Risk Yönetimi Prensipleri

TBB Çalışma Grubu*

Basel Komite'nin sermaye yeterliliğine ilişkin yeni düzenlemesinde (Basel-II) öngörülen hususların uygulanmasına yönelik Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından 30 Mayıs 2005 tarihinde "Basel II'ye Geçişe İlişkin Yol Haritası" kamuoyuna açıklanmıştır. Yol Haritasında Türkiye Bankalar Birliği (TBB) ve BDDK bünyesinde eş çalışma gruplarının oluşturulması öngörülmüştür. Eş çalışma gruplarının oluşturulmasındaki amaç Basel II uygulamasına geçişe ilişkin BDDK ve sektör hazırlıklarının mümkün olduğu ölçüde sorunsuz ve başarılı biçimde tamamlanması amacıyla öngörülen konularda çalışma raporlarının sektör görüş ve önerileri de dikkate alınarak üretilmesi ve yapılacak düzenlemelerde BDKK için bir girdi oluşturulmasını temin etmektir. Bu çerçevede oluşturulan ve Basel II Yönlendirme Komitesi'nin bir üyesi koordinasyonunda çalışmalarını sürdüren alt çalışma gruplarının raporları tamamlanarak BDDK'nın bilgisine sunulmuştur.

Basel II Yönlendirme Komitesi alt çalışma gruplarından birisi olan Risk Yönetimi Prensipleri Çalışma Grubunun raporu aşağıda yer almaktadır.

A. Risk Yönetiminin Organizasyonel Yapısı

1. Bankalar, risk yönetimi sistemlerinin organizasyonunu, yapısal özelliklerini ve faaliyetlerinin kapsamını dikkate alarak belirlemelidir.

Bankanın tüm faaliyet ve finansal sonuçlarından nihai olarak yönetim kurulu sorumludur. Bu itibarla, yönetim kurulunun; bankaya ve banka ortaklarına karşı sadakat görevini yerine getirmeye dönük olarak, banka yönetiminin üzerinde, yönetimi sorgulama gücünü haiz, bankanın günlük işlerinden ziyade hedefler ve hedeflere dönük stratejileri izlemeye odaklanmış, banka politikalarını belirleyen veya onaylayan bir rolü bulunmaktadır. Risk yönetimi, bu bağlamda, fonksiyon olarak doğrudan yönetim kurulunun uhde ve sorumluluğunda olmak durumundadır. Etkili risk yönetimi, en üst seviyeden başlatıldığı takdirde mümkündür. Risk yönetiminin banka içindeki organizasyonu, hesap verebilirlik ilkesi uyarınca doğrudan yönetim kuruluna bağlı olacak şekilde yapılandırılmalıdır.

Yönetim kurulu, risk yönetimi süreçlerini izlemek ve yönetim kurulu ile bu fonksiyonun iletişimini sağlamak üzere, icracı[1] fonksiyonlarla ilintisi olmayan en az bir üyesini risk yönetiminden sorumlu üye olarak görevlendirir.

Yönetim kurulu, riskin belirlenmesi, ölçümü, izlenmesi, kontrol edilmesi ve raporlanması evrelerinden oluşan risk yönetimi sürecinin yönlendirilmesi ve izlenmesini teminen kendisine bağlı alt komite niteliğinde olmak üzere, risk yönetiminden sorumlu yönetim kurulu üyesinin başkanlığında çalışacak bir risk komitesinin üyelerini belirler. Yönetim kuruluna bağlı risk komitesinde, kredi riski, piyasa riski ve operasyonel riskleri üstlenen en üst düzeydeki icracı yöneticiler ile risk yönetimi fonksiyonunda yer alan yetkililerin görevlendirilmesi sağlanır.

Çalışma Grubu Üyeleri: Hasan Candan (T. İş Bankası A.Ş.) başkanlığında; Cenan Aykut (Türk Eximbank), Ayşen Demirkurt (Türkiye Sınai Kalkınma Bankası A.Ş.) , Özlem Öner Ernart (T. Garanti Bankası A.Ş.), Belma Özçoban (Tekstil Bankası A.Ş.), Altay Yaman (T. Vakıflar Bankası T.A.O.), Alp Özateşler (Yapı Kredi Bankası A.Ş.), H. Özgür User (Koçbank A.Ş.), Özge Sevil (Citibank A.Ş.).

Yönetim kurulunun denetim ve gözetim fonksiyonlarının yerine getirilmesine yardımcı olmak üzere faaliyette bulunan denetim komitesinde risk yönetiminden sorumlu yönetim kurulu üyesinin de görev alması, her iki komitenin de yönetim kurulunun alt komiteleri hüviyetiyle yönetim kurulunun aslî iki fonksiyonuna odaklanmaları dolayısıyla mümkündür. Ancak, denetim fonksiyonunun, bankadaki risk yönetimi süreçlerinin denetimini de kapsaması gerektiğinden, belirtilen yapının söz konusu olduğu denetim komitelerinde, üyeler arasındaki iş bölümü ve hiyerarşinin, menfaat çatışmalarına ve süreç çelişkilerine yol açmayacak denli şeffaf ve kayda bağlanmış olması şartı aranmalıdır.

Yönetim kurulu, risk yönetimi fonksiyonuna gerekli uygulama desteğini sağlamalıdır. Yönetim kurulunun, risk yönetimi uygulamalarının içerdiği kavram ve tekniklere mümkün olduğunca yakınlaşması; risk yönetimi faaliyetlerinin amaç ve kapsamı konusunda bilgi sahibi olması; bankanın hedeflerine ulaşması konusunda bu fonksiyonun yol gösterici danışmanlığından nasıl ve ne ölçüde yararlanabileceğini algılama hususunda çaba göstermesi esastır.

Bu bağlamda, yönetim kurulu, risk yönetimi fonksiyonunun ihtiyaç duyduğu bağımsız ve objektif davranabilme ortamı ile donanım, altyapı, gerekli yetkinlikte insan kaynağı gereksinimlerini karşılama konusunda destekçi ve teşvik edici olmalıdır.

Bankalar, risk yönetimi organizasyonunu, doğrudan yönetim kuruluna veya yönetim kurulunun risk yönetiminden sorumlu üyesine veya risk komitesine bağlı olacak şekilde, grup/birim veya komiteler bazında merkezi veya merkezi olmayan bir yapıda tesis ederler.

Bankalar faaliyetlerinin çeşitliliğine, hacmine ve yapısına uygun olarak, farklı özelliklere sahip risklerin izlenmesi ve kontrolü için daha alt kademelerde birden çok birim/komite tesis edebilirler. Bu birimler veya komiteler de risk yönetimi fonksiyonuna bağlı olarak çalışmalıdır.

Banka dahilinde oluşturulmuş aktif-pasif yönetimi komitesi, kredi komitesi gibi diğer komitelerde, bankanın risklilik düzeyinin göz önünde bulundurulmasını teminen risk yönetimi fonksiyonunun temsil edilmesi sağlanmalıdır.

2. Risk yönetiminin icrai fonksiyonlardan bağımsızlığı gözetilmelidir.

Risk yönetimi fonksiyonunun çalışma esasları yönetim kurulunca belirlenmelidir. Risk yönetimi fonksiyonunun çalışması için gerekli usul ve esaslar, görev ve sorumluluklarının ayrıntısı, risk yönetimi fonksiyonunun önerilerinin de dikkate alınması suretiyle, banka yönetim kurulu tarafından oluşturularak yürürlüğe konulan ve üst yönetim tarafından uygulanan risk politikalarına ve bunlara ilişkin uygulama usullerine uygun olarak belirlenmelidir.

Bankanın faaliyetlerinden dolayı üstlendiği risklerin, risk alan fonksiyonlardan yönetsel ve özlük hakları açısından bağımsız bir fonksiyon tarafından ölçümü, izlenmesi, kontrolü ve raporlanması; hata veya zararların gizlenmesi, potansiyel risklerin gözardı edilmesi, performansın gerçeğe aykırı olarak bildirilmesi ve benzeri hususların önlenmesi açısından önem taşımaktadır.

Risk yönetimi fonksiyonu kapsamındaki faaliyetlerin yönetim kurulu, denetim komitesi, üst yönetim[2] ve bankanın her seviyedeki çalışanı tarafından yürütülmesi esastır. Bununla birlikte, bankaların içsel risk yönetimi düzenlemeleri, risk yönetimi organizasyonunun yönetsel bakımdan bağımsız, banka yönetim kuruluna karşı hesap verebilir olmalarını sağlayacak

şekilde yerine getirilmelidir. Risk yönetimi fonksiyonunun bağımsızlığı ilkesi, hesap verebilirlik esasına aykırılık olarak değerlendirilmemelidir.

Risk yönetimi çalışmalarının sürdürülmesi ve risk yönetimi bulgu ve değerlendirmelerinin yönetim kararlarında kullanılması icrai fonksiyonların etkisinden arındırılmış şekilde gerçekleştirilmelidir. Risk yönetimi değerlendirme ve bulgularına yapılacak herhangi bir etki veya baskı, bankanın risklilik ve performansının farklı yansıtılmasına neden olabilecektir. Bu gibi durumların önlenmesine yönelik olarak, risk yönetimi organizasyonunun bankanın genel organizasyon hiyerarşisinden bağımsız olarak tesis edilmesi önemlidir.

3. Risk yönetimi fonksiyonunun etkililiği açısından güçlü bir yapılanma ve yeterli kaynak ayrılması şarttır.

Risk yönetimi fonksiyonunun etkililiği ve işlevselliği, bankaların yönetim kalitesinin önemli göstergelerinden biri olarak algılanmalıdır. Etkililik ve işlevselliğin sağlanması için risk yönetiminin bankanın faaliyetlerinin ayrılmaz parçası olarak düşünülmesi, stratejik ve yönetsel süreçlerde yer verilmesi esastır. Karar alma, stratejik yönetim ve operasyonel süreçlere entegre edilmiş bir risk yönetimi bankaların yönetim kalitesinin artırılmasının temel taşıdır.

Banka, risk yönetiminin entegrasyonunda risk yönetimi hedeflerinin organizasyonun tüm seviyelerine yayılması, risk yönetimi ve bulgularının stratejik planlar, operasyonel süreçler ve kontrol sistemlerinde yer alması, banka içinde risk kültürünün oluşturulması gibi konuları, faaliyetlerini ve yapılarını da göz önünde bulundurarak ele almalıdır.

Etkili bir risk yönetiminin sağlanması açısından risk yönetimi bilgi ve uygulama deneyimine sahip olunmalıdır. Risk yönetiminin başarıyla uygulanması, bilgi sahibi ve donanımlı çalışanların olmasına bağlıdır. Banka yönetim kurulu, etkili risk yönetimi için risk yönetimi bilgi ve deneyimine sahip bir organizasyonel yapılanmayı önemsemelidir. Bu amaçla yönetim kurulunda, risk yönetiminden sorumlu üyesinde/komitesinde, risk yönetimi grup/birim vb. organizasyonel oluşumlarında risk yönetimi deneyim ve bilgisinin varlığını gözetmelidir. Risk yönetimi çalışanları temel bankacılık ile risk yönetiminin gerektirdiği bilgi, donanım ve analitik düşünme becerisine sahip olmalıdır. Risk yönetimi çalışanlarının temel bankacılık ve risk yönetimi bilgi ve deneyimine ve analitik düşünme becerisine sahip olmaları gereklidir.

B. Risk Yönetimi Fonksiyonuna İlişkin Görev ve Sorumluluklar

1. Risk yönetimi politika ve stratejilerinin geliştirilmesinden, banka faaliyetlerinin politika ve stratejilere uyumunun gözetim ve denetiminden, risk yönetimi fonksiyonunun bağımsız ve objektif olarak yerine getirilmesinin sağlanmasından yönetim kurulu sorumludur.

Yönetim kurulu, bankanın hedefleri ve risk algılamasıyla uyumlu risk yönetimi stratejileri ile risk politikalarının onaylanmasından sorumludur. Yönetim kurulu, üst yönetimin gerekli süreçleri tesis ettiğini ve uygulamaları yürürlüğe koyduğunu gözetmelidir.

Yönetim Kurulu, risk yönetimi organizasyonunun kadro ihtiyacının belirlenmesi, bu kadrolarda çalışanların görev ve sorumluluklarının belirlenmesi, icradan bağımsızlıklarının sağlanması, özlük haklarının belirlenmesi ve performanslarının değerlendirilmesinden sorumludur.

Risk yönetimi süreçleri bankanın faaliyetlerinin yapısı ve hacmi ile uyumlu olarak belirlenmeli ve bunlara uygunluk kontrol edilmelidir. Bankanın faaliyetlerinin yapısı ve hacmi ile uyumlu, bütünleşik risk profiline yönelik risklerin tanımlanması, değerlendirilmesi, ölçülmesi, izlenmesi, kontrolü ve raporlanmasını kapsayan süreç proaktif risk yönetimi uygulamasını olanaklı kılacak şekilde belirlenmeli ve faaliyetlerin de bu esaslar çerçevesinde yürütüldüğünün kontrolü sağlanmalıdır.

2. Banka bünyesinde risk kültürünün oluşturulması ve yerleştirilmesini sağlamaya dönük altyapı ve ortam geliştirilmelidir.

Banka genelinde risk kültürünün yerleştirilmesi için çalışanlarda farkındalığın arttırılması ve gerekli eğitim çalışmalarının yürütülmesi gereklidir. Banka çalışanı, yaptığı işin risklerinin ve muhtemel etkilerinin bilincinde olmalıdır. Risk yönetimi fonksiyonunun yönetim kurulundan başlayarak bankanın en alt kademedeki çalışanına kadar değişik seviyelerde sorumluluklar getirdiği hususu gündemde tutulmalıdır.

Yönetim kurulu, bankanın faaliyetleri nedeniyle karşı karşıya bulunduğu riskler ve bu risklerin etkileri hakkında bilgi sahibi olmalıdır. Yönetim kurulu, bankacılık faaliyetlerinin yüksek standartlarda, güvenilir ve sağlam bir şekilde yürütüldüğünden emin olmalıdır. Bu sorumluluğunun yerine getirilmesini kesintiye uğratmayacak, zamanında tam ve doğru bilgilenmeyi sağlayacak süreçleri tesis etmeli, ayrıca bankacılık faaliyetlerinin yerine getirilmesine destek olan bilgi teknolojileri alt yapısı, buna ilişkin riskler, sistem geliştirme projeleri ve bunların stratejileri, hedefleri, kısa ve uzun vadeli bütçeleri ne yönde etkilediği ve uyumu hakkında da bilgi sahibi olmalıdır.

Banka üst yönetimi ve iş birimleri kendi faaliyet alanlarındaki potansiyel risklerin olası etkilerinin farkında olmalıdır. Üst yönetim ve iş birimleri kendi yönetimlerindeki süreçlerin maruz kaldığı risklerin ve bu risklerin bankanın gelirlerine ve sermayesine olası etkilerinin bilincinde olmalıdır. Risk konusundaki farkındalık eğitimle olanaklıdır. Risk yönetimi fonksiyonu, banka çalışanlarının üstlendikleri sorumluluk ve rolleri ile deneyim ve bilgi birikimleriyle uyumlu eğitim programları oluşturmalıdır.

Uygulama birimleri, faaliyetlerinin sonuçlarının bankanın risk iştahı ve politikaları ile uyumlu olmasını sağlamalıdır. Banka üst yönetimi ve uygulamacı birimler risk iştahı ve risk politikaları çerçevesinde faaliyette bulunmak zorundadır. İş birimlerinin hedef ve stratejilerinde, kaynakların dağıtımında risk yönetimi bulgularının gözönünde bulundurulması gereklidir. Yeni faaliyetlere girilmeden önce risk boyutunu da içeren kapsamlı araştırmalar yapılmalı ve yazılı hale getirilmelidir.

C. Risk Ölçüm Süreci

1. Bankalar, maruz kaldıkları risklerin tümünü ölçebilmek için güvenilir ve bütünlük içinde uygulanabilen; yapıları, ürün çeşitleri ve faaliyet alanları ile uyumlu risk ölçüm sistemlerine sahip olmalıdır.

Bankalar, bilgisayar uygulamalarına dayalı analitik modeller kullanarak risklerinin ölçülmesine/tahminine ve geriye dönük testlerle doğruluğunun sınanmasına yönelik süreçleri içeren bir risk ölçüm sistemini tesis etmelidir. Model riskinin yönetilebilmesi açısından, modellerin altyapısındaki varsayımlar ve model algoritmaları en az yıllık dönemlerde düzenli olarak gözden geçirilmelidir.

Banka, risk ölçüm sisteminin ürettiği sonuçların doğru yorumlanması için gerekli tüm tedbirleri almalıdır. Risk ölçüm sistemlerinin geliştirilmesi sürecinin içerdiği karmaşık ve teknik detaylar dolayısıyla sistemin çıktılarının yorumlanması da teknik bankacılık teknik bilgi ve donanımını gerektirecektir. Banka, risk ölçüm sisteminin sonuçlarının karar alma süreçlerine dahil edilmesinde hata ve noksanlıklardan kaynaklanabilecek yorumlama hatalarına karşı gerekli tüm tedbirleri almalıdır.

Risk analiz ve değerlendirmelerinin bankanın risk seviyesini doğru şekilde yansıtacak yöntemlerle yapılması, risk profilinin izlenmesi ve kontrol altına alınması sağlanmalıdır.

Risklerin gelişmiş modeller kullanılarak ölçülmesi, risk getiri dengesinin gözetilmesi, bankanın sağlıklı ve basiretli yönetilmesini sağlar. Bankanın maruz kaldığı tüm risklerin, detaylı ve gelişmiş yöntemler kullanılarak yapılan risk analizleri sonucunda kontrol altına alınması ve raporlanmasının sağlanması gerekmektedir. Risklerin ölçümüne yönelik olarak kullanılan modeller riskleri gerçekçi biçimde yansıtmalı, senaryo analizi, stres testleri gibi ilave analizlerle desteklenmeli, geçerliliği değişen koşullara uygun olarak değerlendirilmelidir. Gelişmiş modeller kullanılarak yapılan risk ölçümleri risk iştahının ve risk toleranslarının belirlenmesinde kullanılmalıdır. Senaryo analizleri ve stres testleri ayrıca bankanın acil ve beklenmedik durum planlarında da göz önünde bulundurulmalıdır.

2. Bankalar, risk ölçüm sisteminin kurulması, idame ettirilmesi, izlenmesi, kontrol edilmesi hususlarına ilişkin olarak sorumluluk paylaşımını, icracı fonksiyonlardan bağımsız olacak şekilde tesis etmeli, ilgili süreçleri ve görev tanımlarını net şekilde yazılı olarak hazırlamalıdır.

Risk yönetiminin amacı, uygun varsayımlar ve parametreler içinde bankanın maruz kalabileceği riskleri yöneterek bankanın risk ayarlı getirisini en üst seviyeye ulaştırmaktır. Bu doğrultuda, risk ölçüm sisteminde kullanılacak varsayımların ve parametrelerin belirlenmesi gerekmektedir.

Banka risk ölçüm sisteminin dayandırılacağı varsayım ve parametreler yazılı olarak belirlenmeli, ilgililerce net bir şekilde anlaşılır olmalı, varsayımların ve parametrelerin risk ölçüm modelinin sonuçlarına olan etkileri düzenli olarak gözden geçirilmeli, gerektiğinde güncellenmeli ve tüm değişiklikler nedenleri ile birlikte kayıt altına alınmalıdır.

Risk ölçüm sisteminin dayandırılacağı varsayım ve parametreler yazılı olarak belirlenmeli; risk yöneticileri ve banka üst yönetimince net bir şekilde anlaşılmalı; varsayımların ve parametrelerin risk ölçüm modelinin sonuçlarına olan etkileri düzenli olarak gözden geçirilmeli; gerek duyulması halinde uygun değişiklikler gerçekleştirilmeli ve tüm değişiklikler nedenleri ile birlikte kayıt altına alınmalıdır.

Bankalar, konjonktürel değişiklikleri ve dalgalanmaları varsayımlarına dahil etmelidir. Konjonktürel değişiklikler küresel ekonominin yönünü tayin eden en önemli unsurdur ve geç farkına varılması nedeniyle uygun aksiyon alınamaması önemli bir risktir. Konjonktürel değişikliklerin etkisinin sayısallaştırılabilmesi amacıyla, senaryo analizlerine bu tarz etkiler varsayımsal olarak dahil edilmelidir.

Bankalar model riskine maruz kalma olasılıklarını engelleyici tedbirleri almalıdır. Model riski, hatalı ve/veya yetersiz parametre ve varsayımlar nedeniyle modelden beklendiği ölçüde doğru sonuçların alınamaması riskini ifade etmektedir. Modelin dayandığı varsayımlar

ve hesaplanan parametrelerin doğruluğu ve yeterliliği iç denetime konu edilmeli, bu yönde düzenli kontroller tesis edilmelidir.

3. Veri yönetimine ilişkin ilkeler

Veri yönetimi sürecinin sahibi yönetim kuruludur. Yönetim kurulu, veri yönetimi sistem ve süreçlerinin bütün önemli yönleri ve özelliklerini bilmelidir. Veri yönetimi konusunda oluşturulmuş sistemlerin işleyişleri, konu ile ilgili iş akışları hususlarında yönetim kurulu bilgi sahibi olmalı, sistemlerin en etkili şekilde işleyişlerini temin etmeye yönelik kontrol süreçlerinin oluşturulmasını sağlamalıdır.

Veri yönetimi politikaları belirlenmeli ve etkili şekilde uygulanması sağlanmalıdır. İç verilerin ölçümleme için yeterli olmadığı koşullarda, dış veriler istatistiki yöntemlerle uygun hale getirilerek, banka veri tabanına dahil edilebilir. Bankanın kendi iç verisi kıymetli olmakla beraber, dış veri havuzunun temin edeceği farklı nitelikte, şiddette, karmaşıklıkta verinin yönetim ve ölçüm sistemlerine dahil edilmesi olanağından mahrumdur. Bu nedenle banka iç veriyi topluyor olsa dahi, bu veriyi desteklemek amacı ile dış veri havuzlarından da yararlanabilmelidir. Dış veri tabanının kullanımı, sadece riskin ölçülmesi değil, aynı zamanda riskin yönetilmesi ve genel anlamda banka stratejisi için de oldukça önem taşımaktadır.

Ölçüme konu edilecek dış veri, bankanın faaliyet alanı, yapısı, iç kontrol ortamı ve ölçeğine uygun olmalıdır. Bankaların kullanacakları dış veriler; bankanın faaliyet alanı, yapısı, ölçeği ile uyumlu olmalı; gerçekleşen kayıp miktarları, olayın meydana geldiği faaliyet kolundaki faaliyetlerin ölçeği, kayıp olayının nedenleri ve ortaya çıktığı koşullar hakkında bilgiler içermelidir. Dış veriler ilgili kurumların kendi kontrol ortamları içinde yaşanmış olayları kapsadığından, bu verileri kendi ölçüm sistemlerinde kullanacak olan banka kendi yapısını, kontrol ortamını, ölçeğini dikkate alarak verileri değerlendirmeli ve ölçüm sistemlerine dahil etmelidir.

Veri toplama süreci bankanın iç denetimine konu bir süreç olmalıdır. Risk ölçüm sistemi kapsamında kullanılacak olan verinin toplanmasına ilişkin süreçler yazılı şekilde oluşturulmalı; verinin zamanında, tutarlı ve güvenilir şekilde teminine ilişkin tüm sistemsel ve yönetsel tedbirler alınmış olmalıdır.

Banka verinin kalitesinden emin olmak için veriyi objektif ve standart kriterlere göre toplamalıdır. Veri kalitesini sağlamak için uygulanan tüm kriterler ve usuller yazılı ve detaylı şekilde açıklanmalıdır. Diğer taraftan, banka, hatalı verinin düzeltilmesi ve eksik verilerin tamamlanması için banka içinde uyguladığı metodu da ilgili prosedür içinde belirtmelidir.

Verinin toplanmasına ilişkin süreç, bankanın tüm önemli faaliyetleri doğrultusunda maruz kalabileceği riskleri içerebilecek şekilde kapsamlı olmalı, önemli faaliyetleri ve risk tutarlarını dışarıda bırakmamalı, toplanacak kayıp tutarlarına ilişkin olarak bankanın faaliyetleri ve ölçeği ile uyumlu bir alt eşiğe sahip olmalıdır. Banka, tarihsel verilerinin ölçüme uygunluğunun devamlılığını sağlamaya yönelik yazılı prosedürlere, tarihsel verilerinin ölçüme uygunluğunun devamlılığını sağlamaya yönelik değerlendirmelere, ölçekleme benzeri ayarlamalara, bunların hangi kapsamda yapılabileceğine ve bu konudaki yetki dağılımına ilişkin yazılı prosedürlere sahip olmalıdır.

Banka, brüt kayıp tutarlarına ilişkin bilgilerin yanı sıra kayıp olayının gerçekleşme zamanı, kaybın karşılanmasına yönelik olarak yapılan geri ödemeler (nakit telafiler, teminat

yolu ile telafi, sigorta ödemesi, tazminat vb.), kayıp olayının nedeni ve olaya neden olan etkenler hakkında açıklayıcı bilgiler de toplamalıdır. Bu bilgilerin detay seviyesi, ilgili brüt kayıp tutarının büyüklüğü ile uyumlu olmalıdır.

Banka, sistem altyapısının değişikliklere açık ve esnek olmasını temin etmelidir. Olası gelişmelere ve değişikliklere adapte edilebilecek, ölçümleme sürecini sekteye uğratmayacak şekilde esnek teknik altyapının kurulması temin edilmelidir. Veri setleri üzerinde geçmişe yönelik olarak düzeltme yapılmamalıdır. Düzeltme, istisnai nedenlerle elzem hale gelmiş ise nedeni ve niteliği yazılı hale getirilmelidir.

Veri tabanının güvenliği sağlanmalıdır. Farklı kaynaklardan bilgi girişi bulunan veri tabanlarında bilgi giriş ve izlemesinde, bilgiye erişimde güvenli bir yapı oluşturulmalı, yetkisiz erişimlerin sistem üzerinde engellenmesine imkan veren yapı tesis edilmelidir. Verilerin kalitesinin düzenli kontrolü için sorumluluklar belirlenmeli, ilgili süreçler yazılı şekilde oluşturulmalıdır.

D. Sermaye Yönetimi

1. Bankalar yasal sermaye yeterliliklerini düzenli olarak değerlendirmeli, sermaye yeterlilik oranının düşük olma eğilimi gösterdiği durumlarda gerekli önlemleri almalıdır.

Bankalar sermaye yeterlilik hesaplama yöntemlerini düzenli olarak gözden geçirmeli ve risklerin yönetimine ilişkin stratejiler geliştirmelidir. Sermaye yeterlilik rasyosundaki değişimlerin nedenleri incelenmeli, değişen risk tutarlarına bağlı olarak artan ya da azalan sermaye yeterlilik rasyosu değerlendirilmelidir. Oranın mevzuatta belirlenen asgari orandan düşük olma eğilimi göstermesi halinde bunun nedenleri araştırılmalı, oranı yükseltecek önlemler alınmalı, hızlı bir şekilde sermaye yeterliliğini uygun düzeye getirme yönünde bir planlama yapılmalıdır. Sermaye yeterlilik oranının asgari orandan düşük olması durumuna ilişkin erken uyarı sinyallerinin belirlenmesi ve bunların takibi de sürecin bir parçası olmalıdır.

Bankanın sermayesinin etkin kullanımı ve bankacılık faaliyetinin güvenilir biçimde sürdürülmesi, sermayenin maruz kalınan risklere tahsis edilerek yönetilmesi yoluyla olanaklıdır. Bankalar maruz kaldıkları her bir risk türü için hesapladıkları ekonomik sermayeyi birleştirilerek tek bir sermaye rakamına ulaşmak için bir yöntem geliştirme konusunda çalışmalar yürütmeli, bu sermaye rakamına ulaştıklarında bunun farklı iş kollarına dağıtımına ve risk bazlı sermaye hesaplamaya yönelik çalışmaları kapsayan bir vizyon geliştirmelidir.

Bankalar maruz kaldıkları risk türlerini göz önünde bulundurarak hesapladıkları ekonomik sermayelerini farklı iş kollarına en verimli şekilde tahsis etmek, riske dayalı fiyatlama ve sermaye tahsisine yönelik sistemler geliştirmek ve bu doğrultuda sermaye hedeflerini ve sermaye tahsis yöntemlerini düzenli olarak gözden geçirmek durumundadırlar. Risklerin tanımlanması, ölçülmesi, raporlanmasına ve yönetimine ilişkin politika ve prosedürler, bu riskler için gerekli sermaye tahsis yöntemine, sermaye hedeflerini ve riskleri dikkate alarak değerlendirmeye, iç kontrol ve teftiş sistemlerine yönelik süreçler oluşturulmalıdır.

Bankalarda belirlenen içsel sermaye hedefleri sağlam temellere dayanmalı, yönetim kurulunun belirlediği risk iştahı ve bankanın faaliyetleri ile tutarlı olmalıdır. Hedef sermaye seviyeleri üst yönetim tarafından izlenip değerlendirilmeli, bankanın faaliyetlerindeki değişikliklere ve alınan risklere bağlı olarak gerektiğinde güncellenmelidir. İçsel sermaye hedefleri

bankanın çeşitli fonksiyonlarına tahsis ettiği ekonomik sermaye seviyesinin değerlendirilmesinde ve banka risk yönetimi ve iç kontrol süreçlerinin etkililiğinin ölçülmesinde önemli bir rol oynamaktadır. Bankalar risk yönetimi sistemlerini, gelecekteki sermaye gereksinimlerini değerlendirerek bankanın stratejik planlarında gerekli ayarlamaları yapabilecek seviyeye getirmelidir.

Güçlü ve etkili risk yönetimi fonksiyonu, bankanın sermaye yönetimindeki en önemli aracıdır. Bankaların riskleri için bulundurdukları sermaye ile risk yönetimi ve iç kontrol süreçlerinin gücü ve etkililiği arasında önemli bir ilişki bulunmaktadır. Sermaye, yetersiz iç kontrol veya risk yönetimi süreçlerine alternatif olarak görülmemelidir.

2. Bankalar mevcut piyasa koşullarının dışında gelişebilecek sistemik riskler, değişen piyasa koşulları ve ekonomik konjonktür nedeniyle uğrayacakları zararları ve bu zararları karşılayacak ekonomik sermayeyi tahmin etmeye yönelik olmak üzere stres testleri ve senaryo analizleri yapmalıdırlar.

Bankaların piyasa koşullarının olumsuz olduğu zamanda acilen sermaye artışına gitmesi, mümkün olsa bile yüksek maliyetli olacaktır. Sermaye yeterliliğinin değerlendirilmesi sırasında ekonomik konjonktür de dikkate alınmalı, bankaları olumsuz etkilemesi olası olayları göz önünde bulunduran, olumsuz piyasa koşullarını içeren stres testleri yapılmalıdır. Geçmiş dönemlerde yaşanan krizlerdeki piyasa koşullarını içeren senaryolar oluşturulmalı ve senaryoların mevcut portföylerdeki etkilerini hesaplamaya yönelik bir yapı geliştirilmelidir. Gerçekleştirilen stres testlerinin, senaryo analizlerinin ve duyarlılık analizlerinin sonuçları ve bu sonuçların sermaye planları ile nasıl ilişkilendirildiği ele alınmalıdır.

E. Risk Politikaları ve Risk Limitleri

1. Bankaların risk algılamalarını ve risk stratejilerini yansıtan, net olarak anlaşılır nitelikte risk politikaları olmalıdır.

Risk yönetimi, ihtiyari değil, bankanın sağlıklı yapısını koruması bakımından zorunlu temel faaliyetlerdendir. Bu bakımdan, risk yönetimi her faaliyetin yönetim ve planlamasının parçası olarak görülmelidir. Güvenilir ve etkili risk yönetimi fonksiyonunun en önemli araçlarından biri risk politikalarıdır. Risk politikaları, risk yönetimi sürecinin kritik evresi olan riskin kontrolü faaliyetini olanaklı kılan üst düzey politikalardır. Risk politikaları yazılı halde olmalıdır.

Risk politikaları, bankanın genel iş stratejisinin parçası olarak değerlendirilerek, yönetim kurulu onayına tabi olmalıdır. Politikalar etkililikleri ve uygunlukları açısından düzenli olarak değerlendirilmelidir.

Risk politikalarının aşağıda belirtilen hususlara netlik kazandırması beklenir:

- Risk iştahı, risk stratejisi ve temel risk alanları: Bankanın, hedeflediği getiri veya kredi derecelendirme notunu elde etmek için katlanmaya hazır olduğu risklilik düzeyinin, risk yönetiminde benimseyeceği stratejinin ve özellikle bankaya özgü risk alanlarının politika kapsamında belirlenmesi şarttır.

- Bankanın risk profili, yeni ürün, faaliyet ve uygulamaların risk profiline olan etkilerinin belirlenmesine ilişkin esaslar: Banka açısından etkisi yüksek olabilecek risk kate-

gorileri ve risklerin belirlenmesine ilişkin esaslar ortaya koyulmalıdır. Yeni ürünlerin geliştirilmesi, müşteriye sunulması, yeni faaliyetlere veya uygulamalara yer verilmesine ilişkin planlamalarda, bunların bankanın genel risk profilinde oluşturması olası değişikliklerin saptanması ve bankanın risk iştahı üzerindeki etkilerinin irdelenmesi gerekir. Risk politikalarının bu hususlarda izlenecek süreçleri belirlemesi gerekir.

- Risk yönetiminin bankadaki örgütlenmesine ilişkin esaslar: Risk yönetimi fonksiyonunun bankadaki organizasyonel pozisyonunun, iletişiminin, yetki ve sorumluluklarının politikalarda saptanmış olması beklenir.

- Kurum çapında risk yönetiminin uygulama esasları: Bankanın risklerin belirlenmesi, ölçümü, kontrolü, izlenmesi ve raporlanması evrelerinde benimseyeceği süreçler ile uygulama esaslarının politikada belirlenmesi gerekir. Risk ölçümlerinde ve ölçüm sonuçlarının sınanmasında kullanılacak yöntemler de risk politikalarında belirginleştirilmelidir.

- Bankaya özgü risk limitlerine ilişkin sistematik ve uygulama esasları: Özgün risk limitlerine ilişkin süreçler ve uygulama esasları belirlenmelidir.

- Risk yönetimi sürecindeki roller ve sorumluluklar: Risk politikalarının onaylanması, gözden geçirilmesi, uygulanması, uygulamanın politikalarla uyumluluğun izlenmesi, politikaya aykırı işlem ve inisiyatiflerin tabi olacakları kuralların belirlenmesi gereklidir.

2. Bankalar, faaliyetlerinin kapsamı ve karmaşıklığıyla orantılı olarak, risk stratejilerini yansıtan ve ilgililerce tereddütsüz algılanabilen, yasal sınırlamalardan bağımsız, özgün risk limitleri belirlemelidir.

Bankaların yönetim kurulunca onaylanmış, uygun risk yönetimi stratejileri mevcut olmalı; bankaya özgü risk limitleri de risk iştahlarını ve risk stratejilerini yansıtmalıdır.

Risk limitleri ilke olarak yönetim kurulunca onaylanır. Üst seviyede yönetim kurulunca belirlenmiş risk limitlerinin alt kırılımlarının belirlenmesine ilişkin yetki devri olanaklıdır. Yönetim kurulu, risk limitlerinin önerilmesi, değerlendirilmesi, onaylanması, banka örgütü içerisinde duyurulması, izlenmesi ve denetlenmesi evrelerine ilişkin uygulama esaslarını belirler ve onaylar. Risk limitleri banka örgütü içinde ilgili personele bildirilir.

Bankanın üstlendiği risklerin, risk limitleri dahilinde olduğu ve banka üst yönetimi tarafından izlendiği konusundaki gözetim sorumluluğu yönetim kuruluna aittir.

Risk limitlerinin, uygulamadaki gelişmelerin güncelliğini yakalayacak şekilde uygun sürelerde gözden geçirilmesi esastır. Gözden geçirme konusundaki aslî sorumluluk, limit belirleme yetkisini haiz olan yönetim kuruluna aittir. Gözden geçirme süreci, limitlerin, riskler ve bankanın risk iştahı karşısında anlamlı ve yeterli olup olmadığını belirlemeye yönelik olmalıdır.

Risk limitlerinin risk bazlı olarak belirlenmesi esastır. Risk bazlı limitler, parasal büyüklüklere bağlı nominal tutarlar olabileceği gibi, risk ölçüm sonuçlarına dayalı (örneğin, ortalama RMD'nin yüzdesi; risk ağırlıklı varlıkların yüzdesi; sektörel ya da borçlu bazında sı-

nırlamalar) oransal limitler de olabilir. Hiçbir durumda, bankaya özgü risk limitleri yasal sınırlamaların üzerinde belirlenemez.

Risk limitleri, önemlilik ilkesi çerçevesinde banka tarafından uygun görülecek tüm risk kategorilerinde tesis edilebilir. Asgari olarak, bir bankanın piyasa, kredi ve operasyonel risklerine ilişkin özgün limitlerinin olması beklenir. Örneğin, piyasa riskine ilişkin, RMD bazlı risk faktörü limitleri, alım-satım limitleri; kredi riskinde, büyük kredi riski limiti, tek borçlu/risk grubu, vade, para birimi yoğunlaşma limitleri, ülke riski limitleri, sektör limitleri; bankaya özgü likidite riski limitleri bu kapsamda sayılabilir.

Bankanın risk limiti yapısı içerisinde, limit aşım istisnaları tanımlanır ve istisnaların tabi olacağı kurallara yazılı olarak ayrıntılı biçimde yer verilir. Limitlerin potansiyel aşıma konu olabileceği durumların önceden saptanabilmesine yardımcı olmak üzere, erken uyarı seviyeleri saptanır; erken uyarı limitlerine ulaşılması halinde yapılması gerekenlere ilişkin uygulama esasları yönetim kurulunca belirlenir.

F. Risk Raporlaması

1. Risk yönetim sistemi, maruz kalınan risklerin etkin olarak analiz edilip değerlendirildiği bir raporlama sistemini içermelidir.

Raporlama risk yönetimi sürecinin temel unsurlarındandır. Bankalar, risklerin yönetimi, stratejilerin belirlenmesi ve kararların alınmasında kullanılmak üzere kapsamlı raporlamaları sağlayan sistemlere sahip olmalı, bu sistemler piyasa, kredi, operasyonel ve diğer risklere ilişkin yeterli düzeyde raporlama sunabilmelidir. Risk raporlarındaki bilgiler bankanın ve iştiraklerinin durumunu yansıtmalı, gelecekte beklenen gelişmelere ilişkin riskleri gösterebilmelidir.

Raporlar, risk tutarlarını ve trendini, risklerin sermaye düzeyine etkisini ve maruz kalınan risklere karşılık olarak yeterli ekonomik sermaye bulundurulup bulundurulmadığını, sermaye yeterliliğinin bankanın hedeflerine uyumluluğunu, gelecekteki muhtemel sermaye gereksinimlerini, stratejik planlarda bu gereksinimlere bağlı olarak yapılabilecek değişiklikleri içermelidir.

Mevcut limitlerin, limit kullanım ve aşımlarının, riske ayarlı getiri analizlerinin, risk yoğunlaşmalarının değerlendirilebileceği raporların yanısıra normal piyasa şartlarının haricinde meydana gelebilecek stres koşullarında risklerin düzeyini gösteren raporların da üretilmesi sağlanmalıdır.

Raporların üretilmesinde kullanılan verilerin doğruluğundan emin olunmalı, gerekli kontroller yerine getirilmelidir.

Gerçeği yansıtmayan verilerle üretilen raporlar banka için kritik önemde olan konularda yanlış kararların alınmasına yol açabilir. Bu nedenle, risklerin ölçülmesinde ve analizinde kullanılan banka verilerinin ve diğer verilerin doğruluğunu sağlamaya yönelik olarak, raporları çıkaran birim tarafından veri kontrolleri yapılmalı, bu kontroller rapor hazırlama sürecinin değişmez birer parçası olmalıdır.

Mali tablolar ve raporlama cetvellerinde yer alan bilgiler ile risk yönetimi raporlarına girdi teşkil eden bilgilerin uyumluluğu sağlanmalı, muhasebe ve iç raporlama sistemlerinin ve

finansal bilgilerin güvenilirliğini ve tutarlılığını incelemeye yönelik kontroller gerçekleştirilmelidir.

Raporlanan risk değerlerinin ilgililere zamanında iletilmesi sağlanmalıdır.

Raporların doğruluğu kadar zamanında hazır olması da önemlidir. İç raporların ilgili birimlere iletilme zamanı raporlama sıklığına bağlı olarak değişebilecektir, örneğin alım satım portföyünün riskinin günlük olarak hesaplandığı ve raporlandığı düşünüldüğünde riske maruz değer raporlarının her gün, önceden belirlenen saatte ilgili birime iletilmesi gerekmektedir. Bankalar raporları zamanında hazırlayacak kapasitede bilgi-işlem ve finansal raporlama sistemlerine sahip olmalıdır.

Risk raporları bankanın pozisyonlarını ve bu pozisyonlardan kaynaklanan risklilik düzeyini ortaya koyan dolayısıyla gizlilik içeren raporlar olduklarından, bu raporların sadece ilgili birim ve kişilere iletilmesini sağlayacak yapı kurulmalıdır.

2. Raporlama sistemleri mevzuata ya da banka içi belirlenen kural ve limitlere aykırılıkların söz konusu olabileceği durumlarda uyarıcı nitelikte olmalı ve gerekli tedbirlerin hızlı bir biçimde alınmasını sağlamalıdır.

Risk raporları, banka içinde belirlenen ve yönetim kurulu tarafından onaylanan kurallara ve limitlere aykırılıkların söz konusu olduğu durumları net olarak belirlemeli ve yönetim kurulu vasıtasıyla uyarı ya da aksiyon alınmasını sağlamalıdır. Aynı şekilde, mevzuata aykırılıklar raporlarla yönetim kurulu ve banka üst yönetiminin dikkatine sunulmalı, gerekli tedbirlerin zamanında alınması temin edilmelidir.

Kredi riski, operasyonel risk, piyasa riski ve diğer risk raporları yönetim kurulu ve üst yönetimle[3] birlikte, riskin oluşmasından ve izlenmesinden sorumlu fonksiyonlara da sunulmalıdır.

Raporların sadece yönetim kurulu ve üst yönetime değil, aynı zamanda riskin oluşmasından ve izlenmesinden sorumlu birimlere de sunulması gerekir. Bu itibarla, risk raporları, iç raporlama sisteminin önemli bir parçası olup, proaktif risk yönetimini de desteklemelidir.

Raporlama sıklığının, içeriğinin ve formatının belirlenmesinde risklilik düzeyi ve raporların iletildiği makam dikkate alınmalıdır.

Raporların sunulduğu makam ve raporlanan riskin düzeyi dikkate alınarak raporlama periyotları ve raporun çerçevesi belirlenmelidir. Risk düzeyinin belirlenmesinde, risk kategorisi ve riskin büyüklüğü göz önüne alınabilir. Raporlama sıklığı, içeriği ve formatı bilgi sağlanan tarafa ve bilginin kullanımına bağlı olarak değişiklik gösterebilir.

Raporların olası kullanımları dahilinde stratejik ve finansal planlama, günlük yönetsel faaliyetler sayılabilir. İş kolunun ve kurumun yapısına, büyüklüğüne göre raporlardaki bilgiler değişiklik gösterebilir. Genel bir kural olarak, risklilik düzeyi arttıkça daha detaylı rapor hazırlanması gerekmektedir. İç raporlamanın sıklığının ve rapor içeriğinin risklilik düzeyi ile tutarlı olması gerekmektedir.

İç raporların bankanın karşılaştığı riskleri önem sırasına göre belirtmesi yerinde olacaktır. Her bir risk türü için risklilik düzeyini etkileyen bileşenler, etki sırasına göre raporlarda

yer almalıdır. Önemli risklerle bunlara ilişkin kontroller ve risk azaltımları da raporlarda yer almalıdır.

Risk ölçüm sistemlerinde kullanılan model ile ilgili bilgiler, analizler, varsayımlar ve parametreler iç raporlarla birlikte ilgili birimlere iletilmelidir.

Raporlama çerçevesinin belirlenmesi bankanın sorumluluğundadır. Risklerin ölçümünde kullanılan model ile ilgili bilgiler, analizler, varsayımlar ve parametreler raporlarda yer almalı, kararlarında bu raporları dikkate alan birimler, ölçüm modellerinde kullanılan varsayımları bilmeli, bunların kullanımının ve değişiklik göstermesinin yarattığı sonuçları anlamalı ve geçerli olmamaları durumunda raporlanan rakamların nasıl değişeceği konusunda fikir sahibi olabilmelidir. Bununla birlikte, aşağıdaki maddelerle kısıtlı kalmamak koşuluyla raporlamanın aşağıda belirtilenleri de içermesi beklenir;

Kredi riski raporlarında;

- derecelendirilmiş portföy tanımları (tutar, borçlu sayısı, her derece bazında temerrüt oranları, derece bazında toplam portföyün ne kadarlık kısmının kapsama alındığı, sektörlerdeki, alt portföylerdeki ve iş kollarındaki bozulmalar)
- toplam portföyün dereceler bazında dağılımı, temerrüt olasılık bandları ve geçen yıla göre karşılaştırmaları
- gerçekleşen kayıp oranları ile beklenen oranların karşılaştırılması
- stres testi sonuçları
- yasal sermaye yükümlülüğünün ve ekonomik sermayenin hazırlanması
- risk dereceleri arasındaki geçişmeler

Operasyonel risk raporlarında;

- yasal ve ekonomik sermaye hesaplamaları
- yeni ya da geliştirilmiş yönetim politikaları, prosedürleri ve uygulamaları (örneğin, iş ortamındaki değişiklikler, iş uygulamaları ve iç kontrol etmenleri)
- risk azaltım ve risk transfer stratejileri (örneğin, herhangi bir beklenen kaybın azaltımının etkisi, sigorta politikalarının maliyet-fayda analizleri, iş kolu/olay türü risk tutarı ve/veya kayıp tutarlarında azaltma, düzeltme işlemleri, azaltım işlemlerinin maliyet-fayda analizleri)
- operasyonel risk tutarları (örneğin, anahtar operasyonel risk olayları ve tetikleyicileri, iş kolları arasındaki operasyonel risk tutarlarının dağılımı, yönü ve geçişmeleri)
- iç ve dış kayıplar (örneğin, kayıp olay türü analizleri, mevsimsellik, coğrafi dağılım ve yönelimler bazında karşılaştırmalar vb.)
- zayıf alanların tanımlanması ve hesaplanması (örneğin, risk hesaplamaları, anahtar risk göstergeleri)
- operasyonel risk yönetimindeki niteliksel gelişmeler ve hesaplama süreçleri ve sistemleri

Piyasa riski raporlarında;

- riske maruz değer hesaplamaları
- ekonomik sermaye ve yasal sermaye yükümlülükleri
- stres testi uygulamaları
- geriye dönük test uygulamaları
- riske göre ayarlanmış sermaye getirisi hesaplamaları
- limitler ve kullanımları

3. Risk yönetimi sistemlerinin ürettiği raporlar iç denetim fonksiyonunu üstlenen birimler tarafından düzenli olarak denetlenmelidir.

Bankaların kullandıkları risk ölçüm modelleri ve üretilen risk yönetimi raporları, yasal olarak raporlamakla yükümlü oldukları raporların doğru verilerle ve düzenleyici otoritenin belirlediği usul ve esaslara uygun bir şekilde hazırlanıp hazırlanmadığı, bu süreçte karşılaşılan aksaklıklar ve zayıflıklar, bankada iç denetim fonksiyonunu üstlenen birimler tarafından düzenli olarak denetlenmeli, gerekli kontrol ve incelemeler gerçekleştirilmelidir.

G. Kamuyu Bilgilendirme

1. Bankalar risk yönetimi uygulamaları ve sermaye yeterlilikleri hakkında kamuyu bilgilendirmelidir.

Bankalar maruz kaldıkları risklerin ölçümü ve bu riskler için bulundurmaları gereken asgari sermaye tutarının hesaplanması için çeşitli yöntem ve teknikler kullanmaktadır. Yatırımcıların, bankaları değerlendirirken, bankaların maruz kaldıkları riskler ve bu riskleri ölçme, azaltma ve yönetmede kullandıkları yöntemler hakkında bilgi sahibi olmaları gerekmektedir. Bu bakımdan bankaların risk yönetimi uygulamaları, risk yönetimi fonksiyonu ve organizasyon yapısı, izledikleri strateji ve süreçler, risk raporlama ve risk ölçüm sistemlerinin kapsamı, risk azaltım teknikleri gibi bilgileri anlaşılır netlikte kamuya açıklamaları önemlidir. Risk ölçümünde ve sermaye gereksiniminin hesaplanmasında daha fazla inisiyatif kullanılmasını gerektiren içsel yöntemlerin kullanılması durumunda bu açıklamaların önemi artmaktadır.

Finansal raporlarda verilen bilgiler dışındaki sermaye ve risklere ilişkin bilgilere nereden ve nasıl erişilebileceği belirtilmelidir.

Bankalar bilgi açıklamalarını düzenleyici otoritenin belirlediği kanallar vasıtasıyla yapacaklardır. Düzenli olarak yayınlanan finansal raporlarda verilen bilgiler dışında bankaların özellikle risk yönetim faaliyetlerine ilişkin bilgilerine kamunun nereden ve nasıl erişeceği belirtilmelidir. Bankaların internet sitelerinde bu konuya ilişkin bilgilendirme yapılmalıdır.

2. Bankalar denetim otoritesinin şart koştuğu asgari bilgiler dışında hangi bilgilerin açıklanmasının uygun olacağına karar verirken önemlilik kavramını esas almalı ve açıkladıkları bilgilerin doğruluğundan emin olmalıdır.

Bir bankanın açıkladığı herhangi bir bilgi, ekonomik kararlar alırken bu bilgiyi temel alan yatırımcıların kararlarını etkileyecek veya değiştirecek nitelikte bir bilgi ise önemli kabul edilmeli, açıklanan bilginin doğruluğundan ve yanlış yönlendirme yapmadığından emin olunmalıdır.

3. Bankalar risk ölçüm yöntemleri, risk büyüklükleri ve diğer hususlarda önemli değişiklikler olması durumunda denetim otoritesinin belirlediği açıklama sıklıkları dışında açıklama yaparak kamuyu bu değişiklikler hususunda bilgilendirmelidir.

Bankalar yürürlükte olan ve yürürlüğe girecek düzenlemelere uygun sıklıklarda açıklamalar yapacaklardır. Ancak bankalarda yatırımcıların kararlarını etkileyebilecek önemde değişiklikler olması durumunda açıklama dönemi gelmemiş olsa da bu değişiklikler hususunda kamuya bilgilendirme yapılması önem taşımaktadır.

4. Açıklanacak bilgilerin denetimden geçme zorunluluğu olmadığı durumlarda bu bilgilerin doğruluğundan banka yönetimi sorumludur.

Bağımsız denetimden geçmemiş bilgilerin doğruluğu konusunda sorumluluğu alan taraf banka yönetimidir. Banka yönetimi de bu sorumluluğun bilincinde olmalı, banka bünyesinde bu tür bilgilerin kontrolüne yönelik süreçlerin oluşturulması yönünde adımlar atılmasını sağlamalıdır.

5. Ticari sır niteliğindeki özel ve gizli bilgilerin açıklanmasının bankayı zarara uğratması muhtemel durumlarda konuyla ilgili genel bilgiler verilmeli ve detaylı bilginin sağlanamama gerekçesi açıklanmalıdır.

Bankalar rakiplerince bilinmesinde, üçüncü kişilere veya kamuya açıklanmasında sakınca gördükleri, gizli kalmasında hassas davrandıkları bilgiler hususunda detaylı açıklama yapmama nedenlerini belirterek genel bilgilendirme yapabilir. Banka ve müşteri sırlarının gizliliği ilkesi kapsamında bulunan ve açıklanması hukuksal boyutta cezai müeyyideye neden olabilecek bilgiler de bu kapsamda açıklanmayacaktır.

6. Bankalarda yönetim kurulu tarafından onaylanmış resmi bir bilgilendirme politikası ve açıklamaların uygunluğunu değerlendiren bir süreç bulunmalıdır.

Bankalarda bilgilendirmenin sıklığını ve kapsamını belirten, yönetim kurulu tarafından onaylanmış resmi bir bilgilendirme politikası bulunmalı, kamuyu bilgilendirme prensipleri ve süreçleri yazılı hale getirilmelidir. Bunlar düzenli olarak gözden geçirilmeli, bilgilendirmenin kapsamı belirlenmeli ve ek bilgilendirme konularının önerilmesi durumunda bu konuların kamuya açıklanmasının uygunluğu değerlendirilmelidir.

H. Bilgi Teknolojileri

1. Bilgi Teknolojileri (BT) risk yönetimi, bankaların görevlerini yapmalarına ve hedeflerine ulaşmalarına olanak sağlayan tüm süreçlerin tamamlayıcı bir parçası olmalıdır.

BT süreci, bankaların diğer süreçlerinden bağımsız bir süreç değildir. BT kontrolleri, birbirine bağlı bir koruma sürecinin bütününü oluştururlar, basit kontroller olabilecekleri gibi teknik nitelikli de olabilirler. BT kontrolleri, politikalar, süreçler, sistemler ve insanlar üzerinde genel ve teknik kontrol olanakları oluşturmak yoluyla banka yönetimini desteklerler.

BT risk yönetimi, ilgili tarafların çıkarlarını korumayı amaçlamalıdır.

BT risk kontrolleri; bankaların sermayesini korumak, özel bilgilerin gizliliği ve kimlik bilgileri gibi müşteri kaygı ve endişelerini gidermek, personelin görevini eksiksiz ve doğru olarak yaptığını kanıtlamak ve yeteneklerini göstermek ve yönetimin otomatik kontrol süreçlerin verdiği güvenceyle duyduğu rahatlığı sağlamak amacıyla gerçekleştirilir. Bu kontroller, aynı zamanda, finansal süreçlerin ve raporlamanın güvenilirliği ile ilgili güvence de sağlar.

2. BT süreçlerinde denetime tâbi olan faaliyet ve bilgiler tanımlanmalı ve kontrollerin yeterliliği değerlendirilmelidir.

Yaygınlıkla kullanılan denetim yaklaşımı, işle ilgili önemli işlemlerin otomatik sistemler tarafından işlenmesinin kurum açısından analizini içermektedir. Bu denetimlerde, denetçi, kontrole tâbi olan faaliyet ve bilgileri tanımlar ve kontrollerin güvenilirliği hakkında yeterli kanıtın mevcut olması da dahil, mevcut kontrollerin güvenilir koruma sağlama yeteneğini değerlendirir. Otomatik iş süreçlerinin içsel denetimleri sıklıkla iç kontrol eksikliklerini gösterdiğinden, iç denetçiler, bazen dikkatlerini sistemlerin tasarımı, geliştirme ve iktisabı, uygulaması ve sürdürülmesi gibi, işle ilgili faaliyetlerin otomatik hale getirildiği süreçlerin denetlenmesine kaydırabilirler veya hatta bu süreçlere katılabilirler.

BT kontrol mekanizmalarının yeterliliğini değerlendirmeye ek olarak, kontrollerin gerektiği gibi işlev görmeye devam ettiklerinden emin olmak amacıyla düzenli incelemeler ve kontroller yapılmalıdır. Mevcut iş sistemlerinin yaygın, karmaşık ve etkileşimli niteliğinden dolayı, denetim testleri, daha somut ve belirgin olarak, önemli otomatik kontroller ve veri analizi üzerinde odaklanma eğilimi gösterirler.

Bankalar işlenen veriler ve uygulamalar üzerinde ve içinde etkili kontrollere olanak sağlayan bir yöntem kullanarak uygulama yazılımlarını geliştirip değerlendirmelidir.

Bankalar, bütün sistem geliştirme projelerinde her projenin özel koşullarına uygun bir metodoloji uygulamalıdır. Uygulama yazılımları, işlenen veriler ve uygulamalar üzerinde etkili kontrollere olanak sağlayan bir yöntem kullanılarak geliştirilmelidir. Tüm bilgisayar uygulama yazılımları, kullanıcıların ihtiyaç duyduğu fonksiyonları etkin ve verimli bir şekilde sağlamalıdır.

Bütün sistem geliştirme çalışmalarında bazı temel kontrol uygulamaları yapılmalıdır:

- kullanıcı ihtiyaçları kaydedilmeli ve bunların karşılanıp karşılanmadığı ölçülmelidir.
- sistemlerin tasarımında, kullanıcı ihtiyaçlarının ve kontrollerin sisteme dahil edilmesini sağlayan bir resmi süreç izlenmeli ve uygulanmalıdır.
- yapılan testler, münferit sistem unsurlarının gerektiği gibi çalışıp çalışmadığını, sistem ara yüzlerinin beklendiği gibi işleyip işlemediğini, kullanıcıların test sürecine katılıp katılmadığını ve amaçlanan işlevselliğin sağlanıp sağlanmadığını kontrol etmelidir.
- uygulama bakım süreçleri, uygulama sistemlerindeki değişikliklerin tutarlı ve istikrarlı bir kontrol yöntemi ile yapılmasını sağlamalıdır. değişiklik yönetimi, iyi yapılandırılmış güvence doğrulama süreçlerine tâbi tutulmalıdır.
- sistemlerin geliştirilmesi hizmetinin dışarıdan alındığı durumlarda, dış kaynaktan temin sözleşmeleri veya tedarik sözleşmeleri için benzer kontroller uygulanmalıdır.

Uygulama sistemleri üzerindeki kontrollerin hedefi:

- tüm verinin amaçlandığı gibi işlenmesini,
- depolanan bütün verilerin doğru ve tam olmasını,
- bütün çıktıların doğru ve tam olmasını,
- veri girişinden depolamaya ve olası çıktıya kadar bütün veri işlemlerini takip eden kayıtların tutulmasını

sağlamaktır. Bankaların herhangi bir uygulamada görmeyi beklemesi gereken bir kaç kontrol tipi vardır:

Girdi Kontrolleri: Bu kontroller, bir iş uygulamasına girilen verilerin doğruluğunu kontrol etmek amacıyla kullanılır. Girdilerin önceden belirlenmiş parametreler içinde kalmasını sağlamak amacıyla girdi kontrolü yapılır.

Süreç Kontrolleri: Sürecin tam, doğru ve yetkilendirilmiş olmasını sağlamak amacına yönelik otomatik kontrollerdir.

Çıktı Kontrolleri: Bu kontroller, veriyle ne yapıldığını gösterir. Bunlar, fiili sonuçları hedeflenen sonuçlarla karşılaştırmalı ve bunları girdilerle kıyaslayarak kontrol etmelidir.

Doğruluk Kontrolleri: Verilerin tutarlı, uyumlu ve doğru kalmasını sağlamak amacıyla, işlenmekte olan ve/veya depolanmış bulunan verilerin izlenmesini içerir.

Yönetim İzlemesi: Veri işleme kontrolleri, yönetimin ilgili işlemleri kaynak noktasından sonuca kadar izlemesine ve kaydedilen işlemleri ve olayları tespit etmek amacıyla sonuçlardan geriye doğru izleme yapmasına olanak sağlarlar. Bu kontroller, genel kontrollerin etkililiğini izlemek için yeterli ve uygun olmalı ve hataları kaynak noktalarına mümkün olduğu kadar yakın bir yerde tespit etmelidir.

3. BT risk kontrolleri, bilgi güvenilirliği ve bilgi hizmetleri konusunda güvence sağlamalı, teknoloji kullanımından kaynaklanan risklerin azaltılmasına yardımcı olmalıdır.

BT kontrolleri, bilgi ve bilişim hizmetleri için güvence veren, bankaların teknoloji kullanımının doğurabileceği risklerin azaltılmasına yardımcı olan süreçleri kapsar. Bu kontroller, banka politikalarından, bunların şifrelenmiş talimatlarla uygulanmasına; eylem ve işlemleri izleme kabiliyeti yoluyla fiziksel erişim korumasından, bunlardan sorumlu olan kişilere ve büyük veri grupları için bilgilerde düzeltme, ek giriş ve düzenleme yapılması olanağından, makul ve uygun olup olmadığının analizine kadar farklılık gösterebilir.

4. BT risk yönetimi politikalarının koşullarını desteklemek için standartlar belirlenmelidir. Standartlar banka üst yönetimi tarafından onaylanmalı, açık ve kolay anlaşılır bir dilde ifade edilmeli ve ilgili tüm uygulamacılara iletilmelidir.

Standartlar, politikaların koşullarını desteklemek için mevcuttur. Standartların amacı, bankaların gereken hedeflere ulaşmasını sağlayacak çalışma yol ve yöntemlerini tanımlamak ve belirlemektir. Standartlar, aynı zamanda, bankaların tüm BT işletim ortamını daha etkin ve verimli işletmesini de sağlarlar.

5. Hiyerarşik görev ve sorumluluk kademelerinin tanımlanmasına ve etkili kontrol sistemlerinin uygulanmasına olanak sağlamak üzere uygun bir örgütlenme yapısı oluşturulmalıdır.

Örgütlenme ve yönetim, bankaların diğer faaliyetlerinde olduğu gibi tüm BT kontrolleri sisteminde de önemli bir rol oynar. Uygun bir örgütlenme yapısı, ilgili hiyerarşik görev ve sorumluluk kademelerinin tanımlanmasına ve etkili kontrol sistemlerinin uygulanmasına olanak sağlar.

Bankaların örgütlenme yapısı, verilerin işlenmesiyle ilgili bütün sorumluluk ve görevlerin sadece aynı kişi veya bölümde toplanmasına izin vermemelidir. Hiç bir kişinin hem bir

hata, ihmal veya başka usulsüzlüğü yaratıp hem de ona yetki verme ve/veya delilleri gizleme imkanına sahip olmamasını sağlamak amacıyla, verileri açma, yetkilendirme, girme, işleme ve kontrol etme fonksiyonları mutlaka farklı kişilerde toplanmalıdır. Uygulama sistemleri için görev ayrımı kontrolleri, sadece veri işleme fonksiyonları ve hassas bilgilere erişme ile ilgili görev ihtiyaçları ve koşullarına uygun olarak erişim imtiyazları ve haklarının verilmesi yoluyla sağlanır.

BT bakımından temel görev ayrımı, sistem geliştirme ile operasyon bölümleri arasındaki ayrımdır. Operasyon bölümü, değişiklikleri uygulama dışında tüm operatif sistemlerin işletiminden sorumlu olmalı; geliştirme süreciyle hiç bir ilişkisi olmamalıdır. Bu kontrol, operatörlerin üretim programları, sistemleri veya verilerine erişmesi veya onlarda değişiklik yapmasına engel olan kısıtlamaları da içerir. Aynı şekilde, sistem geliştirme personelinin de üretim sistemleriyle çok az ilişkisi bulunmalıdır.

I. İş Sürekliliği

1. İş sürekliliği planının etkili bir şekilde uygulanması ve geliştirilmesinden yönetim kurulu ve banka üst yönetimi sorumludur.

İş sürekliliği yönetimi bir plan dahilinde yürütülmelidir. Tüm finansal otoritelere ve finansal endüstri katılımcılarına uygulanabilen duyarlı bir iş sürekliliği yönetiminin ve bunun planlanmasının önemini ortaya koymaktadır. Nihai sorumluluk, diğer risklerin yönetiminde olduğundan farklı olarak yönetim kurulu ve üst yönetimdedir. İş sürekliliği yönetimi, kurumun risk yönetimi programının ayrılmaz bir parçasıdır. Yönetim kurulu ve üst yönetim bu planın etkili bir şekilde uygulanmasından ve geliştirilmesinden sorumludur.

Bankaların, iş sürekliliği planları hem içsel, hem de dışsal iletişim kanallarına uygun olmalıdır.

Bankalar, önemli bir operasyonel sorun olayı ile karşılaştığında hem içsel, hem de dışsal iletişim kanallarının tümüne hitap edebilecek iş sürekliliği planlarının önemini vurgulamaktadır. Bankalar için operasyonel sorun olduğu dönemlerde, hem yurt içi, hem de yurt dışı firmalarla iletişim kurabilmek çok önemlidir. Bu şekilde, özellikle sorunun ilk dönemlerinde, bu sorunun etkisini tahmin etmelerini ve buna uygun kararları almalarına yardımcı olur. İş sürekliliği planları, geniş kapsamlı acil durum iletişim protokolleri ve prosedürlerini içermelidir.

Bankaların, iş sürekliliği planları, gerektiğinde yurt dışı kurumlarla iletişim kurabilmek için bu kurumların iletişim bilgilerini de içermelidir. Bu prensip, Bankaların, herhangi bir operasyonel sorun oluştuğunda, bu tür bir olayda özel bir kavram olarak sınır ötesi iletişiminin önemini ortaya koymaktadır.

Sorunun etkisi, bazı durumlarda ulusal sınırların ötesine de uzanabilir.Bu nedenle, yerel iletişim prosedürleri kadar, uluslararası prosedürler de önem taşımaktadır. İletişim protokollerinde bu tür durumlarda aranacak kurumların listesi bulunmalıdır.Örneğin Merkez Bankaları, gözetim otoriteleri, finans ve hazine bölümleri ve 30 ülkedeki uluslararası finansal kuruluşlar olabilir.İletişimde gizli telefon numaraları, faks numaraları ve e-mail adresleri kullanılabilmelidir ve aranacak kurumların listesi düzenli olarak güncellenmelidir.

İş sürekliliği planları, dönemsel testler süresince gerekli değişikliklerin yapılabilmesine olanak sağlamalıdır.

Bu prensip, Bankaların iş sürekliliği planlarının dönemsel testler süresince gerekli değişikliklerin yapılabilecek olmasının önemini vurgular. Bu tür testler, kurumun fonksiyonlarına ve piyasa işlemlerindeki hacmine bağlı olarak dönemsel olarak yapılmalıdır. Ayrıca bağımsız bir kuruluş, örneğin iç veya dış denetim kurumunun test programının etkililiğini değerlendirmeli, test sonuçlarını gözden geçirmeli ve bulgularını üst yönetime ve yönetim kuruluna sunmalıdır. Test programlarında tüm personel yer almalıdır.

2. Bankalar, operasyonel yapılarında oluşabilecek ve faaliyetin kesintiye uğramasına yol açan aksamalar için faaliyetlerinin yapısı, özellikleri ve risk profillerine uygun iyileştirme yöntemleri geliştirmelidir.

Bankalara, operasyonel yapılarında oluşan sorunlar için bir plan yapılmasının önemini ortaya koymaktadır. Bu husus pekçok kurum için yeni olmakla birlikte bu tür olayların artma sıklığı düşünüldüğünde, konunun önemi ortaya çıkacaktır. Bankalar, bu hususa mutlaka iş sürekliliğinde yer vermeli ve kendi karakterlerine ve risk profillerine uygun, iyileştirme yöntemleri geliştirmelidir. Finansal otorite, finansal piyasaların durumunu yakından izlemeli ve kritik hizmetlerin sürdürülmesi için koordineli olarak çalışmalıdır. Bankalar, 3 önemli bölgede (yedek işyeri, fiziksel altyapı ve ana iş merkezi), iyileştirme planlarının yeterliliğini gözden geçirmelidir.

3. Bankalar, finansal sistemlerinin operasyonunda ortaya çıkan riskleri yansıtacak iyileştirme hedefleri belirlemelidirler. İyileştirme hedefleri, iyileştirme düzeyleri ve iyileştirme zamanlarını da içermelidir.

Bankalar, finansal sistemin operasyonunda ortaya çıkan riskleri yansıtacak iyileştirme hedeflerini geliştirmelidirler. İyileştirme hedefleri, iyileştirme düzeyleri ve iyileştirme zamanlarını da içermelidir. İyileştirme hedeflerinin hazırlanması yönetim kurulu ve üst yönetimin sorumluluğundadır. Bankaların iyileştirme programları finansal sistemin işlemesinde üstlendikleri riskle orantılı olmalıdır.

4. İş sürekliliği yönetimi, denetim otoritesinin incelemesine konu olmalıdır.

İş sürekliliği yönetiminin, finansal otorite tarafından incelenmesini vurgular. Finansal otoriteler kuruluşların etkili ve sürekli güncellenen bir iş sürekliliği yönetimi uygulamalarını ve geliştirmelerini beklemektedir. Bu nedenle; finansal kuruluşların iş sürekliliği planlarını değerlendirirler. Söz konusu değerlendirmeler; iyileştirme planlarını, iş sürekliliği yönetiminin kuruluşun büyüklüğü ve işletmenin amacı ile uyumlu olup olmadığı hususlarını içerir.

Dipnotlar

[1] Bu metin kapsamında, bankanın icracı fonksiyonları tanımı, bankanın gelir getiren ya da gider veya zarar oluşmasıyla sonuçlanan temel bankacılık faaliyetlerini içermektedir. "icra" sözcüğünün işaret ettiği, "uygulama, bir işi ya da fonksiyonu sürdürme ve/veya sonuçlandırma" anlamlarından bağımsız olarak, metinde yer verilmiş olan "icracı" ve "icracı fonksiyon" deyimleri, bankanın gelir ve gider hesapları üzerinde etki yaratmaya dönük faaliyetleri içermektedir.

[2] Bu metin kapsamında "üst yönetim" ibaresi, genel müdür ve genel müdür yardımcıları ile bunların eşleniği diğer unvanlardan oluşan grubu ifade etmektedir.

[3] Üst düzey yönetim: Banka Genel Müdür ve Genel Müdür Yardımcılarını ifade etmektedir.