Takasbank

İstanbul, 29/03/2016

Genel Mektup: 1276
Merkezi Karşı Taraf Bölümü

Konu: Takasbank Merkezi Karşı Taraf Üyelerinin Bilgi, Risk Yönetimi, İç Denetim ve İç Kontrol Sistemleri Hakkında Yönerge.
İlgili: Aracı Kurumlar
Bankalar

Sayın Genel Müdür,

Bilindiği üzere, 30/12/2012 tarih ve 28513 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 6362 sayılı Sermaye Piyasası Kanunu'nun 78 inci maddesinde, merkezi karşı taraf üyelerinin iç denetim ve risk yönetim sistemlerine ilişkin asgari hususların Sermaye Piyasası Kurulu'nun onayı alınmak suretiyle ilgili takas kuruluşu tarafından düzenleneceği hüküm altına alınmıştır.

Bu kapsamda, merkezi karşı taraf hizmeti alması uygun görülen üyelerin, Bankamıza olan yükümlülükleriyle ilgili üstlendikleri risklerin yönetimini ve kontrolünü sağlamak üzere kuracakları; bilgi sistemleri, risk yönetimi, iç denetim ve iç kontrol fonksiyonlarını ve bu fonksiyonların yeterliliğinin gözetimine ilişkin usul ve esasları düzenlemek amacıyla hazırlanan Merkezi Karşı Taraf Üyelerinin İç Denetim, Bilgi, Risk Yönetimi, İç Denetim ve İç Kontrol Sistemleri Hakkında Yönerge, 24/02/2016 tarihli ve 295 sayılı Takasbank Yönetim Kurulu Toplantısı'nda kabul edilmiştir.

Takasbank Yönetim Kurulu kararını müteakiben Sermaye Piyasası Kurulu'nun 10/03/2016 tarih ve 9 sayılı toplantısında onaylanan Yönerge 29/03/2016 tarihi itibariyle kurumsal internet sitemizde yayımlanmaya başlamıştır. Yönerge yayımından bir yıl sonra (30/03/2017 tarihinde) yürürlüğe girecektir.

Bilgi edinilmesini ve gereğini rica ederiz.

Saygılarımızla,

TAKASBANK
İSTANBUL TAKAS VE SAKLAMA BANKASI A.Ş.

M.Ayhan ALTINTAŞ
Direktör

Murat ULUS
Genel Müdür
Yönetim Kurulu Üyesi

Ek 1: Merkezi Karşı Taraf Üyelerinin İç Denetim, Bilgi, Risk Yönetimi, İç Denetim ve İç Kontrol Sistemleri Hakkında Yönerge

TAKASBANK MERKEZİ KARŞI TARAF ÜYELERİNİN BİLGİ, RİSK YÖNETİMİ, İÇ DENETİM VE İÇ KONTROL SİSTEMLERİ HAKKINDA YÖNERGE

İÇİNDEKİLER

TAKASBANK MERKEZİ KARŞI TARAF ÜYELERİNİN BİLGİ, RİSK YÖNETİMİ, İÇ DENETİM VE İÇ KONTROL SİSTEMLERİ HAKKINDA YÖNERGE

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak, Tanımlar ve Kısaltmalar

MADDE 1-Amaç

(1) Bu Yönergenin amacı; merkezi karşı taraf hizmeti alması uygun görülen üyelerin, Takasbank'a olan yükümlülükleriyle ilgili üstlendikleri risklerin yönetimini ve kontrolünü sağlamak üzere kuracakları bilgi sistemleri, risk yönetimi, iç denetim ve iç kontrol faaliyetlerine ve bu faaliyetlerin Yönerge hükümleri açısından yeterliliğinin gözetimine ilişkin usul ve esasları düzenlemektir.

MADDE 2-Kapsam

(1) Takasbank'ın merkezi karşı taraf olarak hizmet verdiği organize piyasalarda işlem yapma yetkisi olan üyeler ile İstanbul Takas ve Saklama Bankası Merkezi Karşı Taraf Yönetmeliği'nin 16 ncı maddesinde belirtilen yükümlülükler ile sınırlı olmak üzere işlemci kuruluşlar bu Yönerge kapsamındadır. Üyelerin tabi oldukları özel mevzuatta bilgi sistemleri, risk yönetimi, iç denetim ve iç kontrol faaliyetleri hakkında yapılan düzenlemeler saklıdır.

MADDE 3-Dayanak

(1) Bu Yönerge 30/12/2012 tarih ve 28513 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren 6362 sayılı Sermaye Piyasası Kanunu'nun 78 inci maddesinin dördüncü fıkrası ile 14/08/2013 tarih ve 28735 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren İstanbul Takas ve Saklama Bankası Anonim Şirketi Merkezi Karşı Taraf Yönetmeliği'nin 7 nci maddesinin birinci fıkrasının (ç) bendi ve 8 inci maddesinin ikinci fıkrasına dayanılarak hazırlanmıştır.

MADDE 4-Tanımlar ve kısaltmalar

(1) Bu Yönergenin uygulanmasında;

a) **Doğrudan Merkezi Karşı Taraf Üyesi:** İstanbul Takas ve Saklama Bankası Anonim Şirketi Merkezi Karşı Taraf Yönetmeliği hükümleri uyarınca sadece kendisinin ya da müşterilerinin takas işlemlerini gerçekleştirmeye yetkili üyeleri,

b) **Genel Merkezi Karşı Taraf Üyesi:** İstanbul Takas ve Saklama Bankası Anonim Şirketi Merkezi Karşı Taraf Yönetmeliği hükümleri uyarınca kendisinin ya da müşterilerinin takas işlemlerinin yanı sıra işlemci kuruluşların da takas işlemlerini gerçekleştirmeye yetkili üyeleri,

c) **İşlemci Kuruluş:** Takasbank'ın MKT olduğu piyasa veya sermaye piyasası araçlarında işlem yapan ancak söz konusu işlemlere ilişkin yükümlülüklerin tasfiyesini bir genel MKT üyesi aracılığı ile gerçekleştiren kuruluşları,

ç) **İz Kaydı (Denetim izi):** Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları,

d) **Kanun:** 06/12/2012 Tarihli ve 6362 Sayılı Sermaye Piyasası Kanununu,

e) **Kurul:** Sermaye Piyasası Kurulunu,

f) **MKT:** Merkezi Karşı Tarafı,

g) **MKT Hizmeti:** Takasbank'ın, Kurul tarafından uygun görülen piyasa veya sermaye piyasası araçlarında açık teklif, sözleşme yenileme veya hukuken bağlayıcılığı olan başka bir yöntemle alıcıya karşı satıcı, satıcıya karşı da alıcı rolünü üstlenerek takasın tamamlanmasını taahhüt ettiği faaliyeti,

ğ) **Merkezi Karşı Taraf Yönetmeliği:** 14/08/2013 tarih ve 28735 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren İstanbul Takas ve Saklama Bankası Anonim Şirketi Merkezi Karşı Taraf Yönetmeliğini,

h) **Takasbank:** İstanbul Takas ve Saklama Bankası Anonim Şirketi'ni,

ı) **Üye:** Takasbank'ın, Merkezi Karşı Taraf olarak faaliyet gösterdiği organize piyasalarda işlem yapma yetkisi olan genel veya doğrudan merkezi karşı taraf üyesini,

i) **Üst yönetim:** Üyenin genel müdür ve genel müdür yardımcıları ile birim yöneticilerini,

j) **Yönetim kurulu:** Üyenin yönetim kurulunu

ifade eder.

İKİNCİ BÖLÜM

Genel Esaslar

MADDE 5- İç denetim, iç kontrol ve risk yönetim sistemlerinin kurulması

(1) Üyeler, Takasbank tarafından verilen MKT hizmetleriyle bağlantılı olarak maruz kaldıkları risklerin izlenmesi ve kontrolünün sağlanması amacıyla, faaliyetlerinin kapsamı ve yapısıyla uyumlu ve değişen koşullara cevap verebilecek nitelikte yeterli ve etkin iç denetim, iç kontrol ve risk yönetim sistemleri kurmak ve işletmekle yükümlüdürler.

MADDE 6-Bilgi sistemlerinin kurulması

(1) Üyeler, MKT hizmetlerine ilişkin; ürettikleri, işledikleri, ilettikleri ve sakladıkları verinin güvenliğini, sürekliliğini ve bütünlüğünü sağlayacak bilgi sistemlerini kurmak ve işletmekle yükümlüdürler.

MADDE 7-Yönetim kurulunun sorumlulukları

(1) Üyeler nezdinde iç denetim, iç kontrol ve risk yönetimi sistemlerinin oluşturulması, etkin, yeterli ve uygun bir şekilde işletilmesi, muhasebe ve finansal raporlama sisteminden sağlanan bilgilerin doğruluğu, güvenilirliği ve muhafazası hususlarında her türlü tedbirin alınması, yetki ve sorumlulukların belirlenmesi yönetim kurulunun sorumluluğundadır.

ÜÇÜNCÜ BÖLÜM

Risk Yönetim Sistemine İlişkin Esaslar

MADDE 8-Risk yönetim sistemi

(1) Risk yönetim sisteminin amacı, üyenin asgari olarak Takasbank'ın MKT hizmeti verdiği piyasalardaki faaliyetlerinden dolayı maruz kaldığı riskleri izlemeye, kontrol altında tutmaya ve gerektiğinde azaltmaya yönelik olarak belirlenen politikalar, uygulama usulleri ve limitler vasıtasıyla risklerin yönetilmesini sağlamaktır.

(2) Üye; Takasbank'ın MKT hizmeti verdiği piyasa veya sermaye piyasası araçlarında taşıdığı ve alacağı pozisyonların doğuracağı riski ve teminat gereksinimini Takasbank ile uyumlu yöntemlerle hesaplar.

(3) Üyenin risk yönetim sistemi, üyeliğe ilişkin faaliyetlerin tamamını ve bunları doğrudan etkileyebilecek diğer süreçlerini de kapsayacak şekilde tesis edilir ve uygulanır.

(4) Risk yönetim sistemi, sistemin temel prensip ve varsayımları ile istisnai durumlara ilişkin onay süreçleri açık ve detaylı olacak şekilde yazılı hale getirilir ve yönetim kurulu tarafından onaylanarak yürürlüğe girer.

(5) Tüm risk yönetim sistemi, asgari olarak yılda bir kez gözden geçirilir. Gözden geçirme süreci MKT Yönetmeliğine uyumun yanı sıra asgari olarak;

a) Risk ölçüm sürecinde gerçekleşen tüm önemli değişikliklerin doğrulanması,

b) Pozisyonlara ilişkin verilerin doğruluk ve tamlığı,

c) Teminatlara ilişkin verilerin doğruluk ve tamlığı,

ç) Pozisyon ve kredi limitlerinin; doğruluk, tamlık ve uygunluğu,

d) Teminat değerleme yöntemlerinin doğruluğu

hususlarını içerir.

(6) Üye, MKT Yönetmeliğine ve faaliyet gösterdiği piyasalara ilişkin Takasbank tarafından uygulanan limitlere uyumu gün içerisinde ve gün sonunda kontrol eder.

(7) MKT üyesi, kendi işlemlerinden ve müşterilerinin aldığı pozisyonlardan kaynaklanan riskler sonucunda garanti fonunun kendisine ait katkı payında meydana gelebilecek değişiklikleri günlük olarak hesaplar ve izler.

(8) Genel MKT üyesi ile işlemci kuruluş arasında yapılan sözleşmede; işlemci kuruluşun yükümlülüklerini kısmen veya tamamen yerine getirmediğinin tespiti halinde Genel MKT üyesinin işlemci kuruluştan risk azaltıcı işlem yapmasını talep etme ve işlemci kuruluşun risk azaltıcı işlemi yapmaması durumunda işlemci kuruluş adına risk azaltıcı işlemleri re'sen yapma yetkisine yer verilir.

MADDE 9-Teminatlandırma esasları

(1) Teminat gereksinimlerinin hesaplanmasında, asgari olarak MKT tarafından belirlenen kural, yöntem ve parametreler esas alınır.

(2) Üye, emirleri Borsa'nın emir sistemine göndermeden önce, emrin gerçekleşmesi durumunda portföyün veya müşterinin yeni emirle birlikte maruz kalacağı olası riskin ölçümüne ve buna göre emrin kabul edilmesi durumunda gerekecek ek teminata ilişkin kontrolleri gerçekleştirir.

(3) Üye, Takasbank'ın MKT hizmeti verdiği piyasalara ilişkin prosedürlerde belirtilen pozisyon ve risk limitleri ile uyumlu limit kontrol mekanizmasını kurar.

(4) Teminatlandırma ve teminat izleme yöntemlerine ilişkin prosedürler, açık ve detaylı olarak yazılı hale getirilir ve yönetim kurulu tarafından onaylanarak yürürlüğe girer.

(5) Üye, teminatlandırma yöntemi ve teminatların kullanımına ilişkin esaslar hakkında internet sitesi üzerinden müşterilerini bilgilendirir. Söz konusu bilgilerin internet sitesi üzerinden duyurulacağına ilişkin olarak müşteriler başlangıçta bir defaya mahsus olmak üzere yazılı olarak bilgilendirilir.

(6) Teminatlandırma parametrelerinin girilmesine ilişkin asgari olarak, ilgili parametrelerin tek bir kişi tarafından değiştirilmesini engelleyecek ve yetkisiz değişiklikleri tespit edecek kontrol mekanizmaları tesis edilir.

(7) Risk ve teminat gereksinim hesaplamaları, asgari olarak Merkezi Karşı Taraf Yönetmeliği'nin 25 inci maddesinde hüküm altına alınan ayrıştırma paralelinde gerçekleştirilir.

(8) Türev piyasalarda işlem yapan üyeler, Takasbank tarafından ilgili piyasa için belirlenen ve Kurul tarafından onaylanan brüt, net ve/veya portföy bazlı teminatlandırma yöntemlerinden birini uygularlar.

MADDE 10-Stres testleri

(1) Stres testleri, üyenin finansal durumunu önemli ölçüde etkileyebilecek faktör ve olayları kapsayacak şekilde ve "Aracı Kurumların Sermayelerine ve Sermaye Yeterliliğine İlişkin Esaslar Tebliği" hükümleri uyarınca hesaplanan sermaye yeterliliği ile ilişkilendirilerek tasarlanır. Stres testlerinde kullanılacak senaryolar, risk karşılığı ya da faaliyet giderleri değerlerinde aşırı değişikliklere yol açacak ya da risk yönetimi için kullanılan araçları olumsuz etkileyecek olan; dayanak varlık değeri, fiyat oynaklığı ve faiz oranı gibi faktörlerdeki gerçekleşme ihtimali düşük olsa da önemli düzeyde kayıplar oluşturabilecek senaryolar ile yaşanabilecek önemli operasyonel kayıplar dikkate alınarak hazırlanır. Stres testlerinin sonuçları ve stres testinde kullanılan metodoloji ve varsayımlar, yönetim kuruluna sunulur ve bu sonuçların üyenin karar alma mekanizmalarına dâhil edilmesi sağlanır.

(2) Stres testleri, genel MKT üyeleri tarafından yıl içerisinde asgari olarak Haziran ve Aralık dönemleri için iki kez, doğrudan MKT üyeleri tarafından ise asgari olarak bir kez Aralık dönemi için yapılır.

DÖRDÜNCÜ BÖLÜM

Bilgi Sistemlerinin Yönetimine İlişkin Esaslar

MADDE 11-Bilgi güvenliği

(1) Üyeler, bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak amacıyla; saklanan, iletilen, işlenen ve üretilen verileri gizlilik, erişilebilirlik ve bütünlük açısından önem derecelerine uygun olarak tasnif eder ve bu dereceler için uygulanması gereken asgari güvenlik kontrollerini belirler, Yönetim Kuruluna onaylatır ve işletir.

(2) Genel MKT üyeleri, genel MKT üyesi olarak hizmet verdiği işlemci kuruluşların ve bu kuruluşların müşterilerinin bilgilerinin gizliliğini sağlamak ve bu bilgilere erişimi, görevi gereği bu bilgileri bilmesi gereken personel ile sınırlamak ile yükümlüdür.

MADDE 12-Erişim ve yetkilendirme

(1) Yetkilendirme sürecinin işletilmesinde, görev tanımları göz önünde bulundurularak gerekli en düşük yetkinin verilmesi prensibi esas alınır.

(2) Yetkilendirme mekanizması, hiçbir kullanıcı, taraf ya da sistemin kendi yetkilerini ve erişim haklarını onaysız yükseltmesine izin vermeyecek şekilde tasarlanır ve işletilir.

(3) Üyeler, ayrıcalıklı yetkiye sahip kullanıcılar için mümkün olan en geniş seviyede iz kayıtlarını tutar ve bu kayıtların bu kullanıcılar ve kullanıcılara bağlı personel haricindeki kişiler tarafından düzenli olarak riskli işlemler açısından gözden geçirilmesini sağlar.

(4) Üyeler, erişilen sistemler ya da verilerin gizliliğine uygun olarak tesis edilmiş yetkilendirme kontrollerini ve bu kontrollerin asgari olarak yılda bir kez gözden geçirilmesini sağlayacak süreçleri tesis eder.

MADDE 13-Kimlik doğrulama

(1) Üyeler, erişilen sistemler ya da verilerin gizliliğine uygun olarak tesis edilmiş kimlik doğrulama kontrollerini ve bu kontrollerin asgari olarak yılda bir kez gözden geçirilmesini sağlayacak süreçleri tesis eder.

(2) Uygulanacak olan kimlik doğrulama mekanizmaları, oturumun başından sonuna kadar geçen tüm süreyi kapsayacak biçimde tesis edilir.

(3) Uzaktan erişimlerde, kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek kontroller tesis edilir.

(4) Kimlik doğrulama verileri şifreli olarak saklanır ve bu verilerin aktarım sırasında güncel ve güvenli bir şifreleme algoritması ile şifrelenmesi sağlanır.

MADDE 14-İz kayıtları

(1) Yetkilendirme sistemleri ile diğer kritik sistemlerdeki kayıtlarda değişikliğe sebep olabilecek durumlar için asgari olarak;

a) Erişim ya da erişim teşebbüsünü gerçekleştiren kişiye,

b) İşlem ya da teşebbüsün zamanına,

c) İşlem ya da teşebbüsün doğasına (yaratma, güncelleme, silme, okuma ya da erişim)

ilişkin bilgileri içeren iz kayıtları tutulur.

(2) Üye nezdinde saklanan veriler ve gerçekleştirilen işlemlere ilişkin uygun seviyede bütünlük ve inkâr edilemezlik kontrolleri tesis edilir ve bu kontroller yeterli iz kayıtları ile desteklenir.

(3) Bu madde kapsamında tutulan iz kayıtları asgari olarak 5 yıl boyunca saklanır.

(4) İz kayıtlarının, kayıtları üreten sistemlerde yönetici hakkına sahip personel tarafından silinememesi ya da değiştirilememesi için gerekli kontroller tesis edilir.

MADDE 15-Birincil sistemler

(1) Üye, üyeliğin gerektirdiği yükümlülüklerin yerine getirilmesi için önem arz eden fonksiyonları destekleyen bilgi teknolojileri hizmetlerinin verildiği birincil sistemlerini yurtiçinde bulundurur.

MADDE 16-İkincil sistemler

(1) Üye, üyeliğin gerektirdiği yükümlülüklerin yerine getirilmesi için önem arz eden fonksiyonları destekleyen bilgi teknolojileri hizmetlerinin verildiği birincil sistemlerde kesinti olması halinde yükümlülüklerin yerine getirilmesini mümkün kılacak yedek sistemleri teşkil eden ikincil sistemleri yurtiçinde bulundurur.

MADDE 17-İş sürekliliği

(1) Üye, üyeliğin gerektirdiği yükümlülüklerin yerine getirilmesi için önem arz eden fonksiyonları destekleyen bilgi teknolojileri hizmetlerinin sürekliliğini sağlar. Bu amaçla, bilgi teknolojileri hizmetleri için; kurtarma hedefleri ve tahammül edilebilir kesinti sürelerinin belirlendiği ve bu hedefler ile uyumlu süreklilik eylemlerinin yer aldığı iş sürekliliği planları hazırlanır.

(2) İş sürekliliği planları, kurtarma ve yedekten dönme süreçlerini de içerir ve ilgili hizmet ya da sistemlerde gerçekleşen değişikliklerin planlara zamanında yansıtılması sağlanır.

(3) Planda yer alan eylemler düzenli olarak test edilir ve test sonuçları üst yönetime raporlanır. Test sonuçları, süreklilik planlarında güncelleme ihtiyacı olup olmadığının değerlendirilmesinde kullanılır ve varsa değişiklikler yapılarak planların güncelliği sağlanır.

MADDE 18-Yedekleme

(1) İş sürekliliği planında belirtilen kurtarma hedefleriyle uyumlu olacak şekilde verilerin yedekleme periyodları belirlenir. Asgari olarak; Yönergede tutulması öngörülen bilgilerin, ayrıcalıkların, bilgi işlem altyapısı yapılandırmalarının, kayıtların ve veri tabanının yedekleri alınır.

(2) Alınan yedeklerin, birincil sistemlerle aynı anda aynı fiziksel tehditlere maruz kalmayacak bir alanda saklanması sağlanır. Yedeklerin alındığı kartuş, manyetik teyp

ve benzeri ortamların zaman içerisinde bozulmasını engellemek ve bu ortamları korumak için uygun saklama koşulları sağlanır.

(3) Yedeklerin alınması esnasında ve saklama süreleri boyunca, yedeklenen verilerin tamlığına ve bütünlüğüne dair güvence sağlayacak kontroller tesis edilir.

MADDE 19-Görevler ayrılığı ilkesi

(1) Bilgi sistemlerine ilişkin; uygulama geliştirme, test etme, sistem yönetimi ve operasyon fonksiyonlarında görevler ayrılığı ilkesi gözetilir. Bu ilke çerçevesinde, kritik bir işlemin tek bir personel ya da tek bir destek hizmeti kuruluşu tarafından sisteme girilmesi, onaylanması ve tamamlanmasına imkân vermeyecek kontroller tesis edilir.

(2) Görevler ayrılığı ilkesinin tam anlamıyla işletilmesinin mümkün olmadığı durumlarda, bu durumlardan kaynaklanabilecek hata ve suiistimallere yönelik risk azaltıcı ya da telafi edici risk yanıtları uygulanır. Bu durumlar ve durumlara ilişkin belirlenen risk yanıtları Yönetim Kurulu tarafından onaylanır.

MADDE 20-Fiziksel güvenlik ve çevre güvenliği

(1) Bilgi işlem altyapısını; yangın, duman, sel, deprem ve diğer doğal afetler ile elektrik kesintisi, patlama, hırsızlık, terör ve yıkıcılık olaylarından makul seviyede koruyacak fiziksel güvenlik tedbirleri alınır.

(2) Bilgi işlem altyapısına fiziksel erişimin sadece yetkili kişilerce yapılması için fiziksel güvenlik tedbirleri alınır.

MADDE 21-Ağ güvenliği

(1) Kritik bilgi işlem bileşenlerine gerek yerel ağ gerekse de dış ağ üzerinden gerçekleştirilen erişim kısıtlanır ve sadece yetkilendirilmiş kullanıcıların ve servislerin erişimine izin verecek kontroller tesis edilir.

(2) Bilgi işlem altyapısına uzaktan yapılan tüm erişimlerde iletişim güvenliği sağlanır. Uzaktan erişimlerde, kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek kontroller tesis edilir.

(3) Uzaktan erişim yapılacak servisler belirlenir ve buna uygun olarak ağ altyapısında gerekli kısıtlamalar yapılır.

Bilgi işlem altyapısına yapılacak olası saldırıları tespit etmek ve önlemek amacıyla gerekli tedbirler alınır.

BEŞİNCİ BÖLÜM
İç Denetim Sistemine İlişkin Esaslar

MADDE 22-İç denetim sistemi

(1) İç denetim sisteminin amacı, üst yönetime üye faaliyetlerinin Kanun ve ilgili diğer mevzuat ile üyenin belirlediği strateji, politika, ilke ve hedefler doğrultusunda yürütüldüğü ve iç kontrol ve risk yönetimi sistemlerinin etkinliği ve yeterliliği hususunda güvence sağlamaktır.

(2) Üyeler, iç denetim sisteminden beklenen amacın sağlanabilmesi için, iç denetim birimlerini kurar ve bu birimlerde yeterli sayıda denetim elemanı bulundurur.

MADDE 23-Dönemsel ve riske dayalı iç denetim

(1) İç denetim faaliyetleri, merkezi karşı taraf üyeliğine ilişkin faaliyetlerin doğurduğu tüm riskleri de kapsayan risk değerlendirmeleri esas alınarak gerçekleştirilir.

(2) Risk değerlendirmeleri, iç denetim birimi tarafından tüm işlemler, süreçler ve hizmetleri kapsayacak şekilde;

a) İşlem, süreç ve hizmetlere ilişkin mevzuat konuları,

b) İşlem, süreç ve hizmetlerin üyelik açısından taşıdığı riskler ve bu risklere ilişkin tesis edilmiş olan kontroller,

c) Risk yönetimi ile görevlendirilmiş bir birim olması durumunda birim tarafından gerçekleştirilen risk değerlendirmeleri,

ç) Diğer birimler tarafından denetim birimine bildirilen önemli mevzuat değişiklikleri,

gözetilerek, yılda en az bir kez gerçekleştirilir ve Yönetim Kurulu'na sunulur.

(3) Riske dayalı denetimlerde, iç denetim birimi nihai karar almadan üst yönetimin görüşlerini alır. Her halükarda değerlendirmelere ilişkin nihai karar alma yetkisi iç denetim birimindedir.

(4) Riske dayalı denetimlerin düzenli olarak gözden geçirilmesi, değerlendirmeleri etkileyecek değişikliklerin değerlendirmelere yansıtılmasını mümkün kılacak iletişim kanallarının tesis edilmesi ve değerlendirmelerin gerekli durumlarda güncellenmesi iç denetim biriminin sorumluluğundadır.

(5) Üyeliğe ilişkin mevzuata uyum, asgari yılda bir kez iç denetim faaliyetlerine konu edilir.

MADDE 24-İç denetim planı

(1) İç denetim faaliyetleri, gerçekleştirilen risk değerlendirmeleri esas alınarak planlanır.

(2) Planın hazırlanması esnasında, ürün ve hizmet yapısında gerçekleştirilmesi öngörülen önemli değişikliklerin denetim dönemlerine dâhil edilmesi esastır.

(3) İç denetim planlarında asgari olarak;

a) Risk değerlendirmeleri neticesinde belirlenen önem ve risk sıralamalarına,

b) Denetim çalışmalarının amaç ve hedeflerine,

c) Denetlenecek işlem, süreç ve hizmetlere ilişkin özet risk değerlendirmelerine,

ç) Denetime konu işlem, süreç ve hizmetlerin tabi olduğu mevzuata,

d) Denetim çalışmalarının planlanan zamanına ve denetim dönemine,

e) Planlanan denetim çalışmaları için gerekli olan kaynaklara ve kaynak kısıtlamalarının olası etkilerine

yer verilir.

(4) İç denetim planı, Yönetim Kurulunun onayı ile yürürlüğe girer.

MADDE 25-İç denetim birimi

(1) İç denetim faaliyetlerinin yürütülmesi için doğrudan yönetim kuruluna bağlı olarak çalışan bir iç denetim birimi görevlendirilir. İç denetim birimi; yönetim kurulu içinde tesis edilmiş, icraî görevi bulunmayan ve denetim ile gözetim faaliyetlerinin yerine getirilmesine yardımcı olmak üzere kurulan denetim komitesine bağlı olarak da görevlendirilmesi mümkündür.

(2) İç denetim birimi yöneticisi ve denetim personelinin, yönetim kurulu ya da denetim komitesi haricinde hiçbir kişiye karşı hesap verme sorumluluğunun bulunmaması sağlanır.

(3) İç denetim personelinin görevlerini ifa edebilmeleri için üyenin tüm bilgi ve belgelerine, herhangi bir kısıtlama olmadan erişmeleri sağlanır.

MADDE 26-İç denetim faaliyetleri

(1) Gerçekleştirilen iç denetim çalışmaları rapora bağlanarak yönetim kuruluna sunulur. Denetim raporlarına mesnet teşkil eden denetim çalışmaları, çalışma kâğıtları ile belgelenir ve bahse konu çalışma kâğıtları denetim çalışmalarının tamamlanması ile birlikte denetim birimine tevdi edilerek asgari olarak beş yıl süreyle saklanır.

(2) İç denetim raporlarında asgari olarak;

a) Denetim kapsamı ve amaçlarına,

b) Denetim çalışmalarının sonuçlarına,

c) Tespit edilen sorunlara,

ç) Üst yönetim tarafından ihtiyaç duyulabilecek diğer bilgilere

yer verilir.

(3) İşlemci kuruluşların genel MKT üyeleri tarafından garanti edilen faaliyetleri, esasları sözleşmede belirlenmek şartıyla, genel MKT üyesinin iç denetim birimi tarafından denetlenebilir.

ALTINCI BÖLÜM

İç Kontrol Sistemine İlişkin Esaslar

MADDE 27-İç kontrol sistemi

(1) İç kontrol sisteminin amacı, üye ve müşteri varlıklarının korunmasını, merkez dışı örgütleri dâhil tüm iş ve işlemlerinin yönetim stratejisi ve politikalarına uygun olarak düzenli, verimli ve etkin bir şekilde mevcut mevzuat ve kurallar çerçevesinde yürütülmesini, hesap ve kayıt düzeninin bütünlüğünün ve güvenilirliğinin, veri sistemindeki bilgilerin zamanında ve doğru bir şekilde elde edilebilirliğinin, hata, hile ve usulsüzlüklerin önlenmesi ve tespitini sağlamaktır.

(2) İç kontrol sisteminden beklenen amacın sağlanabilmesi için;

a) Üye bünyesinde görevler ayrılığı ilkesine bağlı olarak işlevsel görev ayrımının tesis edilmesi ve sorumlulukların paylaştırılması,

b) Muhasebe ve finansal raporlama sisteminin, bilgi sisteminin ve iletişim kanallarının tesis edilmesi,

c) İş sürekliliği planı ve ilgili diğer planların hazırlanması,

ç) İç kontrol faaliyetlerinin oluşturulması,

d) Üyenin iş süreçleri üzerinde kontrollerin ve iş adımlarının gösterildiği iş akış şemalarının oluşturulması, söz konusu iş akış prosedürlerinde; günlük, haftalık veya aylık periyotlarda kontrol edilecek hususların açık olarak belirlenmesi,

e) Üyenin iç kontrol sistemlerine ilişkin tüm politika ve prosedürlerini yazılı hale getirmeleri ve bunların yürürlüğe konulması için yönetim kurulu tarafından onaylanmış olması

zorunludur.

MADDE 28-İç kontrol faaliyetleri

(1) İç kontrol sistemi kapsamındaki faaliyetler, yönetim kurulu, üyenin her seviyedeki personeli ile münferiden kurulmuş bir iç kontrol birimi, iç kontrol birimi olmadığı takdirde ise iç denetimden sorumlu elemanlar tarafından yürütülür.

(2) Üyelerin iç kontrol faaliyetleri, tespit edilen risklerin de izlenmesine olanak verecek şekilde günlük faaliyetlerin ayrılmaz bir parçası olarak düzenlenir ve sürdürülür.

(3) Genel MKT üyesi, genel MKT üyesi olarak hizmet verdiği işlemci kuruluşların ve bu kuruluşların müşterilerinin varlık ve yükümlülüklerinin, kendisinin ve müşterilerinin varlık ve yükümlülüklerinden tamamen ayrıştırmaya imkân sağlayan bir muhasebe sistemi kurar ve işletir.

YEDİNCİ BÖLÜM

Çeşitli ve Son Hükümler

MADDE 29-Takasbank'ın denetim yapma ve bilgi isteme yetkisi

(1) Takasbank, üyenin taşıdığı riske bağlı olarak belirleyeceği sıklıkta ve formatta üyelerden bilgi talep edebilir ve üyelerin genel merkez ve şubelerinde yerinde denetim yapabilir.

MADDE 30-Alınacak önlemler

(1) Takasbank tarafından üyenin iç denetim, iç kontrol, risk yönetimi ve bilgi sistemlerinin taraf olunan MKT hizmetleri ile bağlantılı olarak üstlenilen risklerin kontrol ve yönetiminde yetersiz kaldığı tespit edildiğinde, eksikliklerin mahiyetine göre üye hakkında doğrudan MKT Yönetmeliği ve ilgili diğer mevzuatta öngörülen tedbirler uygulanabileceği gibi, eksikliklerin giderilmesi için makul bir süre de tanınabilir. Verilen süreye rağmen eksikliklerini tamamlayamayan ve üyelik şartlarını kaybettiği kanaatine ulaşılan üyeler hakkında MKT Yönetmeliği'nin 15 inci maddesi tatbik olunur.

MADDE 31-Yönergede hüküm bulunmayan haller

(1) Yönergede hüküm bulunmayan durumlarda, üyenin tabi olduğu ilgili mevzuat hükümleri uygulanır.

MADDE 32-Yürürlük

(1) Bu Yönerge yayım tarihinden 1 yıl sonra yürürlüğe girer.

MADDE 33-Yürütme

(1) Bu Yönerge hükümlerini Takasbank Yönetim Kurulu yürütür.