SİGORTACILIK VE ÖZEL EMEKLİLİK SEKTÖRLERİNDE İÇ SİSTEMLERE DAİR YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 – (1) Bu Yönetmeliğin amacı; sigorta, reasürans ve emeklilik şirketlerinin, sigortacılık ve özel emeklilik sektörlerinde faaliyet gösteren özellikli kuruluşların ve tüzel kişiliği haiz sigorta ve reasürans brokerlerinin kuracakları iç kontrol, risk yönetimi, aktüerya ve iç denetim sistemlerine ve bunların işleyişine ilişkin usul ve esasları düzenlemektir.

(2) Bu Yönetmelik; Türkiye'de kurulu sigorta, reasürans ve emeklilik şirketlerini, yabancı sigorta ve reasürans şirketlerinin Türkiye'deki teşkilatlarını, Güvence Hesabını, Sigorta Bilgi ve Gözetim Merkezini, Emeklilik Gözetim Merkezini, Sigorta Tahkim Komisyonunu, Türkiye Motorlu Taşıt Bürosunu, Doğal Afet Sigortaları Kurumunu, Özel Riskler Yönetim Merkezini ve tüzel kişiliği haiz sigorta ve reasürans brokerlerini kapsar.

Dayanak

MADDE 2 – (1) Bu Yönetmelik; 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanununun 4 üncü, 14 üncü, 21 inci, 28 inci, 30 uncu, 31/B inci, 32 nci, 33/A ıncı ve ek 1 inci maddeleri; 9/5/2012 tarihli ve 6305 sayılı Afet Sigortaları Kanununun 6 ncı maddesi ile 28/3/2001 tarihli ve 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununun 1 inci ve 20/A maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 – (1) Bu Yönetmelikte geçen;

a) Ana hizmetler: Kuruluşların esas faaliyetlerini icra edebilmeleri amacıyla yürütülen ve devamlı olarak sürdürülmesi zorunlu olan hizmetleri,

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

c) Birincil sistemler: Sigortacılık ve özel emeklilik faaliyetlerinin yürütülmesi ve Kanunda, Kanuna ilişkin alt düzenlemelerde ve ilgili diğer mevzuatta bu kuruluşlar için tanımlanan esas faaliyet konusuyla ilgili tüm sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilerin, elektronik ortamda güvenli ve istendiği an erişime imkân sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamını,

ç) Birlik: Türkiye Sigorta Reasürans ve Emeklilik Şirketleri Birliğini,

d) COBIT: Bilgi Sistemleri Denetim ve Kontrol Birliği (ISACA) Bilgi Teknolojileri Yönetişim Enstitüsü (ITGI) tarafından yayımlanmış olan Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (COBIT)'nin güncel versiyonu veya Kurumca kabul edilen versiyonlarını,

e) Denetim komitesi: Asgari olarak icrai görevi bulunmayan iki yönetim kurulu üyesinden oluşan ve denetim ve gözetim faaliyetlerinin yerine getirilmesinde yönetim kuruluna yardımcı olmak üzere kurulan komiteyi,

f) Finansal grup: Hukuksal yönden birbirinden bağımsız olsa bile; sermaye, yönetim ve denetim açısından birbiriyle ilişkili ve içlerinden en az bir tanesi sigorta, reasürans veya emeklilik şirketi olmak şartıyla ortaklıklarının tümü veya çoğunluğu finansal kuruluş olan şirketler bütününü,

g) İcrai birim: Doğrudan gelir getirici, harcama yapıcı veya operasyonel faaliyetlerin icra edildiği birimi,

ğ) İç sistemler: 5684 sayılı Kanunun 4 üncü maddesinde belirtilen sistemler ile aktüerya fonksiyonunu,

h) İkincil sistemler: Birincil sistemler dışında kalan faaliyetlerin yürütüldüğü sistemler ile tüm sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve Kanunda, Kanuna ilişkin alt düzenlemelerde ve ilgili diğer mevzuatta kuruluşlar için tanımlanan tüm

sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istendiği an erişilmesini sağlayan birincil sistem yedeklerini,

ı) İş sürekliliği planı: İş sürekliliği yönetiminin bir parçası olan ve bir kesinti durumunda kuruluşların öncelikleriyle uyumlu olarak faaliyetlerin sürdürülmesine ve mevzuata uyum sağlanmasına yönelik politika, standart ve prosedürlerden oluşan yazılı plan veya planlar bütününü,

i) İş sürekliliği yönetimi: Savaş, terör olayları, grev, lokavt, kargaşalık, salgın hastalıklar, yangın ve doğal afetler ve bilişim tabanlı saldırılar ile iş ortaklarındaki iş kesintileri gibi nedenlere bağlı olarak oluşabilecek bir kesinti veya kriz durumunda etkin önlem alınabilmesi; itibarın, marka değerinin, değer katan faaliyetlerin ve paydaşların çıkarlarının korunabilmesi amaçlarıyla belirlenen operasyonların sürekliliğinin temin edilmesi veya hedeflenen zaman diliminde kurtarılabilmesinin sağlanması ile kriz öncesi duruma dönülmesine yönelik, potansiyel risklerin belirlenmesini de içeren politika, standart ve prosedürleri kapsayan bütünsel yönetim sürecini,

j) Kanun: 3/6/2007 tarihli ve 5684 sayılı Sigortacılık Kanunu ile 28/3/2001 tarihli ve 4632 sayılı Bireysel Emeklilik Tasarruf ve Yatırım Sistemi Kanununu,

k) Kesinti: Kuruluşların faaliyetlerinde veya bir sistemin fonksiyonlarında sürekliliğin, planlı geçişler haricinde mücbir sebeplerle sekteye uğramasını,

l) Konsolidasyona tabi ortaklık: Türkiye finansal raporlama standartları kapsamında tanımlanan kontrol gücüne sahip olunan tüm ortaklıkları,

m) Kurul: Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurulunu,

n) Kuruluş: Bu Yönetmelik kapsamında tanımlanan şirketler, özellikli kuruluşlar ve tüzel kişiliği haiz sigorta ve reasürans brokerlerinin tamamını,

o) Kurum: Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumunu,

ö) Özellikli Kuruluşlar: Güvence Hesabını, Sigorta Bilgi ve Gözetim Merkezini, Emeklilik Gözetim Merkezini, Sigorta Tahkim Komisyonunu, Türkiye Motorlu Taşıt Bürosunu, Doğal Afet Sigortaları Kurumunu ve Özel Riskler Yönetim Merkezini,

p) Rehber: T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayımlanan bilgi ve iletişim güvenliği rehberini,

r) Sigorta grubu: Hukuksal yönden birbirinden bağımsız olsa bile; sermaye, yönetim ve denetim açısından birbiriyle ilişkili sigorta, reasürans ve emeklilik şirketleri bütününü,

s) Şirket: Türkiye'de kurulmuş sigorta, reasürans ve emeklilik şirketleri ile yabancı ülkelerde kurulmuş sigorta ve reasürans şirketlerinin Türkiye'deki şubelerini,

ş) Üst düzey yönetim: Kuruluşun icra kurulu başkan ve üyeleri ile genel müdür ve genel müdür yardımcıları, iç sistemler kapsamındaki birimlerin yöneticileri ile başka unvanlarla istihdam edilseler dahi danışmanlık birimleri dışındaki birimlerin yetki ve görevleri itibarıyla genel müdür yardımcısına denk veya daha üst konumlarda görev yapan yöneticileri,

t) Üst yönetim: Kuruluş yönetim kurulu ile üst düzey yönetimi,

ifade eder.

İKİNCİ BÖLÜM
İç Sistemlerin Kurulması ve Üst Yönetimin Sorumlulukları

İç sistemlerin kurulması

MADDE 4 – (1) Kuruluşlar, maruz kaldıkları risklerin izlenmesi ve kontrolünün sağlanması amacıyla, faaliyetlerinin kapsamı ve yapısıyla uyumlu, değişen koşullara uygun varsa bölge müdürlüklerini, şubelerini, birimlerini, temsilciliklerini ve konsolidasyona tâbi ortaklıklarını kapsayacak şekilde bu Yönetmelikte öngörülen usul ve esaslar çerçevesinde yeterli ve etkin iç sistemler kurmak, işletmek ve geliştirmekle yükümlüdür.

(2) İç sistemlerin kurulmasında ve etkin şekilde işletilmesinde nihai sorumluluk yönetim kurulunda veya her ne ad altında olursa olsun yönetim kurulu görevini sürdüren organdadır. Özellikli kuruluşların mevzuatları gereğince yönetim komitesi, komisyon veya benzeri isimlerle adlandırılmakla birlikte yönetim kurulu görev ve yetkilerini haiz yapılar da bu Yönetmelik kapsamında yönetim kurulu olarak değerlendirilir. Limited şirket şeklinde kurulan ve bu Yönetmelik kapsamındaki brokerler için tanımlanan iç sistemleri kurmak ve işletmekle mükellef olan tüzel kişiliği haiz sigorta ve reasürans brokerlerinde ise nihai sorumluluk genel kurula aittir.

(3) Şirketlerde yönetim kurulu, iç sistemler kapsamındaki görev ve sorumluluklarının sağlıklı bir biçimde yerine getirilmesini teminen iç sistemler sorumluluğu görevini denetim komitesi aracılığıyla ifa eder.

(4) İç sistemler kuruluş organizasyonu içerisinde yapılandırılır. Bu Yönetmelik kapsamındaki özellikli kuruluşlar ile şirketler kendi örgüt yapıları içerisinde ayrı bir iç kontrol birimine, risk yönetim birimine, iç denetim birimine ve bu birimlere ilişkin fonksiyonlara yer verir. Şirketler, Doğal Afet Sigortaları Kurumu, Özel Riskler Yönetim Merkezi ve Türkiye Motorlu Taşıt Bürosu tanımlanan birim ve fonksiyonlara ek olarak aktüerya birimi ve fonksiyonu oluşturmak zorundadır. Ancak, bu Yönetmelik kapsamında aktüerya birimi oluşturma zorunluluğu bulunmayan özellikli kuruluşlar ile tüzel kişiliği haiz sigorta ve reasürans brokerlerinin, aktüerya fonksiyonunu işletmeleri veya aktüerya birimi oluşturmaları halinde bu Yönetmelik hükümlerine uygun olarak bu faaliyetleri yürütmesi gerekmektedir. Kuruluşların faaliyet konuları, faaliyetlerinin karmaşıklığı ve büyüklükleri dikkate alınarak iç denetim birimi hariç diğer birimlerin tamamının veya bazılarının birlikte yapılandırılabilmesine ilişkin usul ve esaslar Kurumca belirlenir.

(5) Mevzuatta belirlenen istisnalar ile iç sistemlerle ilgili faaliyetler hariç olmak üzere, Kuruluş nezdindeki diğer birim yapılanmalarında iç sistem birimlerinin isimleri kullanılamaz; bu isimleri çağrıştıran ifadelere yer verilemez.

Yönetim kurulunun yetki ve sorumlulukları

MADDE 5 – (1) İç sistemlerin oluşturulması, etkin, yeterli ve uygun bir şekilde işletilmesi, geliştirilmesi, muhasebe ve finansal raporlama sisteminden edinilen bilgilerin doğruluğunun sağlanması ve muhafaza edilmesi hususunda gerekli tüm tedbirlerin alınması başta olmak üzere güvence altına alınması, kuruluş içindeki yetki ve sorumlulukların belirlenmesi nihai olarak yönetim kurulunun sorumluluğundadır.

(2) Yönetim kurulu, birinci fıkra çerçevesinde;

a) Kuruluşun organizasyon yapısını ve insan kaynakları politikası başta olmak üzere mevzuatla yönetim kurulunun sorumlu kılındığı politika metinlerini oluşturmak, üst düzey yönetimin atanmasında aranılacak kriterleri belirlemek,

b) İç sistemlere ilişkin strateji ve politikalar ile uygulama usullerini yazılı olarak belirlemek, bunların etkin bir şekilde uygulanmasını, idame ettirilmesini ve birbirleri ile koordinasyonunu sağlamak,

c) İç sistemler kapsamındaki birim yöneticileri ile iç denetim birimi personelinin seçimine ve görevden alınmasına karar vermek, bunların görev, yetki ve sorumluluklarını açık ve görev çatışmaları olmayacak şekilde belirlemek, konu ile ilgili personelin çalışma usul ve esaslarını onaylamak ve gerekli kaynakların tahsisini sağlamak,

ç) Kuruluşun faaliyetlerinden ve varsa konsolidasyona tabi ortaklıklarından kaynaklanan tüm risklerin yönetilmesi için risk yönetim birimi ve ilgili birimler tarafından genel ve her bir risk türü itibarıyla konsolide ve konsolide olmayan bazda hazırlanan risk yönetimine ilişkin politika ve stratejiler ile uygulama usullerini onaylamak, üst düzey yöneticiler itibarıyla azami risk limitleri tahsis etmek,

d) Kuruluşun acenteleri ve temsilcilikleri ile dışarıdan hizmet alımı yoluyla temin edilen hizmetlerin gözetimini uygun bir şekilde sağlamak,

e) İç denetim birimi tarafından hazırlanan ve denetim komitesi tarafından incelenen iç denetim planlarını onaylamak,

f) Hak sahiplerinin şikâyetlerinin ve uyuşmazlıkların incelenerek sonucu hakkında hak sahiplerine ve gerektiği durumlarda Kurum başta olmak üzere ilgililere zamanında ve doğru şekilde cevap verilmesini sağlayacak bir sistemin geliştirilmesini; söz konusu şikâyet ve uyuşmazlıkların belirlenecek içerik ve formatta kendisine düzenli olarak raporlanmasını ve şikâyet edilen hususlara ilişkin gerekli tedbirlerin alınmasını sağlamak,

zorundadır.

(3) Yönetim kurulu, kuruluş iç sistemleri hakkında güvence veren yönetim beyanını denetim dönemi itibarıyla bağımsız denetçiye sunmakla yükümlüdür. Bu Yönetmelik kapsamında sunulacak yönetim beyanına ilişkin usul ve esaslar Kurum tarafından belirlenebilir.

(4) Yönetim kurulu kararlarının etkilenmemesini ve çıkar çatışmasının önlenmesini teminen, kuruluşun genel müdürü hariç olmak üzere yönetim kurulu üyelerinden kendileri, aralarındaki evlilik bağı kalkmış olsa dahi eşleri ya da ikinci dereceye kadar (bu derece dâhil) kan ya da sıhri hısımları, son iki yıl dâhil olmak üzere kuruluşta veya konsolidasyona tabi ortaklıklarda veya kuruluşun hizmet aldığı ya da kuruluşun acentesi olan kurum ve kuruluşlarda görevi bulunanlar; söz konusu hizmetin alındığı veya acentelik ilişkisi bulunan kurum ve kuruluşlar hakkında yahut kendi görevleriyle ilgili iç sistemlere ilişkin birimler tarafından hazırlanan rapor ve değerlendirmelerin görüşüldüğü yönetim kurulu toplantılarına katılamaz. Hizmet alınan veya aracılık hizmeti temin edilen kuruluş aynı zamanda kuruluşun yönetimine etkili ortağı ise söz konusu yasak yalnızca yönetime etkili ortağın kuruluşa sunduğu hizmetten sorumlu olan yöneticileri bakımından uygulanır.

Denetim komitesi üyelerinin nitelikleri

MADDE 6 – (1) Denetim komitesi üyelerinin;

a) Atamanın yapıldığı tarihten önceki son iki yıl dâhil olmak üzere;

1) Kuruluşta icrai görevi bulunan yönetim kurulu üyelerinden olmaması,

2) Kendilerinin veya aralarındaki evlilik bağı kalkmış olsa dahi eşlerinin, ikinci dereceye kadar (bu derece dâhil) kan veya sıhri yakınlarının kuruluşun ve konsolidasyona tabi ortaklıklarının, iç sistemler birimlerinde çalışanlar hariç, personeli olmaması,

3) Kendilerinin, aralarındaki evlilik bağı kalkmış olsa dahi eşlerinin veya ikinci dereceye kadar (bu derece dâhil) kan veya sıhri yakınlarının kuruluşun ve konsolidasyona tabi ortaklıklarının bağımsız denetimini, derecelendirmesini veya değerlemesini yapan işletmelerin veya bu işletmeler ile hukuki bağlantısı bulunan yurt dışındaki işletmelerin ortağı veya bu işletmelerin kuruluşa hizmet sunan birimlerinin personeli olmaması veya bağımsız denetim, derecelendirme ya da değerleme sürecinde yer almaması,

4) Kendilerinin, aralarındaki evlilik bağı kalkmış olsa dahi eşlerinin veya ikinci dereceye kadar (bu derece dâhil) kan veya sıhri yakınlarının kuruluş ve konsolidasyona tabi ortaklıklarına, iç sistemlerle ilgili hususlar haricinde, danışmanlık veya destek hizmeti veren kişilerden olmaması,

b) Kendilerinin, aralarındaki evlilik bağı kalkmış olsa dahi eşlerinin veya ikinci dereceye kadar (bu derece dâhil) kan veya sıhri yakınlarının kuruluşta ve konsolidasyona tabi ortaklıklarda nitelikli pay sahibi olmaması,

c) Kuruluşların acenteliği veya temsilciliği şeklinde ticari bağlantıları bulunan hakim ortağının icrai görevi bulunan yönetim kurulu üyesi veya genel müdürünün aralarındaki evlilik bağı kalkmış olsa dahi eşi veya bunların ikinci dereceye kadar (bu derece dâhil) kan veya sıhri hısmı olmaması,

ç) Bu Yönetmeliğin yürürlük tarihinden itibaren geçerli olmak üzere birbirini izleyen dokuz yıldan fazla süreyle aynı kuruluşun denetim komitesinde görev yapmamış olması veya azami görev süresinin tamamlanması halinde aynı kuruluşun denetim komitesinde tekrar görev yapabilmek için iki yıllık bekleme süresinin tamamlanmış olması,

d) Yönetim kurulu üyelerine yapılan huzur hakkı ödemeleri ile sözleşme ile belirlenen sabit ödemeler ve esas sözleşme hükmüne veya genel kurul kararına dayalı olarak yönetim kurulu üyelerine kârdan yapılan ödemeler hariç olmak üzere, kuruluştan ve konsolidasyona tabi ortaklıklardan, bunların kârlılığına veya performansına dayalı olarak herhangi bir ad altında ücret veya benzeri bir gelir sağlanmaması,

e) En az lisans düzeyinde öğrenim görmüş olması ve sigortacılık, özel emeklilik, finans, iç kontrol, risk yönetimi, aktüerya ve denetim alanlarından birinde yahut bu alanlara ilişkin hukuk işlerinde en az on yıllık deneyime sahip olması,

f) Bu maddedeki diğer hususlar saklı olmak kaydıyla; kuruluşta doğrudan ya da dolaylı pay sahibi olan yurt içinde ya da yurt dışında kurulu tüzel kişiliğe sahip ortaklıklar ve bu ortakların veya kuruluşun gerçek kişi ortaklarının birlikte veya tek başlarına, doğrudan ya da dolaylı olarak kontrol ettikleri ya da sınırsız sorumlulukla katıldıkları yurt içinde ya da yurt dışında kurulu kredi kuruluşları ile finansal kuruluşlar ile sigorta sözleşmesi veya bireysel emeklilik sözleşmesinin düzenlenmesi hariç olmak üzere kuruluş ile çıkar çatışması olmayan ticari kuruluşlar dışında başka bir ticari kuruluşta görev almaması,

g) Kuruluşun faaliyet alanına ve özellikli durumuna göre Kurum tarafından gerekli görülecek diğer nitelikleri taşıması,

şarttır.

(2) Denetim komitesi üyelerinin seçiminde aranan nitelikler üyelerin söz konusu görevleri süresince aranır. Komite üyelerinden en az birinin yurt içinde yerleşik olması zorunludur.

(3) Denetim komitesinde yönetim kurulu üyesi olan üye sayısının herhangi bir nedenle ikinin altına düşmesi halinde, yönetim kurulu en geç bir ay içerisinde bu maddede aranan nitelikleri haiz yeter sayıda üyesini denetim komitesine atamak zorundadır. Yönetim kurulunda bu maddede aranan nitelikleri haiz üye bulunmaması halinde icrai görevi bulunmayan yönetim kurulu üyeleri geçici süreyle denetim komitesine atanabilir. Geçici süreli atamalarda, atama tarihinden itibaren icrai görevi bulunmayan üye niteliğini haiz olması şartı aranır. Yönetim kurulu, geçici görevle atanan denetim komitesi üyesi yerine iki ay içerisinde bu maddede belirtilen nitelikleri haiz birini geçici olarak yönetim kurulu üyeliğine seçip ilk genel kurulun onayına sunar. Ayrıca bu kapsamda ortaya çıkabilecek sorunların çözülebilmesini teminen yönetim kurulu genel kurulun olağanüstü toplantıya çağrılması da dahil olmak üzere her türlü tedbiri almakla yükümlüdür.

(4) Yurt dışında kurulu şirketlerin şubelerinde denetim komitesininin görevleri, icrai faaliyet gösteren birimlerin kendisine tabi olmadığı müdürler kurulu üyelerinden biri tarafından gerçekleştirilir. Bu üyede, birinci fıkranın (a) bendinin (3) ve (4) numaralı alt bentleri ile (ç), (d) ve (e) bentlerinde belirtilen nitelikler aranır. Bu üyenin eş ve çocuklarının; şirkette kendisine bağlı icrai mahiyette faaliyet gösteren bir birim bulunmayan müdürler kurulu üyesi, merkez şubesi müdürü, merkez şubesi müdür yardımcısı ve dengi pozisyonda yönetici olmaması, atamanın yapıldığı tarihten önceki son iki yıl da dâhil olmak üzere, şirketin bağımsız denetimini, derecelendirmesini ya da değerlemesini yapan kuruluşların ortağı veya personeli olmaması veya bağımsız denetim, derecelendirme ya da değerleme sürecinde yer almaması, atamanın yapıldığı tarihten önceki son iki yıl da dâhil olmak üzere danışmanlık veya destek hizmeti veren kuruluşların ortağı veya personeli olmaması veya bu hizmeti veren kişilerden olmaması şarttır.

(5) Organizasyon yapısında genel müdürle hiyerarşik bağı bulunmayan, performans ile mali ve özlük haklarına ilişkin değerlendirmeleri yönetim kurulu ya da denetim komitesi tarafından yapılan ve yetkileri itibarıyla asgari olarak genel müdür yardımcısına denk pozisyonlarda bulunan üst düzey yöneticilerin, icrai görevi bulunmayan asgari iki yönetim kurulu üyesinden oluşan denetim komitesinde yönetim kurulu üyesi harici üye olarak görevlendirilmesi mümkündür. Bu durumda iç kontrol, risk yönetimi veya aktüerya birimlerinin idari ve fonksiyonel açıdan belirtilen üst yöneticilere bağlı olarak çalışması mümkündür. Denetim komitesinde görevlendirilen söz konusu üyeler de yönetim kurulu üyesi olma hariç denetim komitesi üyelerinde aranan nitelikleri taşımalıdır. İç kontrol, risk yönetimi veya aktüerya birimlerinin kendisine bağlı olması halinde yönetim kurulu üyesi olmayan denetim komitesi üyeleri, kendilerine bağlı birimler hakkında iç denetim sisteminin çıktılarına ilişkin kararlara iştirak edemez.

Denetim komitesi üyelerinin genel yetki ve sorumlulukları

MADDE 7 – (1) Denetim komitesi; yönetim kurulunun iç sistem faaliyetlerine ilişkin yükümlülüklerini etkin bir şekilde yerine getirmesinde yönetim kuruluna yardımcı olmak adına kuruluşun iç sistemlerinin etkinliğini ve yeterliliğini, bu sistemler ile muhasebe ve raporlama sistemlerinin Kanun ve ilgili düzenlemeler çerçevesinde işleyişini ve üretilen bilgilerin bütünlüğünü gözetmek, bağımsız denetim kuruluşları ile derecelendirme, değerleme ve yönetim kurulu tarafından belirlenecek önemlilik kriterleri göz önünde bulundurularak kuruluşun iç sistemler kapsamında yürütülen faaliyetleri için hizmet alacağı kişi ve kuruluşların belirlenmesinde gerekli ön değerlendirmeleri yapmak, sözleşme imzalanması halinde bu kişi ve kuruluşların faaliyetlerini düzenli olarak izlemek, Kanuna istinaden yürürlüğe giren düzenlemeler uyarınca konsolidasyona tâbi ortaklıkların iç sistemlerine ilişkin faaliyetlerinin konsolide olarak sürdürülmesini ve eşgüdümünü sağlamakla görevli ve sorumludur.

(2) Denetim komitesi, birinci fıkra kapsamında belirtilen görevlerin yerine getirilmesini teminen kuruluş iç sistemlerinin geneline ilişkin olarak aşağıdaki hususlarda görevli ve yetkilidir:

a) İç sistemlere ilişkin konularda üst düzey yönetimin görüş ve önerilerini almak ve bunları değerlendirmek.

b) Görev ve sorumlulukları kapsamındaki işlerin gereğince yerine getirilmesi, etkinliğinin sağlanması ve geliştirilmesi için ihtiyaç duyulan uygulamalar konusunda ilgili üst düzey yönetim, iç kontrol, risk yönetimi, aktüerya ve iç denetimde çalışan personel ile bağımsız denetim kuruluşunun görüş ve değerlendirmeleri hakkında yönetim kurulunu bilgilendirmek.

c) Altı aylık dönemi aşmamak kaydıyla, dönem içerisinde icra edilen faaliyetlere ve bu faaliyetlerin sonuçlarına, kuruluşta alınması gereken önlemlere, yapılmasına ihtiyaç duyulan uygulamalara ve kuruluş faaliyetlerinin güven içinde sürdürülmesi bakımından önemli görülen diğer hususlara ilişkin yönetim kuruluna bilgi vermek.

ç) İç sistemler kapsamındaki fonksiyonların icrasında görevli kişilerin görevlerini bağımsız ve tarafsız bir şekilde yerine getirip getirmediklerini izlemek.

d) İç sistemler kapsamındaki birimler tarafından hazırlanan raporlarda tespit edilen hususlarda üst düzey yönetimin ve bunlara bağlı birimlerin aldığı önlemleri izlemek.

e) Kuruluşun tüm iş süreçleri ve uygulamalarının Kanuna ve ilgili diğer mevzuata uygunluğu kapsamında bağımsız denetim kuruluşunun değerlendirmelerini gözden geçirmek, ilgili üst düzey yönetimin tespit edilen tutarsızlıklar konusundaki açıklamasını almak.

f) İç sistemler kapsamındaki birimlerin yöneticileri ve personeline ilişkin insan kaynakları prosedürlerini hazırlamak; yönetim kuruluna iç sistemler kapsamındaki birim yöneticilerinde aranması gereken nitelikler ile ilgili önerilerde bulunmak, bu birimlerin yöneticilerinin seçimi ve görevden alınması esnasında yönetim kuruluna görüş vermek, iç denetim hariç iç sistem birimleri yöneticilerinin önerileri çerçevesinde bu birimlerin personelini atamak ve görevden almak.

g) İç sistemler kapsamındaki birimlerde görevli yönetici ve personelin mesleki eğitim düzeylerini ve yeterliliğini değerlendirmek.

ğ) Kuruluş personelinin karşılaştığı problemlerin, şüpheli gördükleri hususların veya kuruluş içindeki usulsüzlüklerin doğrudan kendisine, ilgili yönetim kademelerine, iç kontrol birimine, iç denetim birimine veya ilgili diğer birimlere ulaşabilmesini sağlayacak iletişim kanallarının tesis edilmesini sağlamak.

h) Kuruluşların finansal raporlarının gerçek ve yansıtılması gereken tüm bilgileri kapsayıp kapsamadığını, Kanuna ve ilgili diğer mevzuata uygun olarak hazırlanıp hazırlanmadığını gözetmek, tespit edilen hata ve usulsüzlükleri düzelttirmek.

(3) Denetim komitesinin iki üyeden oluşması halinde kararlar oy birliğiyle, üye sayısının ikiden fazla olması halinde ise kararlar oy çokluğuyla alınır.

(4) Denetim komitesi, iç sistem birimlerinden kendisine intikal ettirilen raporlardaki tespitlerin önemine ve aciliyetine binaen yönetim kurulunun acil gündemle toplanmasını talep edebilir.

Denetim komitesi üyelerinin iç kontrol fonksiyonuna ilişkin görevleri

MADDE 8 – (1) Denetim komitesi, iç kontrol fonksiyonuna ilişkin olarak aşağıdaki hususlarda görevli ve yetkilidir:

a) Bu Yönetmelikte yer alan iç kontrole ilişkin düzenlemelere ve yönetim kurulunca onaylanan şirket içi politika ve uygulama usullerine uyulup uyulmadığını gözetmek ve gerekli görülen önlemler konusunda yönetim kuruluna önerilerde bulunmak.

b) İç kontrol birimi tarafından hazırlanan iç kontrol birimi yönetmeliğine ilişkin değerlendirmelerde bulunmak.

c) İç kontrol birimi tarafından yıllık olarak hazırlanan iç kontrol planlarını onaylamak.

ç) İç kontrol fonksiyonuna ilişkin dışarıdan hizmet alınması halinde hizmet alınacak kuruluşlarla çalışma kapsamı ve süresini belirlemek.

Denetim komitesi üyelerinin risk yönetim fonksiyonuna ilişkin görevleri

MADDE 9 – (1) Denetim komitesi, risk yönetim fonksiyonuna ilişkin olarak aşağıdaki hususlarda görevli ve yetkilidir:

a) Risk yönetim birimi tarafından hazırlanan risk yönetim birimi yönetmeliğine ilişkin değerlendirmelerde bulunmak.

b) Risk yönetim fonksiyonuna ilişkin dışarıdan hizmet alınması halinde hizmet alınacak kuruluşlarla çalışma kapsamı ve süresini belirlemek.

c) Kuruluşun taşıdığı risklerin tespit edilmesi, ölçülmesi, izlenmesi ve kontrol edilmesi için gerekli yöntem, araç ve uygulama usullerinin mevcut olup olmadığını değerlendirmek.

Denetim komitesi üyelerinin aktüerya fonksiyonuna ilişkin görevleri

MADDE 10 – (1) Denetim komitesi, aktüerya fonksiyonuna ilişkin olarak; genel fiyatlama politikasına uyum sağlamak, reasürans anlaşmalarının yeterliliğini ve teknik karşılıkların güvenilirliğini gözetmek, gerekli görülen önlemler ve şirket mali durumu hakkında yönetim kuruluna tavsiyede bulunmakla görevli ve sorumludur.

(2) Denetim komitesi, birinci fıkra kapsamında aşağıdaki hususlarda görevli ve yetkilidir:

a) Aktüerya fonksiyonunun yerine getirilmesini teminen kendisine bağlı aktüerya birimi faaliyetlerinin etkin bir şekilde sürdürülebilmesi için yönetim kuruluna önerilerde bulunmak.

b) Bu Yönetmelik kapsamında tanımlanan sorumlu aktüeri belirlemek.

c) Şirket istatistiklerinin oluşturulması, ilgili personelin erişiminin sağlanması ve uygun hesaplamalar yapılabilmesi için gerekli bilgi sistemleri alt yapısının kurulması ile bilgi işlem desteğinin sağlanmasını temin etmek.

ç) Faaliyetlerin etkin bir şekilde icra edilmesi için gerekli nitelikleri haiz yeterli sayıda personel istihdam edilmesini sağlamak.

d) Aktüerya fonksiyonuna ilişkin dışarıdan hizmet alınması halinde hizmet alınacak aktüer veya kuruluşla çalışma kapsamını ve süresini belirlemek.

Denetim komitesi üyelerinin iç denetim fonksiyonuna ilişkin görevleri

MADDE 11 – (1) Denetim komitesi, iç denetim fonksiyonuna ilişkin olarak aşağıdaki hususlarda görevli ve yetkilidir:

a) İç denetim biriminin bu Yönetmelik ve iç politikalarla belirlenen yükümlülüklerini yerine getirip getirmediğini gözetmek.

b) İç denetim fonksiyonunun kuruluşun mevcut ve planlanan faaliyetlerini ve bu faaliyetlerden kaynaklanan risklerini kapsayıp kapsamadığını gözetmek, yönetim kurulunun onayıyla yürürlüğe girecek iç denetime ilişkin şirket içi düzenlemeleri incelemek.

c) İç denetim birimi tarafından hazırlanan iç denetim planlarını inceleyerek yönetim kuruluna sunmak.

ç) Yılda en az iki kez olmak üzere iç denetçiler ile düzenli aralıklarla belirlenecek program ve gündemler dâhilinde görüşmelerde bulunmak.

Denetim komitesi üyelerinin bağımsız dış denetim fonksiyonuna ve diğer hizmetlere ilişkin görevleri

MADDE 12 – (1) Denetim komitesi, bağımsız dış denetim fonksiyonu ve diğer hizmetlere ilişkin olarak aşağıdaki hususlarda görevli ve yetkilidir:

a) Kuruluşun sözleşme imzalayacağı derecelendirme kuruluşları, bağımsız denetim kuruluşları ve değerleme kuruluşları ile bunların yönetim kurulu başkan ve üyeleri, denetçileri, yöneticileri ve çalışanlarının kuruluş ile ilişkili faaliyetlerinde bağımsızlığını ve tahsis edilen kaynakların yeterliliğini değerlendirmek, değerlendirmelerini bir rapor ile yönetim kuruluna sunmak, dışarıdan hizmet alınması halinde de sözleşme süresince denetim dönemleri ile uyumlu olarak düzenli bir şekilde bu işlemleri tekrarlamak.

b) Finansal raporların mali durumu, yapılan işlerin sonuçlarını ve kuruluşun nakit akımlarını doğru olarak yansıtıp yansıtmadığı ve Kanunda ve ilgili diğer mevzuatta belirlenen usul ve esaslara uygun olarak hazırlanıp hazırlanmadığı konusunda üst düzey yönetim ve bağımsız denetçilerle görüşmek, bağımsız denetim raporu sonuçları ile altı aylık ve yıllık mali tablolar ve bunlara ilişkin dokümanları değerlendirmek ve bağımsız denetçinin tereddüt ettiği diğer konuları çözüme kavuşturmak.

c) Yönetim kurulu tarafından belirlenecek önemlilik derecesi göz önünde bulundurularak iç sistem fonksiyonlarının yürütülmesine ilişkin olarak kuruluşun alacağı önemli destek hizmetlerine ilişkin risk değerlendirmesi yapmak, değerlendirmelerini bir rapor halinde yönetim kuruluna sunmak,

hizmet alınması halinde de sözleşme süresince destek hizmeti kuruluşunun sağladığı hizmetlerin yeterliliğini düzenli olarak izlemek.

Denetim komitesine ilişkin istisnalar

MADDE 13 – (1) Özellikli kuruluşların ve tüzel kişiliği haiz sigorta ve reasürans brokerlerinin denetim komitesi oluşturma zorunlulukları bulunmamaktadır. Ancak bu durumda, özellikli kuruluşlar ile brokerlerde bu Yönetmelik ile denetim komitesinin görev ve sorumlulukları arasında sayılan işlemlerin yönetim kurulu tarafından yerine getirilmesi gerekir. Ayrıca yönetim kurulu üyelerinden birinin belirtilen görevlerin icrası için görevlendirilmesi mümkün olup bu durumda belirlenen üyenin denetim komitesi üyelerinde aranan şartları taşıması gerekir.

(2) Tabi olduğu mevzuat çerçevesinde yönetim kurulundan bağımsız olarak konumlandırılmış denetim kuruluna sahip özellikli kuruluşlar ve brokerler açısından, söz konusu denetim kurulu bu Yönetmelikte belirtilen denetim komitesi olarak kabul edilir. İlgili mevzuatın gerektirdiği hususlar saklı olmak üzere, bu Yönetmelikte denetim komitesi üyelerinin taşıması gereken şartlar mevcut denetim kurulu üyelerinde de aranır.

(3) Tabi olduğu mevzuat çerçevesinde, bu Yönetmelikte denetim komitesinin görevleri arasında sayılan görevlerin tamamını veya bir kısmını yerine getiren icradan bağımsız olarak konumlandırılmış ve denetim komitesi üyelerinin niteliklerini haiz üyelerden müteşekkil bir veya birden fazla komitenin bulunduğu şirketlerde denetim komitesinin görevleri bu komiteler eliyle yürütülebilir. Bu şekilde birden fazla komite olması halinde, iç denetim sistemi ile diğer iç sistem fonksiyonlarına ilişkin işlevsel görev ayrımı tesis edilerek ilgili komitelerin görevlendirilmesi kaydıyla, denetim komitesinin görevleri bu komiteler tarafından yerine getirilebilir.

ÜÇÜNCÜ BÖLÜM
İç Kontrol Sistemi

İç kontrol sisteminin amacı ve kapsamı

MADDE 14 – (1) İç kontrol sisteminin amacı, kuruluşun varlıklarının korunmasını, kuruluşun kontrol ortamına ilişkin makul düzeyde güvence sağlanmasını, faaliyetlerin etkin ve verimli bir şekilde Kanuna ve ilgili diğer mevzuata, kuruluşun iç politikalarına ve sigortacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve finansal raporlama sistemi ile ana hizmetlerin yürütülmesinde kullanılan tüm sistemlerin güvenilirliğini, bütünlüğünü ve bilgilerin zamanında elde edilebilirliğini sağlamaktır.

(2) İç kontrol sisteminden beklenen amacın sağlanabilmesi için;

a) Kuruluş bünyesinde işlevsel görev ayrımının tesis edilmesi ve sorumlulukların paylaştırılması,

b) Sözleşme yapılması, prim üretimi, hasar ödeme ve şikâyet süreçleri başta olmak üzere tüm hizmetlerin yürütülmesine ilişkin sistemlerin, muhasebe ve finansal raporlama sisteminin, bilgi sisteminin ve kuruluş içindeki iletişim kanallarının etkin çalışacak şekilde tesis edilmesi,

c) Risklerle ilgili limit ve standartların belirlenmesi,

ç) İş sürekliliği planı ve ilgili diğer planların hazırlanması,

d) Kuruluşun iş süreçleri üzerinde kontrollerin ve iş adımlarının gösterildiği iş akış şemalarının oluşturulması,

e) İç kontrol fonksiyonunun tanımlanması ve oluşturulması,

zorunludur.

(3) İç kontrol sistemi kuruluşların genel müdürlük birimlerini, bölge müdürlüklerini, şubelerini, temsilciliklerini, konsolidasyona tabi ortaklıklarını kapsayacak şekilde yapılandırılır. Ayrıca, acentelik ilişkisi çerçevesinde acentelerin ve destek hizmeti alınan firmaların kuruluşa sunduğu hizmetlerin de iç kontrol sistemi kapsamında bulunması gerekir.

İşlevsel görev ayrımı ve sorumlulukların tesisi

MADDE 15 – (1) Kuruluşlar nezdinde, hata ve usulsüzlüğün, menfaat çatışmalarının, bilgi kirliliğinin ve kaynakların kötüye kullanımının önlenmesi amacıyla aynı konudaki faaliyetlere ilişkin görev ayrıştırması yapılarak kuruluş içindeki tüm birimlerin ve personelin yetki ve sorumlulukları açıkça ve yazılı olarak belirlenir.

(2) Bir işlemin yapılmasına karar verilmesi, işlemin kayda alınması ve muhasebeleştirilmesi ile işlemin fiilen gerçekleştirilmesi işlevlerinin farklı personel sorumluluğuna verilmesi sağlanır.

(3) Kuruluş için risk yaratabilecek işlevler tespit edilerek mümkün olduğunca diğer işlevlerden ayrılır ve farklı yetkililerin sorumluluğuna verilir. İcrai yetkileri olan personelin sorumlulukları ve yetkileri dönemsel olarak incelenerek bunların kuruluş için potansiyel risk oluşturmaması hususunda gerekli tedbirler alınır.

Bilgi sistemlerinin ve iş süreçlerinin tesisi

MADDE 16 – (1) Kuruluş tarafından gerçekleştirilen faaliyetlerin veya verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yönetilmesine; mevzuattan kaynaklanan yükümlülüklerin yerine getirilmesine, muhasebe ve finansal raporlama ile ana faaliyetlerin yürütüldüğü sistemlerden sağlanan bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin, zamanında elde edilebilirliğinin ve gereken durumlarda gizliliğinin sağlanmasına elverişli ve aynı zamanda bilgi sistemlerinin kullanılmasından kaynaklı risklerin izlenmesini, kontrolünü ve gerekli önlemlerin alınmasını sağlayan iş süreçlerinin ve bilgi sistemlerinin tesisi zorunludur.

(2) Kuruluş içinde tesis edilecek iş süreçlerinin ve bilgi sistemlerinin yapısının, şirketin ölçeği, faaliyetlerinin ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması gerekir.

(3) Bilgi sistemleri asgari olarak;

a) Şikâyet, tahsilat, hasar ve tazminat yönetim süreci başta olmak üzere, kuruluşun iş süreçlerinin etkin ve verimli çalışmasının sağlanmasına, hak sahiplerinin taleplerinin gecikmeksizin sonuçlandırılmasına, iş sürekliliğinin sağlanmasına,

b) Bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin doğruluğunun, bütünlüğünün ve güvenilirliğinin sağlanmasına,

c) Bilgi sistemleri dâhilinde gerçekleşen işlem ve olaylara ilişkin etkin bir iz kayıt mekanizması oluşturulmasına,

ç) Bilgi sistemleri kullanıcılarının görev ve sorumlulukları gereği veri tabanlarına, uygulamalara ve sistemlere erişimi için uygun bir yetkilendirme ile erişim kontrolünün oluşturulmasına ve erişimin uygun bir kimlik doğrulama mekanizmasıyla sağlanmasına,

d) Kuruluşun faaliyetlerinin yürütülmesinde kullanılan verilerin taşındığı, iletildiği, işlendiği, saklandığı ve yedek olarak tutulduğu ortamlarda ve kendi nam ve hesabına veri işleyen kurum veya kuruluşlarda 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamındaki gerekliliklerin yerine getirilmesini de sağlayacak şekilde veri gizliliğinin sağlanmasına,

e) Veri tabanlarının ve bilgi sistemlerinin; sunulan ürünler, faaliyet türleri, coğrafi, demografik, ekonomik, operasyonel, stratejik veya benzeri risk doğuran süreçler bazında analiz yapılabilecek şekilde kurgulanmasına,

f) Devlete, kamuoyuna, Sigorta Bilgi ve Gözetim Merkezi ile Emeklilik Gözetim Merkezine ve ilgili diğer kişi ve kurumlara yapılacak bildirim ve raporlamaların zamanında, eksiksiz ve hatasız yapılabilmesine,

g) Herhangi bir denetim veya inceleme sırasında, ilgili kişilerin ihtiyaç duyduğu bilgi ve belgelerin uygun biçimde ve kısa süre içerisinde verilebilmesine,

ğ) Kurum tarafından belirlenecek diğer gerekliliklerin sağlanmasına,

imkân verecek bir yapıda tesis edilir.

(4) Kuruluş, bilgi sistemlerinin güvenilirliğini sağlamak, düzenli olarak güncelleyerek gerekli değişiklikleri yapmak ve bilgi sistemlerinin kesintisiz olarak devam ettirilmesi ile ilgili tedbirleri almakla yükümlüdür.

(5) Kuruluşların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur. Ancak, elektronik posta hizmetleri, telekonferans veya video konferans gibi hizmetler birincil ve ikincil sistemlerin yurt içinde bulundurulma zorunluluğundan istisnadır.

(6) Birincil ve ikincil sistemler kapsamında destek hizmeti alınıp alınmadığına bakılmaksızın, bu sistemler için iş sürekliliğini sağlamaya yetecek sayıda ve nitelikte kuruluş bünyesinde personel istihdam edilmesi zorunludur.

(7) Üçüncü fıkranın (a) bendi kapsamında hasar ve tazminat yönetim sistemi başta olmak üzere kuruluşun iş süreçlerinin ve bilgi sistemlerinin asgari unsurları ile kontrolüne ilişkin usul ve esaslar ile birincil ve ikincil sistemlerin yurt içinde bulundurulmasına ilişkin esasları belirlemeye Kurum yetkilidir.

İletişim yapısı ve etkin iletişim kanallarının tesisi

MADDE 17 – (1) Kuruluş, organizasyon yapısı içinde bilginin, bilgi güvenliği dâhilinde ilgili tüm kişilere ulaştırılmasını ve kuruluşun amaçları, stratejileri, politikaları, uygulama usulleri ve beklentileri hakkında ilgili birim yöneticilerinin ve operasyonda görevli personelin tam anlamıyla bilgi sahibi olmasını sağlamakla yükümlüdür. Bu çerçevede, gerek yöneticilerden personele gerekse personelden yöneticiye olacak şekilde kuruluş içinde etkin iletişim akışının hem dikey hem de aynı düzeydeki personel ile birimler arasında sağlanması anlamında yatay olarak tesis edilmesi gerekmektedir.

(2) Kuruluş personelinin karşılaştığı problemleri ve mutat uygulamalara göre şüpheli gördükleri hususları ilgili birimlere, yönetim kademelerine, iç kontrol birimine, iç denetim birimine veya denetim komitesine gizlice raporlayabilmesi için denetim komitesinin gözetiminde üst düzey yönetim tarafından uygun iletişim kanallarının tesisi ve idamesi gereklidir.

İş sürekliliği yönetimi ve planı

MADDE 18 – (1) Kuruluşların, savaş, terör olayları, grev, lokavt, kargaşalık, salgın hastalıklar, yangın ve doğal afetler ve bilişim tabanlı saldırılar ile iş ortaklarındaki iş kesintileri gibi nedenlere bağlı olarak oluşabilecek bir kesinti veya kriz anında faaliyetlerinin sürdürülmesini veya zamanında kurtarılmasını sağlamak üzere operasyonel, finansal, yasal ve itibari olumsuz etkileri en aza indirmeyi amaçlayan yönetim kurulu tarafından onaylanmış bir iş sürekliliği yönetim yapısı oluşturmaları zorunludur.

(2) İş sürekliliği yönetimi kapsamında, iş sürekliliğinin gereklerini yerine getirmek üzere süreçler tesis edilir ve uygun görülen tedbirler alınır.

(3) İş sürekliliği planlamasına yönelik olarak iş etki analizi çalışmaları yapılır ve kurtarma stratejileri belirlenir. Bu çalışmalar ışığında bir iş sürekliliği planı oluşturulur ve bu plan yönetim kurulu tarafından onaylanır.

(4) İş etki analizi kapsamında, ilgili çalışanların katılımıyla, iç ve dış bağımlılıklar belirlenir ve meydana gelebilecek bir kesinti durumunda gereken faaliyet düzeyini ortaya koymak üzere operasyonlar önem düzeyleri açısından sınıflandırılır. Farklı kesinti senaryolarının faaliyetler üzerinde yaratabileceği muhtemel riskler ve bunların potansiyel etkileri değerlendirilir.

(5) İş etki analizini temel alan, kurtarma öncelikleri ve hedeflerini ortaya koyan bir kurtarma stratejisi geliştirilir. Kurtarma stratejisinin uygulanması ile ilgili detaylara iş sürekliliği planında yer verilir.

(6) İş sürekliliği planının kuruluşun hedefleri ve öncelikleriyle uyumlu, güncel ve yeterli olması esastır. Risklerin açık ve net olarak tanımlandığı bu planda, faaliyet kesintilerinin yönetilmesi için görev ve sorumlulukların belirlenmesi, plan dâhilinde önemli göreve sahip personele ulaşılamaması durumunda yetki ve karar verme yapısının sürdürülebilmesi ve planın hangi koşullarda uygulamaya alınacağı hususlarına yer verilir. Plan geliştirilirken, varsa destek hizmeti alınan kuruluşlar da dikkate alınır. Personel, iş sürekliliği planı hakkında ilgileri çerçevesinde bilgilendirilir, görev ve sorumlulukları konusunda eğitilir.

(7) Herhangi bir acil veya beklenmedik durumda öncelikli gerçekleştirilecek eylemleri ve alınacak tedbirleri belirlemek üzere iş sürekliliği planının bir parçası olarak acil ve beklenmedik durum planı oluşturulur. Karşılaşılan durum bu plan kapsamında çözülemediği takdirde iş sürekliliği planının diğer kısımları devreye alınır.

(8) Acil ve beklenmedik durum planı kapsamında, ortaya çıkabilecek sorun ya da kriz ile başa çıkmak amacıyla gerekli önlemler alınır, gerektiğinde kullanılmak üzere ana hizmetlerin verildiği ortam ile aynı risklere maruz olmayan bir yönetim ve çalışma ortamı tesis edilir.

(9) İş sürekliliği planı ve bu plan kapsamındaki diğer planlar, ilgili tüm birimlere görev ve sorumlulukları çerçevesinde belirlenmiş bir içerikle dokümante edilerek iletilir. Personelin plan ve bu plan dâhilinde üstlendiği sorumluluk hakkında alternatif iletişim kanalları üzerinden bilgi sahibi olması sağlanır. Planda belirtilen hususların eşgüdümü için yetkili bir birim belirlenir.

(10) Bilgi sistemlerinin sürekliliği, iş sürekliliği planı kapsamında hazırlanan ve yönetim kurulu tarafından onaylanmış bilgi sistemleri süreklilik planı ve acil ve beklenmedik durum planında ele alınır. İş sürekliliği planı kapsamındaki planlar ayrı ayrı hazırlanabileceği gibi tek bir planın parçası da olabilirler.

(11) İç kontrol birimi tarafından, iş sürekliliği planı kapsamındaki planları gözden geçirecek bir sistem oluşturulması sağlanır. Kuruluşun iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra planlar gözden geçirilerek güncellenir. Bu planlar, otomatik ve manuel işleyen süreçlerde olası kısa veya uzun süreli kesintiler dikkate alınarak genel müdürlük, seçilen bölge müdürlükleri ve örnek aracılar ile diğer ilgili taraflarda yılda en az bir kez test edilir. Testlere varsa kritik iş süreçlerine destek veren bilgi teknolojileri sistemlerinin ayağa kaldırılmasında rol oynayacak destek hizmeti kuruluşları da dâhil edilir. Test sonuçları uygun bir değerlendirmeyi müteakip üst düzey yönetime ve yönetim kuruluna raporlanır, gerekmesi halinde planın güncellenmesinde kullanılır.

İç kontrol fonksiyonu

MADDE 19 – (1) İç kontrol fonksiyonu, kuruluşun tüm faaliyetlerinin bir parçasını oluşturur. İç kontrole ilişkin yazılı politika ve uygulama usullerinin, önce faaliyeti gerçekleştiren personel, sonra iç kontrol faaliyetini yürüten personel tarafından icra edilecek bir yaklaşımla geliştirilmesi sağlanır ve kuruluşun tüm personeli gerçekleştirdikleri faaliyetlere ilişkin geliştirilen iç kontrol faaliyetlerine dair politika ve uygulama usulleri hakkında bilgilendirilir.

(2) İç kontrol fonksiyonu asgari olarak aşağıdaki kontrolleri kapsar:

a) Faaliyetlerin icrasına yönelik işlemlerin kontrolü.

b) İletişim kanalları, ana hizmetlerin sürdürülmesine ilişkin tüm sistemler ile bilgi sistemlerinin ve finansal raporlama sisteminin kontrolü.

c) Uyum kontrolleri.

ç) Ana hizmetlerin uzantısı veya tamamlayıcısı niteliğinde olan hizmet alımlarının kontrolü.

Faaliyetlerin icrasına ilişkin kontroller

MADDE 20 – (1) Faaliyetlerin icrasına yönelik işlemlerin kontrolü kapsamında kuruluş tarafından aşağıdaki uygulamaların yapılması şarttır:

a) Raporlama: Üst yönetime sunulmak ve konusuna göre altı ayı geçmemek üzere raporun sunulacağı birimin belirleyeceği periyotlarda, günlük, haftalık veya aylık bazda olağanüstü durum, şüpheli işlem, aykırılık ve genel performans raporları hazırlanır.

b) Onaylama ve yetkilendirme: Çift taraflı ve çapraz kontrol ve imza usulleri tesis edilir, belirli limitlerin üzerindeki işlemler için onay ya da yetki alınır.

c) Sorgulama ve mutabakat sağlama: İşlemlerin detayları sorgulanır, hesaplar karşılaştırılır, düzenli aralıklarla mutabakatlar gerçekleştirilir.

ç) Fiziki kontrol: Kuruluşa ait veya sigortalılar ile katılımcılar ve diğer taraflar adına saklanan nakit para, finansal varlıklar veya poliçeler de dâhil olmak üzere varlıklara erişilebilmesine, bunların kullanılmasına ve saklanmasına yönelik kurallar ve sınırlar belirlenir, tüm maddi varlıkların düzenli aralıklarla envanteri çıkarılır.

d) Temel performans göstergelerine ilişkin kontroller: Şirketlerde yönetim kurulu, özellikli kuruluşlarda ise Kurum tarafından onaylanan temel performans göstergelerine ulaşma kapsamında yapılan faaliyetlerin kontrolü.

e) Yetki ve risk limitlerine uygunluk incelemeleri ile aşım ve aykırılıkların takibi: Genel ve özel risk limitlerine uyulup uyulmadığının incelenmesi ve limit aşımlarının izlenmesi.

İletişim sistemleri ile bilgi sistemlerine ilişkin kontroller

MADDE 21 – (1) İletişim kanallarının kontrolü kapsamında aşağıdaki uygulamaların yapılması şarttır:

a) Kuruluşta üretilen bilgiye personelin erişim imkânlarının oluşturulup oluşturulmadığının ve üretilen bilgiye erişimde yetkilendirmelerin uygun seviyede yapılıp yapılmadığının kontrolü.

b) Kuruluşun, çalışılan birimin ve personelin faaliyet performansına ilişkin personele düzenli bilgi verilip verilmediği kontrolü.

c) Kanunda ve ilgili diğer mevzuatta yapılan değişiklikler ile yeni ürün veya faaliyetler hakkında personelin bilgilendirilip bilgilendirilmediği kontrolü.

ç) Kuruluş personelinin karşılaştığı problemleri ve mutat uygulamalara göre şüpheli gördükleri hususları ilgili birimlere, yönetim kademelerine, iç kontrol birimine, iç denetim birimine veya denetim

komitesine gizlice raporlamasına imkân tanıyan uygun araçların bulunup bulunmadığının ve ihlaller konusunda raporlama yapılabiliyorsa ne kadar sıklıkla raporlama yapıldığının kontrolü.

d) Kuruluş tarafından sunulan hizmetlerden yararlanan sigortalıların, sigorta ettirenlerin, lehdarların veya diğer hak sahiplerinin hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilip bilgilendirilmediğinin, bu kişilerin şikâyetlerini ulaştırmalarına imkân sağlayacak mekanizmaların kurulup kurulmadığının ve kişilere ilişkin bilgi mahremiyetinin sağlanıp sağlanmadığının kontrolü.

(2) Ana hizmetlerin icrasında kullanılan sistemlerin kontrolü kapsamında aşağıdaki uygulamaların yapılması şarttır:

a) Kullanılan sistemlerin hizmetin içeriği ile uyumluluğuna ve bütünlük oluşturup oluşturmadığına dair kontroller.

b) Kullanılan sistemlerden kaynaklı olarak sigortalıların, sigorta ettirenlerin, lehdarların, diğer hak sahiplerinin ve ilgili tarafların hak ve menfaatlerine zarar gelmediğine ve bu kişilere karşı yükümlülüklerde gecikme yaşanmadığına dair kontroller.

(3) Bilgi sistemlerinden beklenen fonksiyonların doğru bir şekilde yerine getirilmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvence oluşturulmasını sağlamak üzere bilgi sistemlerinin kontrolü kapsamında aşağıdaki uygulamaların yapılması şarttır:

a) Mevzuat, rehber veya COBIT kapsamında bilgi sistemi ve yönetimine ilişkin faaliyetler ile bu faaliyetlerin süreçlerinin kontrolüne ilişkin genel bilgi sistemi kontrolünün yapılması.

b) Veri oluşturma ve yetkilendirme, girdi, veri işleme, çıktı kontrollerinden oluşan uygulama kontrollerinin yapılması.

c) Organizasyon içinde veya dışında üretilen, telefon, sesli posta, kâğıt, faks veya e-posta ile alınmış verinin aslına uygunluğu ve bütünlüğünün, veri üzerinde kritik bir işlem yapılmadan kontrol edilmesi.

ç) Hassas bilginin saklanması, iletimi ve nakli esnasında, yetkisiz erişim, değişiklik ve yanlış yönlendirmeye karşı korunup korunmadığının kontrolü.

d) Bilgi sistemlerinin risk ölçüm yöntem veya modelleri kullanılarak risklerin ölçülebilmesine, önceden belirlenen risk limitlerine yaklaşılması halinde zamanında uyarıcı bilgiler üretilebilmesine ve etkin bir şekilde raporlanabilmesine imkân tanıyıp tanımadığının kontrolü.

(4) Finansal raporlama sisteminin kontrolü kapsamında aşağıdaki uygulamaların yapılması şarttır:

a) Finansal raporların Kanuna ve ilgili mevzuata uygun olarak hazırlanıp hazırlanmadığı ile zamanında ve eksiksiz yayımlandığına ilişkin kontroller.

b) İşlemlerin kayda alınması ile finansal raporlara yansıtılması arasında uygulanan sürecin, oluşabilecek hataların ve eksikliklerin saptanabilmesine yönelik kontroller.

c) Finansal raporlardaki bilgilerin kontrolü ve kontrol edilen bilgilere dayanak olan işlemlerin kontrolü.

Uyum kontrolleri

MADDE 22 – (1) Uyum kontrolleriyle, kuruluşun gerçekleştirdiği ve planladığı tüm faaliyetler ile yeni işlem ve ürünlerin Kanuna ve ilgili diğer mevzuata, kuruluş politikalarına ve sigortacılık teamüllerine uyumun sağlanması amaçlanır.

(2) Uyum kontrolleri kapsamında Kuruluş tarafından aşağıdaki uygulamaların yapılması zorunludur:

a) Kanun ve ilgili diğer mevzuat ile kuruluş içi politika ve kurallardaki değişiklikler hakkında, kuruluş personelinin en kısa sürede bilgilendirilmesinin sağlanıp sağlanmadığı.

b) İç kontrol birimi veya uyum kontrolüyle görevlendirilecek ve kuruluşun diğer faaliyetlerinden bağımsız olarak örgütlendirilecek bir birim tarafından uyumun kesintisiz kontrolünün risk bazlı olarak gerçekleştirilip gerçekleştirilmediği.

c) Bağımsız bir uyum birimi kurulması halinde, iç kontrol biriminin bağımsızlığı için aranan şartların uyum birimi için de bulunup bulunmadığı.

ç) Yeni ürün ve işlemler ile gerçekleştirilmesi planlanan faaliyetlerin Kanuna ve ilgili diğer mevzuata, kuruluş politikalarına ve sigortacılık teamüllerine uygunluğunun, suiistimal, kuruluşun ve çalışanların itibar kaybı gibi risklerin yönetiminin sağlanması için uyumun kesintisiz kontrolü ile görevlendirilen birim ile hukuk biriminden görüş alınıp alınmadığı.

(3) Uyum fonksiyonu kapsamında denetim komitesine yapılan raporlamalarda kuruluşun iş birimlerinin uyum standartlarına göre nasıl performans gösterdiği, uyum ihlallerine ve ilgili kamu otoritesi tarafından verilen para cezaları veya disiplin işlemlerine yer verilir.

(4) Kuruluş yöneticilerinden herhangi birinin uyum konusunda ihlallerde bulunduğunun ve üst düzey yönetim ya da diğer yetkili kişilerce düzeltici herhangi bir önlem alınmadığının tespit edilmesi ve gecikmenin kuruluşu yahut poliçe sahiplerini zarara uğratacak nitelikte olduğunun düşünülmesi halinde, uyum fonksiyonundan sorumlu yönetici denetim komitesine, denetim komitesinin bulunmadığı kuruluşlarda yönetim kurulu başkanına bilgi vermekle yükümlüdür.

(5) Özellikle yüksek sorumluluk pozisyonunda olan veya yüksek riskli faaliyetlerde bulunan çalışanlar için temel yasal ve düzenleyici yükümlülükler hakkında düzenli eğitimler planlanır.

Hizmet alımlarına ilişkin kontroller

MADDE 23 – (1) Ana hizmetlerin uzantısı veya tamamlayıcısı olan hizmet alımlarının kontrolü kapsamında kuruluş tarafından aşağıdaki uygulamaların yapılması şarttır:

a) Hizmet alımlarının mevzuata uygun yapıldığına ve hizmet alınan alanlarla sınırlı olarak hizmet sağlayıcının veya tedarikçinin faaliyetlerinin mevzuata uygun olduğuna dair kontroller.

b) Hizmet alımı yapılan kişi ve kuruluşların, alınan hizmetle sınırlı olarak bilgi sistemleri, iş süreçlerinin tesisi ve iş sürekliliği ile risk yönetimine ilişkin gerekliliklerin sağlanıp sağlanmadığına dair kontroller.

c) Hizmet alımı yapılan kişi ve kuruluşa bağımlılık ile bu ilişkisinin beklenmedik şekilde sona ermesi halinde, kuruluşun bilgi kaybı yaşamaksızın faaliyetlerine devam edebilmesine ilişkin kontroller.

ç) Acentelik ilişkisiyle sınırlı olmak üzere şirketin acenteleri nezdinde bilgi sistemleri, iş süreçlerinin tesisi ve iş sürekliliği ile risk yönetimine ilişkin gerekliliklerin sağlanıp sağlanmadığına ilişkin kontroller.

İç kontrol birimi

MADDE 24 – (1) Faaliyetlerin icrasını gerçekleştiren her bir birim iç kontrol politikaları oluşturmaktan ve bu politikaların uygulanmasından birinci derecede sorumludur. Ancak, diğer birimler tarafından yürütülen süreçlerin veya kullanılan kontrollerin tasarımında bu birimlere destek olmak, söz konusu süreçlerin ve kontrollerin yeterliliğini, etkinliğini ve uygunluğunu bu birimlerle birlikte değerlendirmek, bu Yönetmelikte tanımlanan iç kontrol fonksiyonlarını yerine getirmek veya bu fonksiyonların yerine getirildiğini kontrol etmek üzere, bu Yönetmelik kapsamında iç sistemler kurma ve işletme yükümlüğü bulunan şirketler ve özellikli kuruluşlar tarafından, idari ve fonksiyonel açıdan denetim komitesine bağlı iç kontrol birimi kurulması zorunludur.

(2) İç kontrol birimi şirketlerin genel müdürlüklerinde ve özellikli kuruluşlarda ise merkezlerde yer alır. Türkiye'de şube açarak faaliyet gösteren yurt dışında kurulu şirketlerde iç kontrol birimi, Türkiye'de bulunan merkez şubede tesis edilir. Bölge müdürlüklerinin ve temsilciliklerinin büyüklüğü dikkate alınarak gerekmesi halinde bölge müdürlüklerinde veya temsilciliklerinde de iç kontrol birim personeli görevlendirilir.

(3) İç kontrol biriminde bir yönetici ile kuruluşun ölçeği, faaliyetlerinin niteliği ve karmaşıklığına uygun yeterli sayıda ve mesleki uzmanlığa sahip iç kontrol personeli görev yapar. Kuruluşun faaliyetinin büyüklüğü ve karmaşıklığı dikkate alınmak suretiyle bu Yönetmelikte iç kontrol biriminin görevleri arasında tanımlanan tüm faaliyetlerin bir personel ile sürdürülmesinin mümkün olduğu kuruluşlarda, yönetim kurulunun uygun görmesi ve Kuruma bildirim yapılması kaydıyla bu görevlerin iç kontrol birimi yöneticisi tarafından yerine getirilmesi mümkündür. Bu durumda yalnızca iç kontrol birimi yöneticisinin istihdamıyla iç kontrol birimi kurulmuş kabul edilir.

(4) İç kontrol faaliyetini yürüten personele, izledikleri, inceledikleri ve kontrol ettikleri hususlara ilişkin olarak kuruluş personelinden ilave açıklama isteme ve bunların fikirlerine başvurma yetkileri verilir.

(5) İç kontrol sistemi ile iç kontrol faaliyetleri ve bunların nasıl icra edileceği, kuruluşun gerçekleştirdiği tüm faaliyetlerin nitelikleri dikkate alınarak iç kontrol birimi, ilgili birimlerin üst düzey yöneticileri ve personeli ile birlikte tasarlanır.

(6) İç kontrol faaliyetlerinin, kuruluşun operasyonel faaliyetlerini gerçekleştiren personel ile iç kontrol personeli arasında dağılımına ilişkin usul ve esaslar ile hangi kontrol mekanizma ve yöntemlerinin kullanılacağı, üst düzey yöneticilerin ve ilgili personelin görüşleri alınmak suretiyle iç kontrol birimi yöneticisinin önerisiyle denetim komitesi tarafından belirlenir.

(7) İç kontrol birimi tarafından hazırlanan, denetim komitesinin görüşü alınmak suretiyle yönetim kurulu tarafından onaylanarak kabul edilen iç kontrol birimi yönetmeliğinde, iç kontrol biriminin çalışma usul ve esasları ile bu faaliyetleri yürütecek personelde aranan öğrenim durumu, deneyim, bilgi ve beceri seviyeleri ile diğer niteliklere yer verilir.

(8) Birimde çalışan personel kuruluşun tüm faaliyetlerinin güvenli bir biçimde icra edilmesini izlemek, incelemek ve kontrol etmek amacıyla ilgili birimlerden raporlamaya dayalı bilgi talebinde bulunur; çeşitli kontrol dokümanları ve araçları üzerinden genel veya özel gözlemlere ve izlemeye dayalı kontrol ya da inceleme yapar; tespitlerini raporlara bağlar veya uyarı mesajları hazırlayarak ilgili birimlere tebliğ eder.

(9) Kuruluş bünyesinde gerçekleştirilen iç kontrol faaliyetlerinin sonuçları iç kontrol birimine raporlanır. İç kontrol birimine raporlanan kontrol sonuçları bu birim bünyesinde muhafaza edilir. Raporlamalar, operasyonel faaliyetleri yürüten kuruluş personeli ve iç kontrol personeli tarafından yapılanlar olarak ayrıştırılır ve bunlar da niteliklerine göre sınıflandırılır.

(10) İç kontrol faaliyetlerinin yerine getirilip getirilmediği, kurallara ve sınırlamalara uyulup uyulmadığı, hedeflere ulaşılıp ulaşılamadığı hususları, iç kontrol birimi yönetmeliğinde belirlenen yönetim kademelerinde ve ilgili kontrol basamak ve noktalarında kontrol edilerek tespitlerin niteliği de dikkate alınmak suretiyle normal veya acil bir şekilde iç kontrol personelince denetim komitesine bildirilir.

(11) İç kontrol birimi tarafından risk değerlendirmelerine dayalı ve yıllık olarak iç kontrol planı hazırlanır. Plan hakkında üst düzey yönetimin de görüşü alınır ve planlar en geç ilgili yılın aralık ayı sonuna kadar denetim komitesinin onayıyla yürürlüğe konulur. Gerekli hallerde, aynı prosedür takip edilerek iç kontrol planları yıl içinde güncellenebilir.

(12) İç kontrol fonksiyonu kapsamında gerçekleştirilen faaliyet ve bulgulara ilişkin olarak iç kontrol birimi tarafından üçer aylık dönemler itibarıyla genel müdüre ve denetim komitesine raporlama yapılır.

(13) İç kontrol fonksiyonu kapsamında yapılan raporlamada iş birimlerinin iç kontrol standartlarına uyum konusunda gösterdikleri performans değerlendirmelerine, tespit edilen eksiklik ve hatalar ile bunlara ilişkin verilen yanıtlara yer verilir.

(14) İç kontrol fonksiyonunu ve iç kontrol biriminin görevlerini yerine getirmeleri kaydıyla, iç kontrol birimi, uyum birimi ve benzeri isimlerle de kurulabilir. Ayrıca, iç kontrol fonksiyonlarını yerine getirmek için iç kontrol birimi altında, uyum kontrolleri birimi, raporlama kontrolleri birimi gibi alt birimler kurulabilir. 16/9/2008 tarihli ve 26999 sayılı Resmî Gazete'de yayımlanan Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine İlişkin Yükümlülüklere Uyum Programı Hakkında Yönetmelik kapsamında kurulan uyum biriminin iç kontrol birimi altında yapılandırılmasında veya iç kontrol biriminin ilgili yönetmelik kapsamında belirtilen uyum görevlerini yerine getirmesinde sorumlu olunan mevzuattan kaynaklanan gerekliliklerin yerine getirilmesi kaydıyla herhangi bir sakınca bulunmamaktadır.

İç kontrol birimi yöneticisi ve personelinin nitelikleri

MADDE 25 – (1) İç kontrol birimi yöneticisinin atanması ve görevden alınması denetim komitesinin görüşü ile yönetim kurulu tarafından; birim personelinin atanması ve görevden alınması iç kontrol birimi yöneticisinin görüşü ile denetim komitesi tarafından gerçekleştirilir.

(2) İç kontrol birimi yöneticisinin en az dört yıllık üniversite mezunu olması ve sigortacılık, özel emeklilik, finans, iç kontrol, risk yönetimi veya denetim alanlarında en az beş yıllık deneyime sahip olması zorunludur. İç kontrol birim yöneticisinin sigortacılık mevzuatına, ticaret hukukuna ve kuruluşun faaliyet alanı ile ilgili diğer mevzuata hakim olması beklenir. İç kontrol birimi yöneticisi, iç

kontrol personelinin görev, yetki ve sorumluluklarının gerektirdiği nitelikleri haiz olup olmadıklarını değerlendirir, mesleki bilgi, beceri ve yeteneklerinin geliştirilmesine yönelik eğitim programları hazırlar ve bunların görevlerini icrai birimlerin etkisinde kalmaksızın tarafsız olarak icra edip etmediklerini izler.

(3) İç kontrol biriminde görevlendirilecek personelin deneyim hariç birim yöneticisinin niteliklerini haiz olması gerekir.

(4) İç kontrol biriminde görevli personel ve birim yöneticisi, görevlerine ilişkin konularda kuruluşun diğer birimlerine sağlayacakları teknik destek ve danışmanlık hizmeti haricinde kuruluş bünyesinde icrai başka görevler ifa edemez. 4 üncü maddenin dördüncü fıkrası çerçevesinde bazı birimlerin birlikte kurulması halinde, bu madde birlikte faaliyet gösteren birimlerin tamamını kapsayacak şekilde uygulanır.

DÖRDÜNCÜ BÖLÜM
Risk Yönetim Sistemi

Risk yönetim sisteminin amacı ve kapsamı

MADDE 26 – (1) Risk yönetimi sisteminin amacı, faaliyetlerin sürekliliği ile kuruluşun gelecekteki nakit akımlarının ihtiva ettiği risk ve getiri yapısını, buna bağlı olarak faaliyetlerin niteliğini ve düzeyini izlemeye, kontrol altında tutmaya ve gerektiğinde değiştirmeye yönelik olarak belirlenen politikalar, uygulama usulleri ve limitler vasıtasıyla, maruz kalınan risklerin tanımlanmasını, ölçülmesini, izlenmesini ve kontrol edilmesini sağlamaktır.

(2) Kuruluş içinde acentelerin ve destek hizmeti alınan firmaların kuruluşa sunduğu hizmetleri de kapsayacak şekilde uygun ve yeterli bir risk yönetim sisteminin tesis edilmesi için;

a) Faaliyetlerden kaynaklanan risklerin farklı boyutlarını yönetmeye imkân verecek yeterli politikalar, uygulama usulleri ve limitler,

b) Risk yönetimi faaliyetleri,

bu Yönetmelikte belirtilen usul ve esaslara uygun olarak açıkça tanımlanır.

Risk yönetimi politikaları

MADDE 27 – (1) Kuruluş faaliyetlerinden ve varsa konsolidasyona tabi iştirakler, bağlı ortaklıklar, hizmet alınan kuruluşlar ve acentelerden kaynaklanan tüm risklerin her birinin yönetilmesi için ilgili birimler ile risk yönetim birimi tarafından konsolide ve konsolide olmayan bazda hazırlanan ve yönetim kurulu tarafından onaylanan risk yönetim politika ve uygulama usullerinin belirlenmesinde asgari olarak aşağıdaki hususlar dikkate alınır:

a) Kuruluşun faaliyetlerine ilişkin stratejiler, politikalar ve uygulama usulleri.

b) Kuruluşun faaliyetlerinin hacmine, niteliğine ve karmaşıklığına uygunluk.

c) Kuruluşun alabileceği risk düzeyi.

ç) Kuruluşun risk izleme ve yönetme kapasitesi ile risk yönetim araçlarının risklerin niteliğiyle uyumlu şekilde kullanımı.

d) Kuruluşun geçmiş deneyimi ve performansı.

e) Faaliyetleri yürüten birimlerin yöneticilerinin alanları ile ilgili konulardaki uzmanlık düzeyleri.

f) Kanunda ve ilgili diğer mevzuatta öngörülen yükümlülükler.

(2) Risk yönetimi politika ve uygulama usullerinin değişen koşullara uyum sağlaması gerekir. Bu kapsamda risk yönetim birimi iç kontrol sistemi ile iç denetim sistemi çıktılarından da yararlanarak ilgili politikaların yeterliliğini düzenli olarak değerlendirir ve gerekli değişiklikleri yaparak yönetim kurulunun onayına sunar.

Risk limitleri

MADDE 28 – (1) Risk yönetim birimi ve ilgili birimler tarafından hazırlanan ve yönetim kurulu tarafından onaylanan risk yönetim politika ve strateji belgelerinde, genel ve her bir risk türü itibarıyla üstlenilecek risk seviyesi ile yöneticiler ve diğer personel için tahsis edilecek azami risk limitleri ve bunların uygulama usulleri yazılı olarak belirlenir.

(2) Birinci fıkra kapsamında belirlenecek risk limitleri; kuruluşun alabileceği risk düzeyine, faaliyetlerine, ürünlerinin ve hizmetlerinin büyüklüğü ve karmaşıklığına uygun olarak asgari olarak birim ve kuruluş geneli bazında belirlenir.

(3) Risk limitleri risk yönetimi politikalarına uygun olarak gerekli sürelerde ve her hâlükârda azami iki yılda bir gözden geçirilir ve piyasa koşulları ile kuruluş stratejisindeki değişmelere göre uyarlanır.

(4) Risk limitlerinin ilgili birimlere iletilmesi ve ilgili personelin bunları anlaması sağlanır.

(5) Mevcut risk düzeyini artırabilecek veya yeni bir risk türü yaratabilecek yeni faaliyetler ve ürünler, üst düzey yönetim veya yönetim kurulu tarafından onaylanır.

Risk yönetim fonksiyonu

MADDE 29 – (1) Risk yönetim fonksiyonu kuruluşun faaliyet dallarına göre asgari olarak aşağıda belirtilen risk türlerini kapsar:

a) Yazım riski.

b) Sigortacılık faaliyetleri dışındaki varlık ve yükümlülük yönetimi.

c) Sigorta poliçelerine bağlı olarak yapılan yatırımlar hariç olmak üzere yatırım riski.

ç) Likidite riski.

d) Yoğunlaşma riski.

e) Operasyonel ve idari riskler.

f) Yazılım ve bilgi güvenliği riski.

g) Karşı taraf ve üçüncü taraf riski.

ğ) Reasürans ve diğer risk azaltma teknikleri.

h) Uyum riski.

(2) Risk yönetim fonksiyonu asgari olarak şu faaliyetleri kapsar:

a) Risk ölçümü, risklerin izlenmesi, risklerin kontrolü ve raporlanması faaliyetlerinden oluşan risk yönetim sistemini tasarlamak ve uygulamak.

b) Risk yönetim stratejileri esas alınarak risk yönetim politikaları ve uygulama usullerini belirlemek.

c) Risk yönetimi politika ve uygulama usullerinin uygulanmasını ve bunlara uyulmasını sağlamak.

ç) Yeni ürün ve işlemler ile gerçekleştirilmesi planlanan faaliyetlerin, Kanuna ve ilgili diğer mevzuat ile kuruluş politikalarına ve sigortacılık teamüllerine uyumu, suiistimal, kuruluşun ve çalışanların itibar kaybı dahil tüm risklerin anlaşılmasını ve yeterli seviyede değerlendirmenin yapılmasını sağlamak.

d) Risk ölçüm modellerinin tasarımı, seçilmesi, uygulamaya konulması ve ön onay verilmesi sürecine katılmak, modelleri düzenli olarak gözden geçirmek ve gerekli değişiklikleri yapmak.

e) Kuruluşun kullandığı risk ölçüm modellerinden periyodik raporlar üretmek ve raporları analiz etmek.

f) Sayısallaştırılabilen risklerin belirlenen limitler dâhilinde kalmasını sağlamak ve bu limitlerin kullanımını izlemek.

g) Kuruluşa özgü durumlardan kaynaklanabilecek veya finansal piyasalarda ortaya çıkabilecek potansiyel riskler ile kırılganlıkların ölçülmesi ve risk profilinin ileriye dönük bir değerlendirmesini yapmak üzere stres testi programı kurmak, işletmek ve senaryo analizleri yapmak.

ğ) Stres testi ve senaryo analiz sonuçları göz önünde bulundurularak acil durum planları hazırlamak veya acil durum planları hazırlanması için analiz sonuçlarını ilgili birimlere iletmek.

h) Riskin izlenmesi ve zamanında önlem alınmasını sağlayan erken uyarı sistemleri kurmak ve işletmek.

ı) Her bir risk için birim bazında belirlenen limitleri toplulaştırarak kuruluşun tümü bazında belirlenen limitlere uyumunu izlemek.

i) Teşvik edici yapılar ile ödül düzenlemelerinden kaynaklı riskleri takip etmek.

Risk yönetim birimi

MADDE 30 – (1) Faaliyetlerin icrasını gerçekleştiren her bir birim risk yönetim politikaları oluşturmaktan ve bu politikaların uygulanmasından birinci derecede sorumludur. Potansiyel risklerin zamanında tanımlanmasının, değerlendirilmesinin ve yönetilmesinin sağlanması ile bu Yönetmelik kapsamında tanımlanan risk yönetim fonksiyonlarının yerine getirilmesinde ilgili birimlere destek olmak ve bu birimlerle koordineli çalışarak risk yönetim fonksiyonunun yeterliliğini ve etkinliğini

sağlamak üzere şirketler ve özellikli kuruluşlar tarafından idari ve fonksiyonel açıdan denetim komitesine bağlı risk yönetim birimi kurulması zorunludur.

(2) Risk yönetim birimi şirketlerin genel müdürlüklerinde, özellikli kuruluşlarda ise merkezlerde yer alır. Türkiye'de şube açarak faaliyet gösteren yurt dışında kurulu şirketlerde risk yönetim birimi, Türkiye'de bulunan merkez şubede tesis edilir.

(3) Risk yönetim biriminde bir yönetici ile kuruluşun ölçeği, faaliyetlerinin niteliği ve karmaşıklığına uygun yeterli sayıda ve mesleki uzmanlığa sahip risk yönetim birimi personeli görev yapar. Kuruluşun faaliyetinin büyüklüğü ve karmaşıklığı dikkate alınmak suretiyle bu Yönetmelikte risk yönetim biriminin görevleri arasında tanımlanan tüm faaliyetlerin bir personel ile sürdürülmesinin mümkün olduğu kuruluşlarda, yönetim kurulunun uygun görmesi ve Kuruma bildirim yapılması kaydıyla bu görevlerin risk yönetim birimi yöneticisi tarafından yerine getirilmesi mümkündür. Bu durumda yalnızca risk yönetim birimi yöneticisinin istihdamıyla risk yönetim birimi kurulmuş kabul edilir.

(4) Denetim komitesinin uygun görüşü ve yönetim kurulunun onayıyla kabul edilen, birimin çalışma usul ve esasları ile bu faaliyetleri yürütecek personelde aranan öğrenim durumu, deneyim, bilgi ve beceri seviyeleri ile diğer niteliklere yer verilen risk yönetimi birimi yönetmeliği, birim tarafından hazırlanır.

(5) Risk yönetimi birimi yöneticisi tarafından birim personelinin görevlerini icrai birimlerin etkisinde kalmaksızın tarafsız olarak icra edip etmediklerinin takibi yapılır.

(6) Risk değerlendirmesinde kapsanan risklerin ayrıntılı açıklamaları, temel varsayımlar ve kullanılan yaklaşımları da içeren risk ölçümü ve değerlendirme sonuçları risk yönetim birimi tarafından genel müdüre ve denetim komitesine üçer aylık dönemler itibarıyla düzenli olarak raporlanır.

(7) Risk yönetim sistemindeki önemli değişiklikler risk yönetim birimi tarafından yönetim kurulunun onayına sunulur. Değişikliklerin gerekçelerinin de yer aldığı belgeler iç denetim birimi, bağımsız dış denetim ve Kurum denetçilerinin risk yönetimine ilişkin değerlendirme yapabilmelerini sağlamak üzere denetimlerde hazır bulundurulur.

Risk yönetim birimi yöneticisi ve personelinin nitelikleri

MADDE 31 – (1) Risk yönetim birimi yöneticisinin atanması ve görevden alınması denetim komitesinin görüşü ile yönetim kurulu tarafından; birim personelinin atanması ve görevden alınması risk yönetim birimi yöneticisinin görüşü ile denetim komitesi tarafından gerçekleştirilir.

(2) Risk yönetim birimi yöneticisinin en az dört yıllık üniversite mezunu olması ve sigortacılık, özel emeklilik, finans, iç kontrol, risk yönetimi, aktüerya veya denetim alanlarında en az beş yıllık deneyime sahip olması zorunludur. Risk yönetimi birimi yöneticisi, birim personelinin görev, yetki ve sorumluluklarının gerektirdiği nitelikleri haiz olup olmadıklarını değerlendirir, bu kişilerin risk yönetimi faaliyetleri alanındaki mesleki bilgi, beceri ve yeteneklerinin geliştirilmesine yönelik eğitim programları hazırlar.

(3) Risk yönetim biriminde görevlendirilecek personelin deneyim hariç birim yöneticisinin niteliklerini haiz olması gerekir.

(4) Risk yönetim biriminde görevli personel ve birim yöneticisi, aktüerya fonksiyonunun risk yönetimine dair faaliyetleri ile görevlerine ilişkin konularda kuruluşun diğer birimlerine sağlayacakları teknik destek ve danışmanlık hizmeti haricinde kuruluş bünyesinde icrai başka görevler ifa edemez. 4 üncü maddenin dördüncü fıkrası çerçevesinde bazı birimlerin birlikte kurulması halinde, bu madde birlikte faaliyet gösteren birimlerin tamamını kapsayacak şekilde uygulanır.

BEŞİNCİ BÖLÜM
Aktüerya Fonksiyonu ve Aktüerya Birimi

Aktüerya fonksiyonunun amacı ve kapsamı

MADDE 32 – (1) Aktüerya fonksiyonunun amacı kuruluşun genel fiyatlama politikası, reasürans anlaşmalarının aktüeryal açıdan yeterliliği, kuruluş mali durumu, teknik karşılıkların güvenilirliği ile yeterliliği, sigortacılık faaliyetleri ile ilgili varlık ve yükümlülük riski yönetimi ve sigorta poliçelerine bağlı olarak yapılan yatırımlar için yatırım riski konusunda kuruluş üst yönetimine ve Kuruma güvence sağlamaktır.

Aktüerya fonksiyonu

MADDE 33 – (1) Aktüerya fonksiyonu asgari olarak şu faaliyetleri kapsar:

a) Mevzuatta veya Kurum tarafından belirlenen hususlar saklı olmak üzere, aktüerya fonksiyonunun yerine getirilmesi adına kuruluş bilgi sistemlerinde tutulan ve aktüeryal işlemler ile hesaplamalarda kullanılan her türlü verinin asgari içeriğini belirlemek ve kuruluşun ilgili birimleri tarafından kaydedilen verinin belirlenen asgari içeriğe uygun olmasının temini için gerekli tedbirlerin alınmasını sağlamak.

b) Teknik karşılıkların tahmininde ve fiyatlamada kullanılan verinin yeterliliği ve niteliğinin hesaplamaya uygunluğunu takip etmek, gerekli hallerde iyileştirici tedbirlerin alınmasını sağlamak, yeterli verinin bulunmadığı veya bulunan verinin güvenilir olmadığı durumlarda uygulanacak politikaları belirlemek ve ilgili birimlerle koordine etmek.

c) Teknik karşılıkların tahmininde kullanılan metotlar ile bunlara ilişkin içsel aktüeryal modelleri geliştirmek ve bu hesaplamalarda kullanılan varsayımların uygunluğunu sağlamak, belirlenen güven aralığında teknik karşılıkları tahmin etmek.

ç) Teknik karşılıklara ilişkin tahminlerin gerçekleşmesini takip etmek ve periyodik olarak üst düzey yönetime raporlamak, tahmin ile gerçekleşme arasında belirlenen güven aralığına karşılık gelen anlamlılık seviyesinden fazla sapma olması durumunda üst düzey yönetimi ve denetim komitesini bilgilendirmek ve uygulanan metot ve modeller ile kullanılan varsayımlarda gerekli iyileştirmeleri yapmak.

d) Üçer aylık dönemler itibarıyla beklenen hasar prim oranları ve tarife karlılığı başta olmak üzere portföy analizi yapmak, analiz sonuçlarını ilgili birimlere ve üst düzey yönetime raporlamak, bu tarifelerle ilgili olarak tarife değişikliği önerisinde bulunmak, zarar eden tarifeler ile ilgili iyileşme olmaması halinde müteakip raporlama dönemlerinde üst düzey yönetimle birlikte denetim komitesine raporlama yapmak.

e) Asgari olarak primlerin gelecekteki hasar ve masrafları karşılama yeterliliği; enflasyon etkisi, uyum riskleri ve portföydeki değişimlerin etkisini ve şirket portföyünün risk düzeyinin gelişimini ve değişimini içerecek şekilde yazım ve fiyatlama politikası hakkında yazılı olarak üst düzey yönetime görüş bildirmek.

f) Ürün geliştirmeye ilişkin olarak ürün fiyatı ve ürünün sunumu için gerekli sermaye tutarı hakkında çalışmalar yaparak üst düzey yönetime sunmak.

g) Reasürans anlaşmalarının aktüeryal açıdan yeterliliği hakkında ilgili birime ve üst düzey yönetime görüş bildirmek, gerekli tahmin çalışmalarını da içerecek şekilde yürürlükteki reasürans anlaşmalarının teknik sonuçları hakkında üst düzey yönetime ve denetim komitesine raporlama yapmak.

ğ) Kuruluşun oluşturacağı etkin bir risk yönetimi sistemine ve şirketin sermaye yeterliliğinin değerlendirilmesine katkı sağlamak.

h) Sigortacılık faaliyetleri ile ilgili varlık ve yükümlülük riski yönetimi ile sigorta poliçelerine bağlı olarak yapılan yatırımlar için yatırım riski yönetimine ilişkin politikaların belirlenmesine katkı sağlamak; emeklilik planlarına ilişkin devamlılık ve karlılık analizi yapmak, belirlenen politikalar ve yapılan analizlerin sonuçlarını üst düzey yönetime periyodik olarak raporlamak ve yatırım gelirlerinin teknik kısmı ile teknik olmayan kısmı arasında paylaşımı ile kar paylı poliçelerde karın dağıtımı hakkında değerlendirme yapmak.

ı) Kapsamı ve gönderiliş biçimi Kurum tarafından belirlenen aktüerya raporunu hazırlamak ve eşzamanlı olarak yönetim kurulu ile Kuruma sunmak.

(2) Şirketler tarafından denetim komitesine bağlı aktüerya biriminin haricinde, kendisine bağlı icrai birim bulunan bir yöneticiye bağlı aktüerya biriminin kurulması halinde birinci fıkranın (e), (f) ve (g) bentlerinde belirtilen fonksiyonların bu birim tarafından icra edilmesi; bu durumda denetim komitesine bağlı faaliyet gösteren aktüerya biriminin ise yapılan işlemlerin kontrolünü gerçekleştirmesi esastır. Bu durum söz konusu icrai birimin diğer konularda faaliyet gösteremeyeceği anlamına gelmez. Ancak, bu icrai birim belirtilen konularda faaliyet gösterse dahi, aktüerya fonksiyonunun yerine getirilmesinde nihai sorumluluk denetim komitesine bağlı faaliyet gösteren aktüerya birimindedir.

Aktüerya birimi

MADDE 34 – (1) Bu Yönetmelik kapsamında tanımlanan aktüerya fonksiyonlarını yerine getirmek, bu görevlerle ilgili şirket uygulamalarının takibini yapmak ve gerekli hallerde iyileştirici tedbirlerin alınmasını teminen üst yönetime ve ilgili birimlere düzenli raporlamalar yapmak üzere kuruluşlar nezdinde, idari ve fonksiyonel açıdan denetim komitesine bağlı aktüerya biriminin kurulması zorunludur.

(2) Aktüerya biriminin faaliyetlerini etkin bir şekilde yürütebilmesi için gerekli bilgi sistemleri alt yapısı kurulur ve bilgi işlem desteği sağlanır. Bilgi güvenliği ve iş sürekliliği kapsamındaki talepler, sigortalıların hak ve menfaatlerini tehlikeye düşürecek konuların iyileştirilmesi kapsamındaki talepler, iç denetim raporları çerçevesinde iyileştirme gereklilikleriyle ilgili talepler ve mevzuata uyum kapsamında oluşturulan talepler hariç olmak üzere, aktüerya biriminin bilgi işlem sisteminden talepleri öncelikli talep olarak dikkate alınır.

(3) Aktüerya fonksiyonunun aktüerya ve finansal matematik bilgisine sahip, sigorta ve reasürans şirketlerinin doğası, ölçeği ve karmaşıklığına cevap verebilecek nitelikteki kişiler tarafından icra edilmesi esastır. Bu kapsamda aktüerya biriminde kuruluşun ölçeği, faaliyetlerinin niteliği ve karmaşıklığına uygun yeterli sayıda aktüer veya yardımcı aktüer ile stajyer aktüer çalıştırılır. Belirtilen personelden yeterli sayıda kişi bulunamaması halinde, gerekli nitelikleri haiz uzman veya diğer unvanlarda personel de aktüerya biriminde çalıştırılabilir. Ayrıca, yetiştirilmek üzere uzman yardımcısı istihdamı mümkündür. Kurumca belirlenecek kriterlere göre Kurum asgari sayıda aktüer veya yardımcı aktüer bulundurma zorunluluğu getirebilir.

(4) Aktüerya birimi tarafından hazırlanan, denetim komitesinin görüşü alınmak suretiyle yönetim kurulu tarafından onaylanarak kabul edilen aktüerya birimi yönetmeliğinde, aktüerya biriminin çalışma usul ve esasları ile bu faaliyetleri yürütecek personelde aranan öğrenim durumu, deneyim, bilgi ve beceri seviyeleri ile diğer niteliklere yer verilir.

(5) Aktüerya birimi tarafından icra edilen faaliyetlerin bir personel ile sürdürülmesinin mümkün olduğu kuruluşlarda yönetim kurulunun uygun görmesi, aktüerya birimi yöneticisinin aktüer olması ve Kuruma bildirim yapılması kaydıyla aktüerya birimi görevlerinin birim yöneticisi tarafından yerine getirilmesi mümkündür. Bu durumda yalnızca aktüerya birimi yöneticisinin istihdamıyla aktüerya birimi kurulmuş kabul edilir.

Aktüerya birimi personelinin nitelikleri

MADDE 35 – (1) Aktüerya birimi yöneticisinin atanması ve görevden alınması denetim komitesinin görüşü ile yönetim kurulu tarafından; birim personelinin atanması ve görevden alınması aktüerya birimi yöneticisinin görüşü ile denetim komitesi tarafından gerçekleştirilir.

(2) Aktüerya birimi yöneticisinin aktüer olması esastır. Ancak, istihdam edilecek aktüer bulunamaması halinde Kuruluşta istihdam edilen ve 15/8/2007 tarihli ve 26614 sayılı Resmî Gazete'de yayımlanan Aktüerler Yönetmeliği gereğince aktüer unvanının kazanımı için aranan deneyim şartını haiz yardımcı aktüerlerden veya bunların da yokluğunda belirtilen deneyim şartını haiz stajyer aktüerler arasından, aktüerya birimi yöneticisi yönetim kurulu tarafından belirlenir.

(3) Denetim komitesine bağlı aktüerya biriminde istihdam edilecek aktüer, yardımcı aktüer veya stajyer aktüer haricindeki personelin Aktüerler Yönetmeliği gereğince aktüer unvanının kazanımı için aranan şartlardan aktüerlik sınavlarında başarılı olma şartı hariç diğer nitelikleri taşıması gerekmektedir. Ancak uzman yardımcısı unvanındaki personelde deneyim şartı da aranmaz.

(4) Aktüerya birimi yöneticisi, birim personelinin görev, yetki ve sorumluluklarının gerektirdiği nitelikleri haiz olup olmadıklarını değerlendirir; bu kişilerin aktüeryal konulardaki mesleki bilgi, beceri ve yeteneklerinin geliştirilmesine yönelik eğitim programları hazırlar.

(5) Aktüerya biriminde görevli personel ve birim yöneticisi, görevlerine ilişkin konularda kuruluşun diğer birimlerine sağlayacakları teknik destek ve danışmanlık hizmeti haricinde kuruluş bünyesinde icrai başka görevler ifa edemez.

Sorumlu aktüer

MADDE 36 – (1) Kapsamı ve gönderiliş biçimi Kurum tarafından belirlenen aktüerya raporlarını, mali tabloları ve tarife teknik esaslarını onaylamaktan ve aktüerya fonksiyonuyla ilgili Kuruma yapılacak diğer raporlamalardan sorumlu olmak üzere aktüerya biriminde istihdam edilen yahut

dışarıdan hizmet alınan aktüerlerden biri denetim komitesi tarafından sorumlu aktüer olarak belirlenir. Sorumlu aktüer denetim komitesine bağlı aktüerya biriminin parçasıdır ve aktüerya biriminin görevlerini yerine getirmesinde ve aktüerya fonksiyonunun icrasında birimle birlikte sorumludur.

(2) Aktüerya birimi yöneticisi sorumlu aktüer olarak seçilebilir.

(3) Seçilen sorumlu aktüer, seçimi müteakip ay başında Kuruma bildirilir.

(4) Sorumlu aktüerin kuruluşta istihdam edilmemesi halinde denetim komitesi, hizmet alımı yoluyla seçilen sorumlu aktüerin kuruluşla olan ilişkisinde aktüerya fonksiyonu kapsamına giren konular hariç olmak üzere herhangi bir çıkar çatışması olup olmadığının takibini yapar. Hizmet alımı yoluyla seçilen sorumlu aktüerin veya bu aktüerin çalıştığı firmanın, kuruluşla dış denetim veya başka bir adla hizmet sunup sunmadığının takibi de bu kapsamda yapılır. Çıkar çatışması bulunduğunun tespiti halinde denetim komitesi derhal sorumlu aktüeri değiştirir.

(5) Kurum tarafından sorumlu aktüerin görevini yerine getirmede gerekli yeterlilikleri sağlayamadığının veya sorumlu aktüerin çıkar çatışmalarına konu olduğunun tespit edilmesi halinde Kurumun sorumlu aktüerin değiştirilmesini talep etme yetkisi saklıdır.

Aktüerya fonksiyonuna ilişkin istisna

MADDE 37 – (1) Beşinci bölüm kapsamında aktüerya fonksiyonuna ilişkin faaliyetleri gerçekleştirmek ve aktüerya birimi kurmak yalnızca şirketler ile Doğal Afet Sigortaları Kurumu, Özel Riskler Yönetim Merkezi ve Türkiye Motorlu Taşıt Bürosu için tanımlanmış bir görevdir. Belirtilen özellikli kuruluşlar haricindeki kuruluşlar ile tüzel kişiliği haiz sigorta ve reasürans brokerleri bu bölümden istisnadır.

ALTINCI BÖLÜM
İç Denetim Sistemi

İç denetim sisteminin amacı ve kapsamı

MADDE 38 – (1) İç denetim sisteminin amacı, kuruluş faaliyetlerinin Kanun ve ilgili diğer mevzuat ile kuruluş içi strateji, politika, ilke ve hedefler doğrultusunda yürütüldüğü ve iç kontrol, risk yönetimi ve aktüerya sistemlerinin etkinliği ile yeterliliği hususunda yönetim kuruluna makul bir güvence sağlamaktır.

İç denetim fonksiyonu

MADDE 39 – (1) İç denetim fonksiyonundan beklenen amacın sağlanabilmesi için kuruluşun genel müdürlük birimleri, tüm yurt içi ve yurt dışı şube, bölge müdürlüğü, konsolidasyona tabi ortaklıkları ile acenteleri ve hizmet alınan kuruluşları nezdinde yapılan dönemsel ve riske dayalı denetimlerde asgari olarak;

a) İç kontrol, risk yönetimi ve aktüerya birimlerinin uygulamaları ile yeterlilik ve etkinliklerinin değerlendirilmesi,

b) Muhasebe kayıtları ile finansal raporların doğruluğu ve güvenirliğinin incelenmesi,

c) Operasyonel faaliyetlerin mevzuata ve belirlenmiş olan usullere uygunluğu ile bunlara ilişkin iç kontrol uygulama usullerinin işleyişinin test edilmesi,

ç) Bilgi sistemi ile ana hizmetlerin yürütülmesinde kullanılan tüm sistemlerin güvenilirliğinin gözden geçirilmesi,

d) İşlemlerin, Kanuna ve ilgili diğer mevzuata, kuruluş içi strateji, politika ve uygulama usulleri ile diğer iç düzenlemelere uygunluğunun denetlenmesi,

e) Kuruluş içi düzenlemeler çerçevesinde yönetim kuruluna yapılan raporlamalar ile Kuruma yapılan raporlamaların doğruluğu, güvenilirliği ve zaman kısıtlamalarına uygunluğunun denetlenmesi,

f) Eksiklik, hata ve suiistimalin ortaya çıkarılması; sorunların yeniden ortaya çıkmasının önlenmesine ve kuruluş kaynaklarının etkin ve verimli olarak kullanılmasına yönelik görüş ve önerilerde bulunulması,

g) Acentelik ilişkisi ile sınırlı olmak üzere acentenin bilgi sistemleri, iş süreçlerinin tesisi ve iş sürekliliği ile risk yönetimine ilişkin yükümlülüklerinin denetlenmesi,

ğ) Yönetim kurulu tarafından belirlenen önemlilik kriterleri göz önünde bulundurularak tüm hizmet alımlarının denetlenmesi,

zorunludur.

İç denetim birimi

MADDE 40 – (1) İç denetim biriminin doğrudan yönetim kuruluna bağlı ve idari açıdan bağımsız olarak örgütlenmesi sağlanır. Bununla birlikte iç denetim birimi fonksiyonel olarak yönetim kurulana denetim komitesi aracılığıyla raporlama yapar.

(2) Kuruluşlarda iç denetim fonksiyonu, iç denetim birimi ya da teftiş kurulu tarafından yürütülür. İç denetim biriminde kuruluşun büyüklüğüne, faaliyetlerinin karmaşıklığına, yoğunluğuna, kapsamına ve risk düzeyine bağlı olarak, Kanun ve ilgili mevzuat ile kuruluş içi düzenlemelerde öngörülen denetim hizmetlerinin aksatılmadan ve bu hizmetlerin gerektirdiği seviyede yerine getirilmesi amacıyla yeterli sayıda iç denetçi çalıştırılır. Sigorta grubuna ait şirketlerde tek bir iç denetim birimi sigorta grubuna dahil tüm şirketlerin iç denetim faaliyetlerinde tamamen veya kısmen görev alabilir.

(3) Kuruluşun faaliyetlerinin kapsamı ve karmaşıklığı dikkate alınarak, iç denetim faaliyetlerinin bir iç denetçi ile sürdürülmesinin mümkün olduğu kuruluşlarda, yönetim kurulunun uygun görmesi ve Kuruma bildirim yapılması kaydıyla denetim faaliyetlerinin, iç denetim birimi yöneticisi tarafından yerine getirilmesi mümkündür. Bu durumda yalnızca iç denetim birimi yöneticisinin istihdamıyla iç denetim birimi kurulmuş kabul edilir.

(4) İç denetim birimi tarafından hazırlanan, denetim komitesinin görüşü alınmak suretiyle yönetim kurulu tarafından onaylanarak kabul edilen iç denetim birimi yönetmeliğinde, iç denetim biriminin çalışma usul ve esasları ile bu faaliyetleri yürütecek personelde aranan öğrenim durumu, deneyim, bilgi ve beceri seviyeleri ile diğer niteliklere yer verilir.

(5) İç denetçi, iç denetim faaliyetlerini denetim faaliyetlerine yönelik politika ve uygulama usulleri ile iç denetim planları çerçevesinde yürütür.

(6) İç denetim birimi yöneticisi tarafından;

a) İç denetim faaliyetlerine yönelik politika ve uygulama usulleri belirlenir, denetim komitesinin uygun görüşü alınır ve yönetim kurulunun onayıyla politika ve uygulama usulleri yürürlüğe konur.

b) İç denetim faaliyetleri gözetlenir; denetim politika, program, süreç ve uygulamaları izlenir ve yönlendirilir.

(7) İç denetim birimi yöneticisi, asgari üç ayda bir denetim komitesine iç denetim birimi tarafından icra edilmiş faaliyetlere ilişkin bir rapor sunar ve bunları denetim komitesi ile birlikte mütalaa eder. Denetim komitesi gelen bu raporu, mütalaası ile birlikte, en geç on iş günü içinde yönetim kuruluna iletir. Söz konusu raporda asgari olarak aşağıdaki hususlara yer verilir:

a) Tamamlanan, devam eden, ertelenen ve iptal edilen denetim faaliyetleri ve yıllık denetim planına uyum düzeyi.

b) İç denetçilerin raporlama döneminde aldıkları eğitimler.

c) Önemli muhasebe sorunları ile Kuruma yapılan raporlamalara ve denetim bulgularına ilişkin tereddütlü hususlar.

ç) Risk değerlendirmeleri ve bunların özeti.

d) Denetim bulguları.

e) Düzeltici önlemleri almaya yetkili yöneticilere intikal ettirilen önemli zayıflıkların giderilmesine yönelik görüşler.

f) Kuruluş yönetiminin düzeltici ve risk azaltıcı önlemlere uyma derecesi.

g) Denetim komitesi ve iç denetim birimi tarafından yer alması uygun görülen diğer konular.

(8) Kuruluşların mali durumunu ciddi biçimde zayıflatacak veya olağandışı sonuçlar doğuracak herhangi bir durumun varlığının tespit edilmesi halinde iç denetim birimi hazırlayacağı raporu en kısa zamanda kuruluş denetim komitesine ve yönetim kuruluna sunar. Tespite yönelik en fazla bir ay içinde herhangi bir aksiyon alınmaması halinde bu hususu Kuruma iletir.

İç denetim birimi yöneticisi ve personelinin nitelikleri

MADDE 41 – (1) İç denetim birimi yöneticisi ve personelinin atanması, performans değerlendirmesi ve görevden alınması denetim komitesinin görüşü alınarak yönetim kurulu tarafından yapılır.

(2) **(Değişik:RG-14/2/2025-32813)** İç denetim birimi yöneticisinin en az dört yıllık üniversite mezunu olması ve sigortacılık, özel emeklilik, finans ve denetim alanlarında en az yedi yıl deneyime

sahip olması zorunludur. İç denetim birimi yöneticisi ile aralarındaki evlilik bağı kalkmış olsa dahi eşleri, ikinci dereceye kadar (bu derece dâhil) kan veya kayın hısımları, iç denetim birimi hariç olmak üzere son iki yılda kuruluşta veya konsolidasyona tabi iştiraklerinde çalışamaz; kuruluşla veya iştirakleriyle iş ilişkisinde bulunan kurum ve kuruluşlarda kuruluşla ve iştirakleriyle maddi sonuç doğuran işlemlerde karar alıcı olamaz veya yetkili pozisyonda bulunamaz. İç denetim biriminin denetim ile görevlendirdiği personel, denetim görevini ifa edeceği birimde kan, kayın veya denetime engel teşkil edecek yakınlığı bulunması durumunda iç denetim birimine bu durumu derhal bildirir. Bildirimde bulunan personelin denetime ilişkin görevlendirmesi, iç denetim birimi tarafından iptal edilir.

(3) İç denetçilerin deneyim hariç birim yöneticisinin niteliklerini haiz olması gerekir.

(4) İç denetçilerin mesleki bilgi, beceri ve yeteneklerinin geliştirilmesi amacıyla genel kabul görmüş iç denetim standartları çerçevesinde iç denetim birimi yöneticisi tarafından eğitim programları hazırlanır ve bu programlar dahilinde asgari olarak denetim tekniği, sigorta tekniği, sigorta hukuku ve ticaret hukuku konularında personelin düzenli eğitimler almaları sağlanır.

(5) İç denetçiler görev ve sorumluluklarını tarafsız ve bağımsız olarak icra eder. Bu amaçla iç denetçilerin iç denetim birimi yöneticisi, denetim komitesi veya yönetim kurulu haricinde kuruluş yönetiminde yer alan hiçbir kişiye karşı hesap verme sorumluluğu bulunmaz. İç denetçilerin görevlerinin icrasında menfaat çatışmalarından uzak olmaları sağlanır.

(6) Yönetim kurulunca, iç denetçilere görev ve sorumluluklarını etkin bir şekilde yerine getirebilmeleri için, kuruluşun tüm bölüm ve birimlerinde inisiyatif kullanabilecek, tüm personelinden bilgi alabilecek ve tüm kayıt, dosya ve verilerine ulaşabilecek yetkiyi haiz olmaları sağlanır.

(7) **(Değişik:RG-14/2/2025-32813)** İç denetim birimi yöneticisi, kuruluşta ve sigorta grubunda yeni ürünler, hizmetler veya politika ve uygulama usulleri konusunda sağlayacakları danışmanlık hizmeti haricinde kuruluşta ve sigorta grubunda başka görevler ifa edemez ve iç denetim birimi haricinde herhangi bir birimde görevlendirilemez. Farklı birimlerde geçici olarak görevlendirilen iç denetim birimi çalışanları, iç denetim birimine dönmelerinin ardından bu birimlere ilişkin denetimlerde 1 yıl süreyle görevlendirilemez.

(8) Yedinci fıkra kapsamında iç denetim birimi yöneticisi ve personeli tarafından verilen danışmanlık hizmetleri, danışmanlık konusuna giren hususlara onay verildiği anlamına gelmez.

İç denetim birimi çalışma esasları

MADDE 42 – (1) Kuruluşların dönemsel ve riske dayalı iç denetim faaliyetleri iç denetim planının hazırlanması, yürürlüğe konması, genel kabul görmüş iç denetim standartları esas alınarak çalışma programları aracılığıyla icrası ve denetim raporları çerçevesinde ilgili birim yönetimlerince alınan önlemlerin izlenmesi faaliyetlerini kapsar.

İç denetim planı

MADDE 43 – (1) İç denetim planı, risk değerlendirmelerine dayalı ve yıllık olarak hazırlanır. Takip eden yıla ait iç denetim planı hakkında üst düzey yönetimin ve denetim komitesinin görüşü alınır ve planlar en geç içinde bulunulan yılın aralık ayı sonuna kadar yönetim kurulunun onayıyla yürürlüğe konulur. Kuruluşların yıllık denetim planlarının haricinde uzun dönemli denetim planları hazırlamaları mümkündür.

(2) İç denetim planları dönem içerisinde gerçekleştirilecek özel tahkikatlar, danışmanlık hizmetleri ve alınacak eğitimler de dikkate alınarak hazırlanır. İç denetim planlarında;

a) Riske dayalı değerlendirmeler sonucunda önem ve öncelik değerlendirmesine de yer verilerek dönem içerisinde denetlenecek alanlara,

b) Denetimin amacına,

c) Denetlenecek her bir alan veya faaliyet ile ilgili özet risk değerlendirmelerine, Kanun ve ilgili diğer mevzuata,

ç) Planlanan denetim çalışmasının gerçekleştirileceği zamana ve denetim dönemine,

d) Denetim faaliyetleri için gerekli olan kaynaklara ve kaynak kısıtlamalarının olası etkilerine,

yer verilir.

(3) İhtiyaç hasıl olması halinde iç denetim birimi, tesis edilmiş politikalara uygun olarak denetim planlarını günceller. Denetim planlarında yapılan önemli değişiklikler ve güncellemeler,

denetim komitesinin uygun görüşü ve yönetim kurulunun onayıyla yürürlüğe konulur. Güncellenen planda, güncelleme tarihine kadar gerçekleştirilmiş olan denetim çalışmaları ile bunlara ayrılan zamana ve yapılan önemli değişikliklerin nedenlerine ilişkin açıklamalara yer verilir.

Çalışma programları

MADDE 44 – (1) İç denetim planında belirlenen denetim alanları kapsamında verilen her bir denetim görevi için, kuruluşun denetim alanındaki tüm işlemleri, kullanılacak denetim teknikleri, bilgi elde etmede izlenecek yollar, belgelendirmeye ilişkin uygulamalar ve ulaşılan sonuçlar ile denetim raporunun sunulmasını kapsayacak şekilde bir çalışma programı hazırlanır. Çalışma programında denetim hedefi ve bu hedefe ulaşılması için yapılacak çalışmalara ayrıntılı olarak yer verilir.

(2) Denetimde kullanılan denetim usulleri çalışma kâğıtları şeklinde belgelendirilir. Çalışma kâğıtlarının, denetim görevinin çalışma programında öngörülen şekilde tamamlanıp tamamlanmadığını ve görevin icra ediliş şeklini gösterecek mahiyette tutulması ve ilgili iç denetçinin adı ve soyadı belirtilerek imzalanması esastır. Gerekli tedbirler alınarak ve elektronik imza veya dijital imza kullanılarak bu süreçler dijital olarak da yürütülebilir.

(3) Çalışma programları olağan koşullarda asgari olarak aşağıdaki hususlara ilişkin uygulamaları içerir:

a) Gerek duyulması halinde yapılacak beklenmedik denetimler.

b) Denetlenecek kayıtların kontrolü.

c) İç kontrol sistemlerinin, politikaların ve uygulama usullerinin incelenmesi ve değerlendirilmesi.

ç) Risk değerlendirmeleri.

d) Kanunun ilgili maddesi ya da ilgili mevzuat, düzenleme ve kuralların gözden geçirilmesi.

e) Örnekleme metot ve tekniklerinin kullanımı.

f) Seçilmiş işlemlerin ve hesap bakiyelerinin aşağıdaki uygulamalar yoluyla teyidi:

1) Yardımcı hesaplar, büyük defter kayıtları ve kontrol kayıtlarının birbirleriyle tutarlığının incelenmesi.

2) Kayıtlara esas belgelerin incelenmesi.

3) İstisnai uygulamaların doğrudan incelenmesi ve uygun izleme faaliyetleri.

4) Fiziksel denetimler.

Denetim dönemi

MADDE 45 – (1) Denetim dönemi, iç denetimlerin sıklığını ifade eder. Denetim dönemini olağan koşullarda, denetlenecek faaliyetler ve alanlar ile iç denetçiler ve denetimin yapılabileceği zaman belirler. Risk değerlendirmeleri neticesinde daha riskli olduğu değerlendirilen alanlar, diğer alanlara göre daha sık denetlenir. Ancak her koşulda belirli bir alana ilişkin iki denetim dönemi arasındaki süre 3 yılı geçemez.

(2) İlgili mevzuatta Kurum tarafından yıllık olarak denetleneceği belirtilen alanların ve işlemlerin, iç denetim tarafından da yıllık olarak denetime tabi tutulması gerekmektedir.

(3) İç denetim birimi tarafından; kuruluş merkezi veya genel müdürlükteki tüm birimler, bölge müdürlükleri ve şubeler ile taşra teşkilatları, acenteler ve anlaşmalı servisler de dâhil olmak üzere tüm hizmet alımları yönetim kurulunca önemlilik dereceleri göz önünde bulundurularak onaylanan iç denetim politikaları çerçevesinde gerek yerinden gerekse uzaktan denetlenir ve ulaşılan sonuçlar raporlanır.

(4) Dönemsel ve riske dayalı denetimler haricinde, yönetim kurulunun veya Kurumun talebi üzerine, iç denetimin amacına uygun olarak özel denetimler de iç denetim birimi tarafından yerine getirilir.

İç denetim raporları

MADDE 46 – (1) İç denetim raporlarında denetim konusuyla ilgili olduğu ölçüde ve varsa;

a) Denetimin kapsam ve amaçlarına,

b) Önceki denetim sonrasında alınan önlemlere ilişkin değerlendirmelere,

c) Tespit edilen sorunlar ve sonuçlara ilişkin özete,

ç) Detaylı denetim sonuçlarına (tespit edilen hususlar çerçevesinde denetlenen konuya verilen önem derecesi ve ayrıntılı nedenleri),

d) Önerilere ve bunların faydalarına,

e) Çeşitli kontrol dokümanları ve araçları üzerinden genel veya özel gözlemlere ve izlemeye dayalı kontrol ya da incelemelere,

f) İzledikleri, denetledikleri ve kontrol ettikleri hususlara ilişkin olarak kuruluş personelinden veya acentelerden istenen ilave açıklamalara, bunların bilgi ve görüşlerine, gereken durumlarda kuruluşta bulunan diğer birimlere yapılan uyarılara,

g) Üst yönetim tarafından ihtiyaç duyulabilecek diğer bilgilere,

yer verilir.

(2) Denetim tamamlandıktan sonra, taslak denetim raporunu müzakere etmek, yanlış bilgilerin düzeltilmesini sağlamak, ilgili birim yönetiminin tespitlere ve alınacak önlemlere ilişkin değerlendirmelerini almak üzere iç denetçiler ilgili birim yöneticisiyle görüşür. Bu görüşmeden sonra denetim raporunda yer alan tespitlerin nihai hale gelmesi için alınacak aksiyonlar ve tamamlanma tarihlerine yönelik ilgili birimler ile mutabakat sağlanır. Nihai hale getirilen raporlar iç denetim birimi tarafından denetim komitesine sunulur.

(3) Denetim komitesi gelen raporu mütalaası ile birlikte 10 iş günü içerisinde yönetim kuruluna iletir. Rapor ilk yönetim kurulunda gündeme alınır ve rapor sonuçlarına göre yapılacak işlemler karara bağlanır.

İzleme faaliyetleri

MADDE 47 – (1) İç denetçiler denetim raporlarında önerdikleri ve yönetim kurulunca karara bağlanan konularda düzeltici önlemleri almaya yetkili yöneticilere intikal ettirilen hususlara yönelik uygulamaları izler.

(2) İç denetçiler izleme faaliyetlerinin sonuçlarını ve değerlendirmelerini denetim komitesine iletilmek üzere raporlar. Bu raporlar gelecek dönemlerde yapılacak iç denetim planlarında dikkate alınır.

YEDİNCİ BÖLÜM
İç Sistemlere İlişkin Genel Hükümler

Dışarıdan hizmet alımı ve faaliyetlerin birlikte yürütülmesi

MADDE 48 – (1) İç sistemlere ilişkin birimlerin kuruluş organizasyonu içerisinde yapılandırılması, gerekli personel istihdamının sağlanması ve çalışma planlarının ilgili birimler tarafından hazırlanması koşuluyla; bu birimlerinin yetersiz kaldığı konularda sınırlarının belirli olması kaydıyla iç kontrol, risk yönetimi, aktüerya ve iç denetim fonksiyonlarının yürütülmesinin dışarıdan hizmet alımı yoluyla yerine getirilmesi mümkündür.

(2) İç denetim biriminde teknik yeterliliğe sahip personelin bulunmaması halinde, bilgi sistemleri ile aktüerya fonksiyonunun bulunduğu kuruluşlarda bilgi sistemlerine ve aktüerya fonksiyonuna ilişkin yürütülecek iç denetim faaliyetlerinin dışarıdan hizmet alımıyla gördürülmesi zorunludur. Ancak 33 üncü maddenin ikinci fıkrasında belirtildiği şekilde kendisine bağlı icrai birim bulunan yöneticiye bağlı aktüerya biriminin kurulması ve denetim komitesine bağlı faaliyet gösteren aktüerya biriminin ise yapılan işlemlerin kontrolünü gerçekleştirmesi halinde, aktüeryal faaliyetlerin denetiminde iç denetim biriminin dışarıdan hizmet alımı zorunlu değildir.

(3) İç denetim kapsamında hizmet alınan kişi ve kurumların, sigorta sözleşmesi veya bireysel emeklilik sözleşmesinin düzenlenmesi hariç olmak üzere kuruluşla çıkar çatışması oluşturacak şekilde iş ilişkisinin bulunmaması gerekir.

(4) İç sistemler kapsamında hizmet alınan kuruluşlar tarafından, iş süreçlerinin tesisi ve bilgi sistemleri ile iş sürekliliğinin sağlanması hususunda bu Yönetmelikte belirtilen nitelikler ile hizmet alınan konuya ilişkin ilgili mevzuattan kaynaklanan diğer gerekliliklerin yerine getirilmesi gerekmektedir.

(5) İç sistemler fonksiyonlarının yürütülmesinde dışarıdan hizmet alınması halinde, hizmet alınacak kişi ve kuruluşlarla çalışma kapsamı ve süresi yönetim kurulu veya denetim komitesi tarafından belirlenir. Hizmet alınan kuruluşun nitelikleri ve hizmet alınan alanlara ilişkin bilgiler Kuruma düzenli olarak raporlanır.

(6) Birden fazla şirketle iş ilişkisi bulunan acentelerde yürütülecek iç kontrol, risk yönetimi ve denetim faaliyetlerinden her şirket kendi acentelik ilişkisi kapsamında ayrı ayrı sorumludur. Ancak, şirketin politikalarıyla uyumlu olması kaydıyla, bu acenteler için belirtilen faaliyetlerin acentelik veren şirketlerce koordinasyon halinde icra edilmesi veya diğer şirket tarafından yürütülen bu konulardaki faaliyetlerin sonuçlarının kullanılması mümkündür.

(7) Finansal grup bünyesinde yer alan şirketlerde, finans sektöründe faaliyet gösteren konsolidasyona tabi ortaklıklar dışındaki bir ortağın iç sistemler kapsamında yürüttüğü faaliyetler, üçüncü fıkra hariç olmak üzere bu maddede yer alan gerekliliklerin sağlanması kaydıyla ve yönetim kurulunun uygun görmesi halinde, iç sistemler kapsamında dışarıdan hizmet alımı olarak değerlendirilebilir.

(8) Sigorta grubuna ait şirketlerden birindeki denetim komitesi ile iç sistemler kapsamında kurulan birimler sigorta grubuna dahil tüm şirketlerin iç sistemler kapsamında yürüteceği faaliyetlerde tamamen veya kısmen ortak olarak kullanılabilir.

Önemlilik seviyesi

MADDE 49 – (1) Açıkça belirtilmiş olsun veya olmasın, bu Yönetmelik kapsamında yürütülen faaliyetler önemlilik seviyesi gözetilerek yürütülür.

(2) Önemlilik seviyesinin belirlenmesine ilişkin ilke ve esaslar yönetim kurulu tarafından belirlenir. Önemlilik seviyesinin belirlenmesinde, işlemin finansal etkisi ile iş sürekliliği, bilgi güvenliği ve kuruluş itibarına etkisi gibi hususlar birlikte dikkate alınır.

(3) Kuruluşun genel ölçeğindeki önemlilik seviyesi üst düzey yönetimin ve iç sistem birim yöneticilerinin görüşü alınarak yönetim kurulu tarafından, icrai birimlerin her birinin faaliyetlerindeki önemlilik seviyesi ise yönetim kurulu tarafından belirlenen ilke ve esaslara uygun olarak ilgili üst düzey yöneticiler tarafından belirlenir. Birimler için belirlenen önemlilik seviyesinin uygunluğu, ilgisine göre iç kontrol, risk yönetimi ve iç denetim birimlerince yürütülen faaliyetlerde kontrol edilir.

(4) Finansal tabloların yeniden yayımlanmasını gerektirecek nitelikteki finansal etkiler ile hasar ödeme süreçlerinde veya paydaşların kullandığı sistemlerde yarım iş gününü aşan kesintiler, aktif azaltıcı işlem yasağı kapsamına giren hususlar, yatırım politikalarına dair mevzuatta getirilen kısıtlamalar ve Kurum tarafından belirlenecek diğer hususlar kuruluşun genel ölçeğinde her hâlükârda önemlidir.

Brokerlerin iç sistemler kapsamındaki yükümlülükleri

MADDE 50 – (1) Tüzel kişiliği haiz sigorta ve reasürans brokerleri bu Yönetmelikte tanımlanan ve asgari olarak bilgi sistemleri, iş süreçlerinin tesisi ve iş sürekliliğini kapsayan iç kontrol ve risk yönetimine ilişkin gereklilikleri sağlamak ve iç denetim fonksiyonunu ifa etmekle yükümlüdür. Bu brokerlerin iç kontrol ve risk yönetim fonksiyonlarının ifasında ayrı bir birim kurma yükümlülüğü bulunmamakla birlikte, faaliyetlerinin nitelikleri ve işletme büyüklükleri dikkate alınarak iç denetim birimi kurma zorunluluklarına ilişkin usul ve esaslar Kurum tarafından belirlenir.

İç sistemler birim yöneticisi ve personelinin mali ve sosyal hakları

MADDE 51 – (1) İç sistemler birim yöneticisi ve personelinin mali ve sosyal hakları ile performans kriterleri denetim komitesi veya yönetim kurulu tarafından belirlenir. Ancak, bu birimler için doğrudan kuruluşa kâr veya gelir sağlama odaklı performans kriteri belirlenemez. Doğrudan kuruluşa kâr veya gelir sağlama odaklı olmayan bu kriterlere göre yapılan ödemeler, esas sözleşme hükmüne veya genel kurul kararına dayalı olarak tüm personele kârdan yapılan ödemeler ve istihdam edilen biriminin faaliyetleri kapsamında sağlanan haklar hariç olmak üzere, birim yöneticisi ve personeline performansa dayalı olarak herhangi bir ad altında ücret veya benzeri bir gelir sağlanamaz.

İç sistem birim personelinin görevden alınması ve istifası

MADDE 52 – (1) İç sistem birimi yöneticilerinin, sorumlu aktüerin ve iç denetim birimi personelinin herhangi bir nedenle görevden alınması halinde söz konusu değişiklik gerekçeleriyle birlikte kuruluş tarafından Kuruma yazılı olarak bildirilir. Görevden almaya ilişkin kuruluşça yapılacak bildirimde birim yöneticileri ve personelinin görevden alınması halinde görevden alınan kişilerin sorumlu oldukları fonksiyonlara ilişkin konularda, sorumlu aktüerin görevden alınması halinde ise

sorumlu aktüerin aktüeryal konularda kuruluşla anlaşmazlık yaşanıp yaşanmadığına ilişkin beyanına da yer verilir.

(2) İç sistem birimi yöneticilerinin, iç denetim birimi personelinin ve sorumlu aktüerin göreviyle ilgili nedenlerle veya kuruluşun yönetimine ilişkin uygulamalar sebebiyle istifa etmesi halinde, istifa gerekçesinin Kuruma yazılı olarak bildirilmesi gerekir.

Doğal Afet Sigortaları Kurumu ve Özel Riskler Yönetim Merkezi hakkında özel hüküm

MADDE 53 – (1) Doğal Afet Sigortaları Kurumu ve Özel Riskler Yönetim Merkezi için iç sistemlerin işletici şirketler bünyesinde kurulması mümkündür.

(2) İşletici şirketler işlevsel görev ayrımını tesis etmek kaydıyla iç kontrol, risk yönetimi ve aktüerya fonksiyonunu, ayrı bir birim kurmaksızın kendi bünyelerinde kuracakları birimler eliyle yürütebilir. Bu durumda, Doğal Afet Sigortaları Kurumu ve Özel Riskler Yönetim Merkezi için bu Yönetmelik gereği yapılacak faaliyetler kapsamında doğrudan bu kurumların yönetim kurullarına karşı sorumlu olunur; işletici şirketlerin yönetim kuruluna karşı sorumlu olunmaz.

(3) İşletici şirketler iç denetim fonksiyonunu münhasıran Doğal Afet Sigortaları Kurumu ve Özel Riskler Yönetim Merkezi için çalışan iç denetçiler eliyle yürütür. Bu kurumların birden fazlasının faaliyetlerinin aynı işletici şirket tarafından yürütülmesi halinde, ilgili kurumların yönetim kurullarınca uygun görülmesi şartıyla, görevlendirilen iç denetçiler bu kurumların tümü adına görev yapabilir. Bu iç denetçiler idari olarak işletici şirketin iç denetim biriminde çalışsa bile, seçiminde ve görevden alınmasında işletici şirketin yetkisi bulunmaz.

SEKİZİNCİ BÖLÜM
Raporlamalar ve Kurumun Denetleyici Görevleri

Kuruma yapılacak raporlamalar

MADDE 54 – (1) İç kontrol fonksiyonu kapsamında aşağıdaki raporlar hazırlanır:

a) Kuruluş tarafından tanımlanan iş süreçlerinin ve bu süreçlerde yıl içinde yapılan değişikliklerin açıklandığı ve güncel iş akış şemaları ile bu şemalarda yıl içinde yapılan değişikliklerin verildiği iş süreçleri hakkında rapor.

b) Bilgi sistemlerinin yapısı, bilgi sistemleri kapsamında yapılan hizmet alımları, iş sürekliliğinin sağlanması konusunda alınan tedbirler ve bu konularda planlanan ve yürütülen çalışmalar ile yapılan testlere ilişkin bilgi sistemleri raporu.

c) İç kontrol fonksiyonu kapsamında yıl içinde yapılan kontroller ve sonuçları hakkında rapor.

(2) Risk yönetim fonksiyonu kapsamında aşağıdaki raporlar hazırlanır:

a) Risk yönetim politikaları ve bu politikalarda yıl içinde yapılan değişiklikler ile risk limitleri ile ve bu limitlerde yıl içinde yapılan değişikliklere ilişkin bilgiler.

b) Üstlenilen ve maruz kalınan risklerin uzun vadeli olarak sermaye yeterliliğine ve şirket sürekliliğine etkilerinin ölçüldüğü sermaye yeterliliği etki analiz raporu.

c) Kurumca belirlenen senaryolar altında uygulanacak stres testi sonuçlarına ilişkin rapor.

ç) Risk yönetim fonksiyonunun icrası kapsamında yıl içinde yapılan takip ve izleme faaliyetlerinin sonuçları hakkında rapor.

(3) Aktüerya fonksiyonu kapsamında aşağıdaki raporlar hazırlanır:

a) Kapsamı Kurum tarafından belirlenen aktüerya raporu.

b) Tarife karlılığı tespit raporu ile tarife karlılığının temini için yıl içinde yapılan önerilere dair özet rapor.

c) Şirket tarafından uygulanan aktüeryal metotlar ile kullanılan modeller ve varsayımlar ile bu o modeller ve varsayımlarda yıl içinde yapılan değişiklikler ile gerekçeleri hakkında rapor.

ç) Aktüerya fonksiyonunun icrası kapsamında yıl içinde yapılan işlemler hakkında rapor.

(4) İç denetim fonksiyonu kapsamında aşağıdaki raporlar hazırlanır:

a) Yıl içinde yürütülen iç denetim faaliyetleri ile bu denetim faaliyetlerindeki bulgular hakkında rapor.

b) Raporlama dönemine ait yıl için hazırlanan denetim planı.

c) İlgili yıl için planlandığı halde gerçekleştirilmemiş denetim faaliyetlerine ilişkin tamamlanmama gerekçelerine dair rapor.

(5) Yönetim kurulu tarafından aşağıdaki raporlar hazırlanır:

a) Yönetim kurulu üyeleri ile iç denetim birim yöneticisinin ve personelinin kendileri ile ikinci dereceye kadar (bu derece dâhil) kan veya sıhri hısımlarının; kuruluşla, kuruluşun konsolidasyona tabi iştirakleriyle ya da kuruluşla acentelik veya ticari temsilcilik şeklinde ticari bağlantıları bulunan kuruluşun hakim ortaklarıyla iş ilişkisi veya ticari bir ilişkisinin bulunup bulunmadığına dair rapor.

b) İç sistemler kapsamında kurulan birimlerin yönetim kuruluna yaptığı raporlamalar kapsamında yapılan işlemler ve alınan tedbirler hakkında rapor.

c) İç sistemler kapsamında yapılan dış hizmet alımlarının kapsamı ve süresi ile hizmet alınan kişi veya kuruluşların, kuruluşla diğer iş ilişkileri hakkında rapor.

(6) Yönetim kurulu tarafından gönderilecek raporlar hariç olmak üzere, her yıla ilişkin raporlar müteakip yılın Nisan ayı sonuna kadar, yönetim kurulunun hazırladığı raporlar ise Mayıs ayı sonuna kadar Kuruma gönderilir. Birimler tarafından hazırlanacak raporda birim yöneticisi ile en az bir denetim komitesi üyesinin imzasının bulunması şarttır. Kurum, denetleyici görevlerinin etkin şekilde yürütülmesini, kuruluşların iş yükünün dengeli olmasını ve raporlama faaliyetlerinde yeknesaklığın sağlanmasını teminen raporların kapsamı ve gönderiliş biçimi ile ilgili düzenleme yapabilir, her bir kuruluşa mahsus özel rapor isteyebilir.

Kamuoyuna yapılacak raporlamalar

MADDE 55 – (1) Kuruluşlar tarafından her hesap yılı itibarıyla düzenlenecek yıllık faaliyet raporunda, diğer konulara ek olarak, iş sürekliliği yönetimi kapsamında yapılan faaliyetlere, iç sistemler kapsamında kurulan birimlerin ayrı ayrı faaliyetlerine, şirket iç sistemleri ve iç sistemler dışındaki bölümlerinin dış hizmet alımlarına ilişkin bilgilere yer verilir.

(2) **(Değişik:RG-14/2/2025-32813)** Ticari sır niteliğindeki bilgiler hariç olmak üzere ve kişisel verilerin korunması kapsamındaki hususlar dikkate alınmak suretiyle şirketler ve özellikli kuruluşlar, kapsamı ve içeriği Kurum tarafından belirlenen raporları kullanıcılar tarafından ana sayfa üzerinden kolayca ulaşılabilecek şekilde kendi internet sitelerinde Ocak-Mart, Nisan-Haziran, Temmuz- Eylül, Ekim-Aralık dönemleri için üçer aylık dönemler itibarıyla dönem bitimini takip eden ay sonuna kadar yayımlar. Bu raporlar beş yıl boyunca yayımdan kaldırılmaz ve dönemler itibarıyla karşılaştırılabilir olarak sunulur.

(3) İkinci fıkrada belirtilen raporların yayımlanması Birlik tarafından takip edilir. Her yayım dönemini takip eden hafta, raporları yayımlamayan şirketler ve özellikli kuruluşlar Birlik tarafından uyarılır. Ek bir hafta içinde raporları yayımlamayanlar ve normal süresinden geç yayımlayanlar bir liste ile Kuruma bildirilir.

(4) Birlik, şirketlerin ve özellikli kuruluşların raporlarından Kurum tarafından belirlenenleri toplulaştırır ve şirketler itibarıyla karşılaştırma yapılabilir şekilde kendi internet sitesinde yayımlar.

(5) **(Mülga:RG-14/2/2025-32813)**

DOKUZUNCU BÖLÜM
Çeşitli ve Son Hükümler

Yürürlükten kaldırılan yönetmelik

MADDE 56 – (1) 21/6/2008 tarihli ve 26913 sayılı Resmî Gazete'de yayımlanan Sigorta ve Reasürans ile Emeklilik Şirketlerinin İç Sistemlerine İlişkin Yönetmelik yürürlükten kaldırılmıştır.

Geçiş hükümleri

GEÇİCİ MADDE 1 – (1) Denetim komitesi üyeleri için sayılan şartları sağlayan en az iki yönetim kurulu üyesi en geç bu Yönetmeliğin yayımlanmasını takip eden iki yıl içinde atanır. Bu süre içinde denetim komitesinin görevleri yönetim kurulu eliyle yürütülür. Yönetim kurulu üyelerinden en az birinin belirtilen görevlerin icrası için görevlendirilmesi mümkündür. Belirlenen bu üyenin görevini bağımsız ve tarafsız olarak yürütmesi gerekir.

(2) 5 inci maddenin dördüncü fıkrasında belirtilen iç sistemlere ilişkin konuların görüşüldüğü yönetim kurulu toplantılarına katılacak yönetim kurulu üyelerinin, 6 ncı maddenin birinci ve dördüncü fıkralarında tanımlanan denetim komitesi üyelerinin ve 41 inci maddenin ikinci fıkrasında belirtilen iç denetim birimi yöneticisi ile personelinin kendilerinin, aralarındaki evlilik bağı kalkmış olsa dahi eşlerinin ya da ikinci dereceye kadar (bu derece dâhil) kan ya da sıhri hısımlarının ilgili maddelerde belirtilen görevlerde son iki yıllık sürede bulunmamasına ilişkin getirilen sınırlama bu Yönetmeliğin yayımı tarihinden itibaren şirketler ve özellikli kuruluşlar için üç yıl, brokerler için beş yıl uygulanmaz.

(3) İç sistemler birim yöneticileri; şirketlerde bu Yönetmeliğin yayımlanmasını takip eden altı ay içinde, özellikli kuruluşlarda bir yıl içinde, iç denetim birimi özelinde sigorta ve reasürans brokerleri için ise beş yıl içinde atanır. Mevcut durumda, bu Yönetmelikte belirtilen nitelikleri haiz birim yöneticileri bulunan kuruluşlarda atama yapılmış kabul edilir.

(4) Bu Yönetmeliğin yayımı tarihinden itibaren 3 yıl süreyle aktüerya birimi yöneticisinde aktüer, yardımcı aktüer veya stajyer aktüer olma şartı aranmaz.

(5) İç sistemler birimlerinin kuruluşu ve organizasyonu birim yöneticilerinin atanmasından sonra bir yıl içinde tamamlanır ve fonksiyonlar işlerlik kazanır. Mevcut durumda kuruluşlarda kurulu bulunan birimlerin ise bir yıl içinde bu Yönetmelikte belirtilen fonksiyonları icra edebilir hale getirilmesi gerekir. İç kontrol ve risk yönetim faaliyetlerine ilişkin birim kurma zorunlulukları bulunmayan tüzel kişiliği haiz sigorta ve reasürans brokerlerinin, bu Yönetmeliğin yayımını takip eden beş yıl içinde iç kontrol ve risk yönetim sistemlerini oluşturmaları gerekir.

(6) Bilgi sistemlerinin belirlenen standartlara uyumlu hale getirilmesi için Kurumun üç yılı aşmayacak şekilde yayımlayacağı uygulama planı esas alınır.

(7) 5 inci maddenin dördüncü fıkrasında yer alan toplantılara katılma yasağı bir yıl boyunca uygulanmaz.

(8) İç sistemler kapsamında mevcut durumda Kuruma yapılan raporlamalar ile yönetim kurulunun yapacakları dışında ilk kez yapılacak raporlamalar iç sistemler birim yöneticileri atandıktan bir yıl sonra yapılır. İlk raporlamalarda, yapılan faaliyetler yerine fonksiyonun kuruluşu kapsamında yapılan işlemler ve birimin planlanan yapısı hakkında özet bilgi verilir.

(9) Yönetim kurulu bu Yönetmelikte öngörülen raporlama faaliyetlerini öngörüldüğü tarihte yapar. Ancak, raporların içeriğinde bu maddede öngörülen geçiş süreleri kapsamında yürütülen işlemler dikkate alınır.

(10) 55 inci madde kapsamında ilk raporlama 2023 yılının Ocak-Mart döneminde yürütülen faaliyetler için yapılır. Bu tarihten önce yapılan faaliyetler için raporlama yapılması gerekmez.

(11) Kurum, kuruluş iç sistemlerinin kurulması ve işletilmesine, denetim komitesinin, birim yöneticilerinin ve personelinin atanmasına, bilgi sistemlerinin bu Yönetmelikte belirtilen standartlara uyumlu hale getirilmesine, Kuruma ve kamuoyuna yapılacak raporlamalara ilişkin bu maddede belirtilen geçiş sürelerini ihtiyaç duyulması halinde bir yıl uzatabilir.

Yürürlük

MADDE 57 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 58 – (1) Bu Yönetmelik hükümlerini Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu Başkanı yürütür.

	Yönetmeliğin Yayımlandığı Resmî Gazete'nin	
	Tarihi	**Sayısı**
	25/11/2021	31670
	Yönetmelikte Değişiklik Yapan Yönetmeliklerin Yayımlandığı Resmî Gazetelerin	
	Tarihi	**Sayısı**
1.	14/2/2025	32813
2.		