız operasyonel risk yönetim sürecinin oluşturulması ve geliştirilmesi şeklinde sorumlulukları olarak ele alınması gerekmektedir. Bu risk yönetimi kapsamında riskin ölçümü, bankanın çeşitli birimlerinden raporlar almak ve risk birimine ve yönetim kuruluna raporlama yapmak şeklinde süreçler oluşturulur. Bankaların iç sistem birimleri merkezi operasyonel risk yönetiminin önemli bir parçasını oluşturmaktadır.

3.3. Bağımsız Gözden Geçirme; banka iç sistem birimleri veya banka dışı yeterli niteliğe sahip kişiler/üçüncü taraflar tarafından da yerine getirilir. Bağımsız gözden geçirme aşağıdaki bileşenleri içermektedir;

3.3.1. Operasyonel Risk Çerçevesinin Yeterliliğine İlişkin Değerlendirme; bankanın iç sistem birimleri tarafından düzenli aralıklarla gerçekleştirilir. Değerlendirme sürecine banka dışından uygun görüldüğü takdirde nitelikleri haiz bağımsız taraflar da katılabilmektedir. Değerlendirme faaliyetinde genel operasyonel risk yönetiminin etkinliği ile yönetim kurulu tarafından onaylanan süreçlerle olan uyumu, doğrulama süreçlerinin bağımsızlığı ve operasyonel risk yönetimi uygulamasının bankanın mevcut politikaları ile tutarlı bir şekilde yapılıp yapılmadığı incelenmektedir.

3.3.2. Model Doğrulaması; banka tarafından riskin sayısallaştırılması için kullanılan sistemlerin yeterli nitelikte olduğu hususunda güvence veren bir sistemdir. Ayrıca doğrulamanın, sistemlerin girdileri, varsayımları, süreçleri ve çıktıları arasında sağladığı uyumun seviyesi konusunda görüş veren bir sistem olduğu göz ardı edilmemelidir. Bağımsız doğrulama süreci, risk ölçüm sonuçlarının, bankanın operasyonel risk profiline uygun bir sermaye yükümlülüğü hesaplayıp hesaplamadığına dair güvence vermekle mükelleftir. Bankanının iç işleyişi ile ilgili doğrulamada önemli olan hususlar, sayısal hesaplamaya ilişkin yöntemlerin incelenmesi, veri girişlerinin doğrulaması, operasyonel risk modellerinin metodolojisi ve sistem çıktılarından oluşmaktadır.

4. Sağlam bir operasyonel risk yönetiminin en önemli karakteristik özelliği, üçlü savunma fonksiyonu ile operasyonel risk arasında iyi bir altyapının kurulmuş olması ve bu alt yapının bankalarda güçlü bir risk kültürünün oluşmasına destek sağlamasıdır.

5. Sağlam bir operasyonel risk yönetimi, bankanın her bir biriminin riskin yönetiminde sorumluluk sahibi olmaları ve tüm personelin görev alanıyla ilgili olarak bankanın maruz kaldığı operasyonel risk düzeyi hakkında bilinçli ve bu gibi durumlarda operasyonel riskleri tespit edebilecek yeterliliğe sahip olmalarını gerektirmektedir.

6. Yönetim kurulu operasyonel risk yönetimine ilişkin politika, süreç ve sistemlerin tüm karar aşamalarında ve faaliyetlerde etkin bir şekilde uygulanmasının gözetiminden yeni ürün geliştirme sürecinde üründen kaynaklı ortaya çıkabilecek operasyonel riske ilişkin değerlendirme aşamasının oluşturulması, iç sistem birimlerine bağlı personelin görevlerinin icrası sırasında bağımsız hareket edebilmelerinin sağlanması dâhil sorumludur.

7. Yönetim kurulu sağlam bir operasyonel risk yönetimi oluşturmak amacıyla;

7.1. Risk kültürünün yerleşmesini sağlayacak önlemler geliştirmeli, gözetim sorumluluğunu yerine getirebileceği süreçleri oluşturmalı, bankanın strateji ve faaliyetlerinden kaynaklanan riskleri anlamalı ve bankanın tüm risk yönetim sistemine bütünüyle dâhil edilmiş kapsamlı dinamik bir kontrol sistemi oluşturmalı,

7.2. Operasyonel risk yönetimi doğrultusunda somut olarak yönlendirilmeli, üst düzey yönetim tarafından hazırlanan süreç ve politikaların uygunluğunu değerlendirerek onaylamalı ve bunların uygunluğunu belirli aralıklarla gözden geçirmeli,

7.3. Üst düzey yönetim tarafından politikalara uygun aksiyonların gerekli durumlarda yeterli etkinlikte alınıp alınmadığını kontrol etmeli,

7.4. 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 yönetimini düzenli olarak gözden geçirmeli ve

7.5. Bağımsız üçüncü taraflar veya iç sistem birimleri tarafından da operasyonel risk yönetiminin gözden geçirilmesini sağlamalıdır.

8. Banka, operasyonel risk yönetim sürecinde politikalar oluşturmalı, yönetim kurulu tarafından onaylanmasını sağlamalı ve düzenli aralıklarla gözden geçirilmelidir. Bu politikalar, operasyonel riskin yönetimi ve kontrolü de dâhil olmak üzere bankanın stratejisini ve süreçlerini yansıtmalıdır. Yönetim kurulu, banka yönetiminin bu strateji, süreç ve politikaları etkin olarak uygulamasını ve bütünüyle bankanın risk yönetimine dâhil etmesini sağlamalıdır.

9. Etkin bir kontrol çevresi, merkezi operasyonel risk yönetimi fonksiyonu ile iş birimleri ve iç sistem birimleri arasında yeterince ayrıştırılmış, açık ve anlaşılır görev tanımlarının bulunmasını gerektirmektedir. Sağlam bir operasyonel risk yönetim sürecinin oluşturulabilmesinde, banka genelinde operasyonel riskin yönetimine ilişkin görev ve sorumlulukların açıkça tanımlandığı etkin bir kontrol çevresinin oluşturulması kritik öneme haiz olup bu husus yönetim kurulunun sorumluluğundadır.

**İlke – 2 Üst düzey yönetim, bankanın risk iştahı ve risk kapasitesi ile uyumlu olarak tüm faaliyet, iş süreci ve ürünlerde operasyonel risk yönetim sürecinin tutarlı ve etkin bir şekilde uygulanmasından ve sürdürülmesinden sorumludur.**

10. Operasyonel riskin yönetimi kapsamında bankalar, yaşanan gelişmeleri izler, değerlendirir ve uygun önlemleri alır.

11. Bankanın çeşitli faaliyetlerinin fiyatlama ve performans ölçümünde operasyonel risk faktörünün uygun biçimde dikkate alınmasının sağlanması üst düzey yönetimin sorumluluğundadır. Operasyonel riskin dikkate alınmaması, bankanın risk iştahı ve risk kapasitesi ile uyumsuz düzeyde risk almasına neden olabilir.

12. Bilanço kalemlerine ilişkin değerleme uygulamalarında ve risk ölçümü öncesi yapılan değerlemeler hakkında benimsenen yaklaşım, metod ve menkul kıymetlerin değerlemesinde kullanılan verim eğrisi gibi varsayımların üst düzey yönetim tarafından hazırlanacak süreç kapsamında yazılı hale getirilmesi ve yönetim kuruluna onaylatılması esastır.

13. İç sistem birimleri, banka nezdinde uygulanan operasyonel risk yönetimi sürecinin tüm yönleriyle, bağımsız olarak değerlendirilmesinden sorumludur.

14. İç sistem birimleri, operasyonel risk yönetimi politika ve süreçlerinin banka genelinde etkin bir şekilde uygulanıp uygulanmadığını ortaya koyabilmek için yeterli kaynağa ve yerinden denetim yapısına sahip olmalıdır. Yönetim kurulu bu çerçevede iç sistem birimlerinden iç denetim tarafından belirlenen denetim programının kapsamı ve sıklığını bankanın maruz kaldığı operasyonel risk düzeyine uygun olduğunun sorumluluğunu sağlamakla yükümlüdürler. Denetim sürecinde tanımlanan ve raporlanan her bir operasyonel riskin konusu bankanın üst düzey yönetimi tarafından zamanında ve etkili bir şekilde ele alınmalı ve uygun olduğu ölçüde yönetim kurulunun dikkatine sunulmalıdır.

**İlke – 3 Bankalar oluşturdukları operasyonel risk yönetimi süreciyle banka genelinde yerleşik bir risk kültürünün oluşmasını sağlamalıdırlar. Yönetim kurulu ve üst düzey yönetim, bu yükümlülüğün yerine getirilmesinde öncü rol üstlenmeli, amaca yönelik olarak bankanın taşıdığı operasyonel riskin temel unsurlarının farkında olmalı ve bu riski yönetilmesi gereken ayrı bir risk olarak görmelidir.**

15. Bu kapsamda belirlenecek politikalar, süreçler ve sistemler, verilecek meslek içi eğitimler, oluşturulacak etkin iç sistem birimleri kontrol mekanizmaları bankada risk yönetimi bakış açısına sahip güçlü bir kurumsal kültürün oluşturulmasını, tüm birim ve faaliyetlere operasyonel risk yönetim kültürünün dâhil edilmesini sağlamalıdır.

16. Yönetim kurulu tarafından ücretlendirme politikalarının belirlenmesi önem arz etmektedir. Banka nezdinde uygulanan ücretlendirme politika ve süreçleri, bankanın risk iştahı, risk kapasitesi, finansal hedefleri ve uzun vadeli stratejileri ile uyumlu olmalıdır.

17. Üst düzey yönetim 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.

### 1.2. RİSKİN YÖNETİMİNE İLİŞKİN POLİTİKALARIN VE SÜREÇLERİN OLUŞTURULMASI

18. Bankalar, operasyonel risk, strateji ve politikalarını uygulamak için uygun yazılı süreçler geliştirmelidir. Süreçler, ilgili operasyonel risk kontrollerini gerçekleştirmek için gerekli iş akışlarını ayrıntılı bir şekilde açıklamalıdır. Üst düzey yönetim bankada, açık bir yetki-sorumluluk dağılımı ve raporlama hiyerarşisi oluşturmalı ve operasyonel riskin yönetim kurulu tarafından yazılı olarak belirlenmiş risk iştahı ve risk kapasitesine uyumlu olarak yönetilmesini sağlamalıdır.

19. Üst düzey yönetim operasyonel riskin tespiti/tanımlanması, ölçülmesi, izlenmesi ve kontrol edilmesi için gerekli teknik uzmanlık ve deneyime sahip personel istihdam edilmesini sağlamalıdır. Kilit öneme sahip personelin geçici eksikliği durumunda faaliyetlerin aksamadan devam etmesini sağlayacak nitelik ve sayıda personel bulundurularak uygun iş bölümü belirlemelidir. Strateji, politika ve süreçlerin ilgili banka personeline duyurulması amacıyla banka bilgi işlem sisteminde gerekli yazılımsal

altyapı kurulmalı, altyapı sürekli olarak ilgili personelin kullanımına açık tutulmalı ve bunların personel tarafından anlaşıldığından emin olunmalıdır.

20. Süreçler düzenli olarak gözden geçirilmeli ve yeni faaliyetler, sistemlerdeki önemli değişimleri bilgi yönetim, raporlama, risk yönetimi, ödeme ve takas ve benzeri gibi ve piyasadaki yapısal değişimler dikkate alınarak güncellenmelidir. Süreçler, operasyonel risk doğuran bütün faaliyetleri kapsamalıdır.

21. Bankadaki birimlerin yöneticileri, kendi birimlerindeki faaliyetlerden kaynaklanan risklerin yönetiminde ilk aşamadaki sorumlulardır. Bundan dolayı, her bir birimin kendi alanına özgü ve bankanın operasyonel risk çerçevesiyle uyumlu olan ilave politika ve süreçleri oluşturması beklenmektedir.

22. Operasyonel risk yönetimi altında oluşturulan politika ve süreçlerde asgari olarak uygulaması gereken unsurlar;

22.1. Yaşanan veya yaşanması muhtemel iç ve dış olaylardan hareketle bankaya özgü operasyonel riskin tanımlanmasında, derecelendirilmesinde ve risk yönetimi amaçlarına ulaşmada tutarlılığı sağlamak üzere operasyonel risk terimleri için ortak bir sınıflandırma ve tanımlama sistematiği geliştirilmeli, bankanın maruz kaldığı operasyonel risk ve kayıp çeşitlerini yeterli kapsam ve içerikte somut olarak tanımlaması ve sınıflandırması, riskin sayısallaştırılmasını ve yönetilmesine yönelik temel unsurları içermelidir.

22.2. Operasyonel riskin bileşenlerinden yeni müşteri, ürün ve bilgi yönetimi sistemlerinin onaylanması, destek hizmeti kullanımı, iş sürekliliği planları, asgari kriz yönetimi ve kara para aklama gibi konulara yönelik kurallara yer vermelidir.

22.3. Riskin yönetimi kapsamında uygulanan raporlama sürecinin ve ilgili taraflara düşen sorumlulukların açıkça belirlendiği organizasyon yapılarını oluşturmalıdır.

22.4. Riskin ölçümü ve değerlendirilmesi için kullanılan yöntemler ve bu yöntemlerin kullanım bilgileri bulunmalıdır.

22.5. Bankanın yazılı stratejisinde yer alan operasyonel risk iştahı ve risk kapasitesi çerçevesinde, doğrudan veya dolaylı olarak maruz kalabileceği operasyonel riske ilişkin limitler, onaylanmış risk azaltma yöntemleri ve ilgili diğer hususlar tespit edilmelidir.

22.6. Bankanın maruz kaldığı operasyonel riske yönelik limit takip süreci bulunmalıdır.

22.7. İzleme ve raporlama sürecinde kullanılan yönetim bilgi işlem sistemi altyapısı kurulmalıdır.

22.8. Bağımsız tarafların operasyonel riske ilişkin değerlendirme ve denetim yapmalarını sağlayacak süreçler var olmalıdır.

22.9. Bankanın operasyonel risk profilinin önemli ölçüde değiştiği durumlarda politikaların gözden geçirilmesi veya güncellenmesi mutlaka yapılmalıdır.

### 1.3. DİKKATE ALINMASI GEREKEN ÖZEL HUSUSLAR

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

### 1.3.1. Yeni Ürün ve Faaliyetler

23. Operasyonel risk düzeyi bankanın yeni faaliyetler veya yeni ürünler geliştirdiği dönemlerde ve özellikle faaliyet ve ürünlerin bankanın temel yapısına yabancı olduğu durumlarda belirgin olarak yükselmektedir. Banka yeni ürün/faaliyet onaylama süreçlerini belirli standartlar altında yazılı politika ve süreçlere dayandırmalı, ürün ve faaliyete ilişkin görev ve sorumlulukları açık bir biçimde tanımlamalıdır. Bu politika ve süreçlerin temel amacı, yeni bir girişimin veya mevcut faaliyet yapısındaki değişikliğin kontrollü olarak uygulamaya geçirilmesi ve ilgili birimlerinin uygulama sürecine hazır hale getirilmesidir.

24. Bankanın yeni ürün, faaliyet, süreç ve sistemler dolayısıyla maruz kalacağı muhtemel risk türleri ve düzeyleri özel olarak değerlendilmelidir. Değerlendirme ve onaylama süreci asgari olarak

    -Yeni ürün, hizmet ve faaliyetin doğuracağı muhtemel riskleri,

    -Yeni ürünlerin değerlemesi yapılırken ortaya çıkabilecek zorlukları,

    -Ekonominin stres dönemlerinde söz konusu değerlemeleri,

    -Bankanın mevcut operasyonel risk profili, risk iştahı ve risk kapasitesinde yaratacağı değişiklikleri,

    -Uygun olan kontrol ve risk yönetim süreçleri ile risk azaltma stratejilerini,

    -Kontrol sonrası ortaya çıkacak artık riskleri,

    -İlgili eşik değer ile limitlerde değişikliği ile

    -Yeni ürün ve faaliyetlerden kaynaklanacak risklerin ölçümünde, izlenmesinde ve yönetiminde kullanılacak süreçler ve ölçüm yöntemlerini açıklığa kavuşturmalıdır.

### 1.3.2. Bilgi Teknolojileri Güvenliği ve Değişimleri

25. Bilgi teknolojileri imkânlarının yaygın kullanımı, bankanın etkin bir kontrol sistemine sahip olmasını sağlamaktadır. Fakat ürünlerin sunumunda, faaliyet ve süreçlerde ya da hizmet dağıtım kanallarında kullanılan teknolojik altyapılar bankanın stratejik, operasyonel, itibar dâhil risklere veya maddi kayıplara maruz kalmasına sebep olabilmektedir. Bu nedenle bankanın; oluşturacağı 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;

    -Alınan destek hizmetleri 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, risk kapasitesinin ve performans beklentilerinin oluşturulması,

    -Risklerin tespit edilmesi ve değerlendirilmesine imkân sağlayan politika ve süreçlerin belirlenmesi,

-Politika ve süreçler kapsamında etkin bir kontrol çevresinin oluşturulması ve risk transfer-azaltma stratejilerinin ortaya konulması gereken durumlarda uygulamaya sokulması ve

-Belirlenen eşik değerler ve limitlere uyum düzeyinin izlenmesi unsurlarını içermektedir.

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

27. Banka üst düzey yönetimi, bankanın normal şartlar altındaki faaliyet düzeyinin yanı sıra stresli piyasa koşulları altında faaliyetlerinde aksamaya yol açmayacak, mevcut ve uzun vadeli faaliyet planlaması için yeterli kapasiteye haiz bir teknoloji altyapısına sahip olmasını sağlamakla yükümlüdür. Bu altyapı, gerekli verilerin sağlanmasına, sistem bütünlüğüne, güvenliğine, sisteme zamanında ulaşılabilirliğe, kapsamlı risk yönetimine ve yetkili üçüncü taraflar tarafından talep edilen bilgilerin esnek bir biçimde istenilen şekil ve içerikte sunulabilmesine imkân sağlamalıdır.

### 1.3.3. Alternatif Dağıtım Kanalları

28. Alternatif dağıtım kanallarından 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 önlenmesini konu alan müşteri güvenliği uygulamaları ve riskin yönetimini amaçlayan diğer kontrolleri içermelidir.

### 1.3.4. Destek Hizmetleri

29. Bankaların, destek 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 ve beklenmedik 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 süreçler geliştirmekle sorumludur.

30. Bankanın destek hizmeti alımından kaynaklı riskleri yeterli ölçüde yönetemediği, ancak hizmet alımının durdurulmasının makul bir seçenek olarak görülemeyeceği durumlarda banka üst düzey yönetimi, kontrol zaafiyetlerini ortadan kaldırmak amacıyla maruz kaldığı riskleri üçüncü bir tarafa transfer edebilir. Yönetim kurulu bu durumda bankanın finansal gücünü dikkate alarak yönetebileceği azami 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.

### 1.3.5. Kara Paranın Aklanması

31. Banka, kara paranın aklanması ve terörün finansmanı ile mücadele kapsamında müşterini tanı, mevzuata uyum, yasal otoritelerle işbirliği ve sürekli personel eğitimleri ve bunun gibi hususlarda politika, süreçler ve kontroller geliştirmekle mükelleftir.

### 1.3.6. Uygun Müşteri Seçimi

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

### 1.3.7. Yurtdışı Şubeler ve İştirakler

33. 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 sisteminde mümkün olan en üst seviyede bütünüyle izleyebilmeli, faaliyet süreçlerini yeterli kapsam ve içerikte dokümante etmeli, meydana gelen değişimlerin etkilerini anlamalı ve yurtdışı operasyonları üzerinde uygun kontrol mekanizmalarını geliştirmelidir.

### 1.3.8. Dış Dokümantasyon

34. Dış dokümantasyon, bankalar tarafından düzenlenerek müşterilere, üçüncü taraflara veya herhangi bir karşı tarafa sunulan ve bankaya hak/yükümlülük getiren dokümanları 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;

    -Yasal mükellefiyetlere uygunluk,

    -Dokümanlarda kullanılan standart ve standart olmayan terimlerin kapsamı,

    -Dokümanların yayımlandığı kanallar,

    -Onay mekanizmasının uygunluğu ve

    -Sözleşmenin banka tarafından hazırlanan standart sözleşme tiplerine uygunluğu bazında kontrol edilmesi uygun olacaktır.

## İKİNCİ KISIM
RİSK ÖLÇÜM SÜREÇLERİNİN YÖNETİMİ

**İlke – 4 Bankalar, ürünleri, faaliyetleri, süreçleri ve sistemleri dolayısıyla maruz kaldıkları operasyonel riskin düzenli olarak ölçülmesi, değerlendirilmesi, izlenmesi ve kontrolüne yönelik bir risk yönetim sürecine ve yeterli kaynaklara sahip olmalıdır.**

35. Kredi riski ve piyasa riskine benzer şekilde operasyonel riskin yönetimi de bağımsız ve merkezi bir birim tarafından icra edilmelidir. Birimin temel sorumluluğu, maruz kalınan operasyonel risklerin anlaşılması ve yönetilmesi kapsamında üst düzey yönetime ve risk yönetimi faaliyetlerinin izlenmesi kapsamında yönetim kuruluna rapor hazırlamak ve sunmaktır.

36. Banka, tüm faaliyetlerinin büyüklüğüne ve karmaşıklığına uygun olarak operasyonel riskin ölçülmesi, izlenmesi ve kontrolüne yönelik bir sistem oluşturur.

37. Risk yönetim birimi tarafından yerine getirilmesi gereken görevler aşağıdaki gibidir;

37.1. Solo ve konsolide düzeyde operasyonel risk yönetimi ve kontrolleriyle ilgili politika ve süreçlerin oluşturulmasında üst düzey yönetime yardımcı olmak,

37.2. Operasyonel risk yönetimi politikalarının ve süreçlerinin banka genelinde tutarlı bir şekilde uygulanmasına yönelik izleme yaparak yönetim kuruluna sunulmak üzere solo ve konsolide bazda raporlar hazırlamak,

37.3. Bankanın solo ve konsolide bazda maruz kaldığı operasyonel risk düzeyine ilişkin ölçümler ve değerlendirmeler yaparak üst düzey yönetimi bilgilendirmek,

37.4. Bankanın operasyonel risk ölçüm ve değerlendirme araçları ile risk raporlama sistemlerini tasarlayarak uygulamaya koymak,

37.5. Banka tarafından yürütülen genel risk yönetimi faaliyetleriyle operasyonel risk yönetimi uygulamaları arasında koordinasyonu sağlamak,

37.6. Operasyonel risk yönetimi eğitimleri düzenlemek ve faaliyet birimlerine maruz kaldıkları operasyonel riskin yönetimi kapsamında danışmanlık yapmak ve

37.7. Banka nezdinde denetim gerçekleştiren iç sistem birimleri ve dış hizmet alımı yapılan kuruluşlarla düzenli bilgi alışverişi gerçekleştirmektir.

### 2.1. RİSK ÖLÇÜMÜ

**İlke – 5 Bankalar, uluslararası faaliyetlerinin büyüklüğüne ve karmaşıklığına uygun olarak operasyonel riskin ölçülmesi, izlenmesi ve kontrolüne yönelik bir sistem oluşturur. Üst düzey yönetim tüm önemli ürün, aktivite, süreç ve sistemlerdeki operasyonel risklerin tespit edilmesi ve değerlendirilmesinden sorumludur.**

38. Banka, operasyonel risk profilini en doğru şekilde ortaya koymak ve sahip olduğu kaynakları en uygun şekilde risk yönetimine tahsis edebilmek amacıyla, öncelikle maruz kaldığı operasyonel risk çeşitlerini mümkün olan en somut biçimde tespit etmeli ve 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. Bu faktörlerden bazıları aşağıdaki gibidir;

-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 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 edilmesinden sonra 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 aşağıdaki gibidir;

41.1. **Denetim Bulguları;** iç ve dış denetimlerde elde edilen bulgular, esas olarak banka faaliyetlerindeki kontrol zaafiyetlerine ve güvenlik açıklarına odaklanmakla birlikte maruz kalınan operasyonel risk düzeyinin belirlenmesi sürecinde önemli girdilerdir.

41.2. **Banka İçi Kayıp Verilerin Toplanması ve Analizi**; operasyonel anlamda kayıp veriler bir bankanın iç sistem birimlerinin bu anlamdaki iş süreçlerinin etkinliğinin ve maruz kaldığı operasyonel risk düzeyinin belirlenmesinde anlamlı girdiler sağlamaktadır. Kayıp veri olaylarının analiz edilmesi, kontrol hatalarının olay bazında mı, yoksa sistematik bir hatadan mı kaynaklandığı gibi hususlarda bu kayıpların nedenleri ile ilgili bilgi edinilerek anlaşılmasını sağlamaktadır.

41.3. **Banka Dışı Verilerin Toplanması ve Analizi**; bankanın dışındaki kuruluşlarda gerçekleşen brüt operasyonel kayıp tutarları, kayıp yaşanan tarihler, sigorta, personelden tahsil ve benzeri durumlardaki tazmin tutarları ve kayıpların nedenlerinden oluşmaktadır. Banka dışı veri kayıpları, banka içi veri kayıpları ile karşılaştırılarak bankanın kontrol çevresindeki muhtemel zayıflıkların tespit edilmesinde ya da daha önce tanımlanamayan risk faktörlerinin tespitinde kullanılmaktadır.

41.4. **Risk Değerlendirmesi;** bankanın operasyonel riske ilişkin kendi iç 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 iç sistem birimleri dâhil birimlerinin gerçekleştirdiği kontrolleri içeren risk kontrol sürecini de değerlendirmesi gerekmektedir. Bu kapsamda banka, kontrol öncesi risk düzeyini değerlendirir, kontrol çevresinin etkinliğini gözden geçirir ve kontrol sonrası geriye kalan risk faktörlerini içeren artık riskleri belirler. Böylece riskler banka tarafından ağırlıklandırılabilmekte ve skor kartlar

kullanılabilmektedir. Bu sistem, değerlendirme sonuçlarının metrik sisteme aktarılmasını sağlayarak, kontrol çevresinde kullanılabilecek bir derecelendirme imkânı sağlamaktadır.

41.5. **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. Her bir alt faaliyetin iş ve işlemlerinin icra edilme yöntemlerini gösteren iş akış şemaları da bu haritanın tamamlayıcı unsuru olmaktadır. Bankanın söz konusu haritaları, belirlenen kurallar çerçevesinde bilgi işlem sisteminin desteği ile ilgili personelin bilgisine sunmalıdır. Bu süreç 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.

41.6. **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 faydalı olmaktadır. 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 gibi sayısal ağırlıklı operasyonel risklerin tespit edilmesini ve değerlendirilmesini sağlamaktadır. Risk göstergeleri, temel risklere ilişkin muhtemel etkenlerin izlenmesinde kullanılmakta olup performans göstergeleri ise operasyonel zayıflık, hata ve kayıplar yaşanan iş süreçlerinin mevcut durumu hakkında anlamlı bilgiler sağlamakta kullanılmaktadır. Her iki gösterge de risk seviyelerinin belirlenen limitlere yaklaştığı veya aştığı ve acil risk azaltma gerektiren tetikleyici seviyelerde bir uyarı mekanizması işlevi görmektedirler.

41.7. **Senaryo Analizleri;** banka, birimlerinde 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 azaltma için gereksinimin belirlenmesinde etkili bir araçtır. Senaryo analizlerinin sübjektif olma özelliği göz önünde bulundurularak, analiz sürecinde etkinliğin, tutarlılığının ve objektifliğin sağlanması amacıyla banka tarafından ilave önlemler alınması uygun olacaktır. Bankanın risk yönetimi uygulamalarında yer vereceği senaryo analizlerine ilişkin kapsamlı açıklamalar "Bankaların Sermaye ve Likidite Planlamasında Kullanacakları Stres Testlerine İlişkin İyi Uygulama Rehberi"nde yer alacaktır.

41.8. **Risk Ölçümü;** banka, banka içi kayıp verileri, denetim bulguları, senaryo analizleri ve buna benzer risk değerlendirme araçlarının çıktılarını, operasyonel risk ölçümü yapılan modelde girdi olarak kullanmak suretiyle maruz kaldıkları operasyonel risk düzeyini sayısallaştırılmalıdır. Modelin sonuçları bankanın ekonomik sermayesinin hesaplanması sürecinde ve risk-getiri ilişkisine göre birim bazında yapılacak değerlendirmelerde kullanılabilmekte olup 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 gerekmektedir. Kayıp olaylarına ilişkin banka tarafından oluşturulan veri tabanı; ampirik analizlerde, model kurulmasında ve birbiriyle ilişkili kayıp olaylarının sayısallaştırılmasında kullanılabilmektedir.

41.9. **Karşılaştırmalı Analizler;** bu tür analizler bankanın risk profiline ilişkin kapsamlı bir değerlendirme yapmak üzere muhtelif değerlendirme araçlarından elde edilen sonuçların karşılaştırılması temeline dayanmaktadır. Senaryo analizinde kullanılan verilerin, iç ve dış verilerle karşılaştırılması sayesinde bankanın maruz kalabileceği riskin büyüklüğünü daha iyi görülebilmesini sağlamaktadır.

## ÜÇÜNCÜ KISIM
İZLEME SÜREÇLERİNİN YÖNETİMİ

### 3.1. RİSK İZLEME SÜRECİ ve LİMİTLERE UYUM

**İlke – 6 Yönetim kurulu bankanın operasyonel riskine ilişkin genel, ürün, birim ve bunun gibi alt unsurlar bazında risk iştahı ve risk kapasitesini, çeşitli eşik değerler, rasyolar ve limitler bağlamında belirlemeli ve gözden geçirmeli, bu işlevleri yerine getirebilmesi için gerekli sistem ve süreçleri oluşturmalıdır.**

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

43. Yönetim kurulu belirlenen 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 azaltma 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.

44. Yönetim kurulu, operasyonel riskin yönetiminden sorumlu personel ile üstlenilen riskler, piyasa ve destek hizmetlerinden kaynaklanan riskler de dâhil diğer risklerin 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.

**İlke – 7 Bankalar operasyonel risk profillerini ve maruz kaldıkları kayıpları düzenli olarak izlemek amacıyla süreç ve sistem belirlemelidir.**

45. Operayonel riskin izlenme süreci bankanın maruz kaldığı her türlü operasyonel risk türlerine yönelik nitel ve nicel değerlendirmeleri, alınan düzeltici önlemlerin ve risk azaltma kapsamındaki aksiyonların kalitesinin ve uygunluğunun değerlendirilmesini, yeterli oranda kontrol noktasının etkin olarak devrede olup olmadığının gözden

geçirilme uygulamalarını içermelidir. Oluşturulan süreç aynı zamanda bankanın ölçeğine, risk profiline ve faaliyet yapısına uygun olmalıdır.

46. 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 birimler tarafından düzenli olarak izlenir. Temel göstergeler şeklinde belirlenen 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 verebilecektir.

47. Operasyonel riskin izlenmesi süreci, banka faaliyetlerine bütünüyle dâhil edilmeli ve bu kapsamda her bir birimin operasyonel risk oluşturma potansiyeli değerlendirilmeli, değerlendirme sürecinde faaliyet gösterilen iş süreçlerindeki değişikliklerin sıklığı ve özellikleri de dikkate alınmalıdır.

### 3.2. RİSKİN ANALİZİ ve RAPORLANMASI

**İlke – 8 Bankalar, operasyonel riske ilişkin analiz çalışmaları yapar. Bu çalışmalarda tehdit oluşturabilecek olayların gerçekleşme olasığı analiz edilerek, risklerin değerlendirme süreçlerinde dikkate alınması için yönetim kuruluna sunulur.**

48. 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 yurtiçi ve yurtdışı piyasa koşulları hakkında bilgiler yer almalıdır. Bu raporlamanın temel amacı, banka yönetimine bankanın operasyonel risk profilini ve doğurduğu etkileri yeterli kapsam ve içerikte anlaşılmasını sağlayacak bilgilerin sunulmasıdır. Bu raporlarda banka yönetim kurulunun, üst düzey yönetimin ve ilgili birimlerin özellikle bilgi sahibi olmasını amaçlayan hususlar aşağıdaki gibidir;

48.1. Bankanın karşı karşıya olduğu mevcut veya potansiyel, temel risk göstergelerinin doğrudan veya trend analizi yoluyla işaret ettiği olumsuz değişimler, denetim veya uyum raporlarında yer verilen değerlendirmeler dâhil kritik operasyonel riskler,

48.2. Önemli düzeyde risk doğuran olaylar, veri kaybı yaşanan tecrübeler, bunların nedenleri ve gerekli görülen iyileştirici önlemler,

48.3. Risk azaltma ve risk transfer stratejileri,

48.4. Alınan önlemlerin seviyesi ve/veya etkinlik düzeyi,

48.5. Yeni ürünlerden kaynaklanan operasyonel riske ilişkin bilgiler,

48.6. Zayıf alanların tanımlanması,

48.7. Operasyonel risk tutarlarının birimler arasındaki dağılımı, yönü ve geçişmeleri,

48.8. Bankanın risk iştahı, risk kapasitesi ve risk politikalarında bilinçli veya bilinçli olmayan sapmalar, operasyonel riske ve kayıp düzeylerine yönelik önceden tanımlanmış limit ve eşiklerde gerçekleşen veya gerçekleşmesi olası ihlaller gibi istisnai raporlamalar ve

48.9. Önem arz eden banka dışı olaylar ve bunların banka ve bankanın operasyonel risk sermayesi üzerindeki muhtemel etkileri.

49. Bankada risk izleme sürecinin tüm sonuçları, iç sistem birimleri tarafından tespit edilen bulgular, bağımsız dış denetçiler ve denetim otoritesi tarafından hazırlanan raporlar mümkün olduğu ölçüde, hazırlanan operasyonel risk yönetim/izleme raporunda yer almalıdır.

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

51. 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 dönemlerde mutat olarak yapılması esastır.

52. Bankanın halihazırdaki raporlama ve veri toplama süreçleri, mevcut risk yönetim performansının iyileştirilmesi ve risk yönetimi politika, süreç ve uygulamalarının geliştirilmesi amacıyla düzenli olarak gözden geçirilip iyi uygulamalar kapsamında takip edilmelidir.

53. Banka üst düzey yönetimi, operasyonel riskin yönetimine ilişkin raporlamaların kapsamlı, doğru, tutarlı ve kullanılabilir olmasını sağlamalıdır. Bu 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 yönelik ve güvenilir olmasını sağlamak üzere üst düzey yönetim, bankada oluşturulan raporlama sisteminin zamanlama tablosuna uyumunu, tam ve doğru bilgi sağlayıp sağlamadığını, farklı birimler tarafından hazırlanan raporlarda aynı başlıkta yer alan bilgilerin tutarlılığını, raporların ilgili mercilere zamanında ulaşmasını, banka ölçeği ve risk profiline uygunluğunu ve yapılan iç sistem birimleri kontrol faaliyetlerine ilişkin istatistikleri düzenli olarak gözden geçirmelidir.

## DÖRDÜNCÜ KISIM
KONTROL SÜREÇLERİNİN YÖNETİMİ

### 4.1. KONTROL FAALİYETLERİ

**İlke – 9 Bankalar, operasyonel riski izleyen ve raporlayan bir bilgi işlem sistemine, risk yönetimi sistemine ve kontrol sistemine sahip olmalıdır. Bilgi işlem sistemlerinin, belirlenen operasyonel limitleri güncel olarak izlemeye imkân verip vermediği ve gerekli durumlarda uygun önlemlerin alınmasını sağlayıp sağlamadığı düzenli olarak gözden geçirilir. Bankalar bu sistemden yaralanarak iç sistem birimleri kontrol faaliyetlerini, risk azaltma ve/veya transfer stratejilerinin uygulandığı güçlü bir operasyonel risk kontrol ve azaltma sürecini oluşturmak zorundadır.**

54. Banka nezdinde yerine getirilen iç sistem birimleri kontrol uygulamaları, banka operasyonlarının verimli ve etkili olmasına, personel hatalarının minimize edilmesine, varlıkların güvence altında tutulmasına, güvenilir finansal raporların üretilmesine, uyulması gereken mevzuata uyum gösterilmesine imkân sağlamalıdır.

55. Oluşturulan kontrol süreçleri, banka politikalarına uyum düzeyini arttırmaya yönelik, herhangi bir iş sürecinde yapılan işlemler ile bahse konu iş sürecine ilişkin süreçte öngörülen işlemler arasındaki uyumsuzlukları konu eden farklılık raporları gibi uygulamaları içermelidir. Politikalara uyum düzeyinin değerlendirilmesi kapsamında aşağıdaki unsurların dikkate alınması yararlı olacaktır;

55.1. Belirlenen hedeflere yönelik işleyen sürecin, banka üst düzey yönetimi tarafından sürekli olarak takip edilmesi,

55.2. Uyum sağlanmamış noktalara ilişkin olarak alınan önlemler üzerinden kaydedilen gelişmelerin düzenli olarak üst düzey yönetim tarafından gözden geçirilmesi,

55.3. İlgili yönetim seviyelerinde hesap verilebilirliğin sağlanması amacıyla gerekli yetkilendirme ve onaylama süreçlerinin belirli aralıklarla gözden geçirilmesi ve

55.4. Eşik değerler ve limitlerdeki istisnai uygulamaların veya politikalardaki diğer bilinçli/bilinçsiz sapmaların izlenmesine yönelik etkin bir raporlama sürecinin oluşturulması.

56. Etkin bir kontrol çevresi, banka içinde görev ve sorumluluk dağılımının mümkün olduğu ölçüde ayrıştırılmasını ve çapraz kontrol noktalarının belirlenmesini gerektirir. Personel arasında çatışmaya neden olan veya kontrol süreci bulunmayan görevlendirmeler, bankada kayıpların, hataların ve yasal olmayan aksiyonların gizlenmesine sebep olacaktır. Bu nedenle, çıkar çatışmasına yol açabilecek potansiyel noktaların tespit edilmesi, minimize edilmesi ve bağımsız izleme/kontrol süreçlerine tabi kılınması önem arz etmektedir.

57. Banka risk yönetimi kontrol altyapısını, aktif büyümesine ve faaliyet yapısındaki genişlemeye ve artan karmaşıklık düzeyine paralel şekilde geliştirmek ve genişletmekle mükelleftir. Bu süreç yeni ürün, iştirak-şube ağı, yabancı piyasalara girişi gibi önemli gelişmeleri mutlaka içermelidir.

58. Bir bankanın operasyonel risk kontrol uygulamaları genel itibarıyla aşağıdaki unsurlardan oluşmaktadır;

58.1. Personel arasındaki çıkar çatışmalarını, kayıpların-hataların gizlenmesini ve personelin diğer yasal olmayan davranışlara girmesini engelleyici nitelikte etkin görev dağılımı ve açık bir biçimde tasarlanmış yetkilendirme ve onay süreçlerini,

58.2. Belirlenen risk eşik değerlerine ve limitlere bağlılığın yakından izlenmesi ve ihlallerin araştırılmasını,

58.3. Banka varlıklarının ve veri tabanlarının kullanımına ilişkin etkin bir yetkilendirme ve güvenlik sürecini,

58.4. Tüm seviyelerdeki banka faaliyetlerinde uzmanlaşmanın sağlanması ve sürdürülmesine yönelik olarak, uygun personel seçimi ve eğitim imkânlarının geliştirilmesini,

58.5. Bankada yürütülen faaliyetlere ilişkin hazırlanan eğitim dokümanlarının çalışanların kolay ulaşımına imkân verecek şekilde bilgi sistemi bünyesinde bulundurulması ve bunların düzenli biçimde güncellenmesini,

58.6. Önemli ölçüde beklentilerin dışında gelir/fayda sağlayan faaliyet birimi ve ürünlerin önceden tespit edilmesine yönelik 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 sistem birimleri kontrol zaafiyetinden kaynaklanıp kaynaklanmadığının araştırılması gibi süreçleri,

58.7. Banka işlemlerinin ve muhasebe hesaplarının düzenli olarak mutabakatının sağlanmasını ve

58.8. İzin, hastalık ve bunun gibi durumlardan dolaylı olarak görevini belirli bir süre yerine getiremeyecek personele ait sorumlulukların sekteye uğramasına engel olacak nitelikte bir izin ve vekâlet politikasını.

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

60. Banka sigorta gibi risk azaltma tekniklerinden faydalanmak suretiyle maruz kaldığı riskleri üçüncü taraflara transfer edebilir. Bununla birlikte risk azaltmada kullanılan araçların banka tarafından operasyonel risk kontrollerinin yerine kullanılması doğru bir yaklaşım olarak değerlendirilmemelidir.

### 4.2. ACİL VE BEKLENMEDİK DURUM PLANI

**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.**

61. 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 zarar görmesine de yol açabilmektedir. 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.

62. 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.

63. Bankalar bu süreçte öncelikle kritik faaliyetlerini, solo ve konsolide bazda bağımlı olduğu banka içi ve dışı hizmet çeşitlerini ve bunlara ilişkin uygun esneklik seviyelerini belirlemelidir.

64. Banka tarafından oluşturulan olumsuz durum senaryoları, finansal, operasyonel ve itibar risklerinin etkileri açısından değerlendirilmeli, ortaya çıkan risk değerlendirmeleri bankanın kurtarma öncelikleri ve hedefleri için temel oluşturmalıdır. Acil ve beklenmedik durum planları bankada acil durum stratejilerini, kurtarma-yeniden başlama süreçlerini, yönetimin, personelin, yasal otoritenin, müşterilerin, hizmet sağlayıcıların ve gerekli olan durumlarda meslek kuruluşlarının bilgilendirilmesine yönelik iletişim planlarını içermelidir.

65. 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.

66. Acil ve beklenmedik durum 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.

67. 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.

## YÜRÜRLÜLÜK

68. Bu Rehber, Resmi Gazete'de yayımlandığı tarihten başlayarak yürürlüğe girer.