TÜRKİYE BANKALAR BİRLİĞİ

(UK Financial Services Authority-FSA)

Finansal Kurumlar İçin Risk Değerlendirme Çerçevesi*

Ocak 2004

(*) İngiltere Finansal Hizmetler Otoritesi (Financial Services Authority-FSA) tarafından yayımlanan "The Firm Risk Assessment Framework" başlıklı bu doküman Türkiye Bankalar Birliği tarafından FSA'nın izni alınarak İngilizce'den Türkçe'ye derlenmiştir. Dokümanın orijinal metni FSA'nın web sayfasında (*www.fsa.gov.uk*) yer almaktadır.

İçindekiler

Giriş

Ekler:

Giriş

1. 2000 yılı Haziran ayında "A New Regulator for the New Millennium"da (Yeni Milenyumda Yeni Düzenleyici) gelecekteki düzenlemelere ilişkin olarak önerdiğimiz yaklaşım tanımlanmıştır. Bu çalışmada, yasal hedeflerimizi paylaşmak amacıyla yerleştirmeye çalıştığımız operasyonel çerçevenin sınırları çizilmiştir.

2. Finansal düzenlemelerle ilişkili olarak seçilen 4 yasal hedef amaçlarımızı açıklamaktadır. Bu hedefler üzerinde çalışırken iyi düzenleme prensibinin dikkate alınması gerekmektedir. İkinci kez güncellenmiş olan "Yeni Düzenleyici İlerleme Raporu 2" (New Regulator Progress Report 2), hazırladığımız firma değerlendirme çerçevesi ile söz konusu temel hedeflerin ve prensiplerin, organizasyonların şeffaf, bütünleşmiş ve risk temeline dayalı bir yapıda faaliyet göstermeleri sürecine nasıl aktarılacağını göstermektedir.

Risk değerlendirme çerçevesi nedir?

3. Bir grup stratejik amacın kullanıldığı değerlendirme çerçevesi yasal hedeflerimize ulaşmak için çalışmalarımızı planlamamızda yardımcı olacaktır. Bu amaçlar, daha geniş bir faaliyet çevresinin değerlendirilmesinden, risk değerlendirme çerçevemizin sonuçlarına, aldığımız herhangi bir yeni sorumluluğa kadar uzanmaktadır. Stratejik amaçlar (ve ne elde etmek istediğimizi tanımlayacak olan stratejik sonuçlar) hem firma hem de tüketici, ürün, piyasa ya da sektör düzeyinde düzenleyici yaklaşımımızı belirlemek açısından önceliklerimizi ve kaynak dağılımını yönlendirmektedir. Yılda bir kez, bu işlev gerçekleştirilir, plan ve bütçemizde sonuçlar rapor edilir.

4. Bu doküman, firmaların genel değerlendirme çerçevesinin bir unsuru- risk değerlendirme çerçevesi- hakkında çok daha detaylı bilgi vermek ve firmaların bu değerlendirmelere hazır olmalarına yardımcı olmaktadır.

5. Geliştirdiğimiz bu risk değerlendirme çerçevesi geçmişte hazırlanan ve önde gelen kuruluşlarca kullanılan tüm diğer dokümanların yerini almıştır. Sonuç olarak, FSA'nın tüm çalışmalarında aşağıda yer alan "risk değerlendirme çerçevesi" dokümanı esas alınacaktır.

Firmanız için risk değerlendirme süreci niçin önemlidir?

6. Risk değerlendirme süreci ve yönetiminin firmanız için önemli olmasının nedenleri aşağıda yer almaktadır;

- Firmanızın taşıdığı riskler hakkındaki kararımız düzenleyici programımızın genel yoğunluğunu belirleyecektir.
- Risk azaltma programı çerçevesinde yapılanlar doğrudan risk değerlendirme sürecinin sonuçlarına dayanmaktadır.
- Üst düzey yönetimin sorumluluğuna yüksek düzeyde güven duyulması konusuna ayrı bir önem verilmektedir.
- Firmanın sermaye yeterlilik rasyosunun değiştirilip değiştirilmeyeceğine karar verme sürecinde risk değerlendirmesi dikkate alınacak en temel veridir.

Dokümanın içeriği nedir?

7. Bu dokümanın içinde yer alan bölümler hakkındaki açıklamalar aşağıdadır;

- Birinci bölümde risk çerçevesine genel bir bakış yer almaktadır.
- İkinci bölümde bir risk değerlendirmesine hazırlık için neler yaptığımız, riskleri nasıl değerlendirdiğimiz, yasal hedeflerle nasıl ilişkilendirdiğimiz, risk azaltma programının nasıl hazırlandığı ve dahili değerlendirme sürecimiz anlatılmaktadır.
- Üçüncü bölümde firmanız için risk değerlendirme çerçevesinin ne anlama geldiği açıklanmaktadır; bu çerçevede risk değerlendirme ve risk azaltma evreleri için tipik bir zaman çizelgesi sunulmakta, firmalardan talep ettiğimiz bilgi türleri belirtilmekte, risk değerlendirme süreci ve sonuçlarının firmaya ne şekilde iletileceği hakkında bilgi verilmektedir.
- Eklerde ise konuyla ilgili diğer ayrıntılılara ve sıkça sorulan sorular bölümüne yer verilmiştir.

Bu dokümanı kimler okumalıdır?

8. **Bu doküman, risk değerlendirme çalışması ve sonuçlarına ilişkin karar alınmasında üstlendiği göreve dayanarak yönetim kurulu üyeleri de dahil olmak üzere firma üst düzey yönetimi için hazırlanmıştır.** Buradaki yaklaşımımız, etkin iç kontrollerin işleyişi ve firmanın yasal yükümlülüklere uygun olarak faaliyet göstermesinde üst düzey yönetimin taşıdığı sorumluluğa verdiğimiz öneme paralellik göstermektedir. Doküman aynı zamanda, firmada bizimle iletişimde olan ve risk değerlendirme çalışmasının koordinasyonunda yer alan diğer firma çalışanlarına (örneğin, mali işler, risk, uyum ve iç denetim fonksiyonlarının üst yönetiminde bulunan kişiler) da hitap etmektedir.

9. Firma risk değerlendirme çerçevesi tüm yetkili firmalara ve resmi teşekküllere uygulanmaktadır.

10. Yetkili firmalar (authorized firms) ile yetkili teşekküllere (recognized bodies) uygulanan risk değerlendirme çerçevesinde önemli farklılıklar bulunması halinde bu iki kavram farklılığına başvurulmasına rağmen, uyum **açısından dokümandaki finansal kurumların tümü için "firma" kavramı kullanılmaktadır.**

İngiltere Finansal Hizmetler Otoritesi (FSA)

Türkiye Bankalar Birliği'nin Değerlendirmesi

Finansal kurumların etkin gözetimi ve denetimi ödeme sisteminin çalışmasında ve tasarrufların dağıtılmasında önemli bir rol oynayan finansal sektörün güven içinde ve verimli çalışmasının en önemli unsurlarından birisidir. Gözetim ve denetim işlevinin temel amacı, finansal kurumların taşıdıkları risklere karşılık yeterli sermayeyi tutabilmelerini sağlamak ve bu kurumların, sermayelerinin korunması için güvenilir koşulların yaratıldığı bir ortamda faaliyette bulunmalarını temin etmektir.

Finansal kurumlarda etkin gözetim ve denetim, her ülkenin finansal sistemindeki istikrarın sağlanmasında kritik rol oynar. Etkin bir gözetim ve denetime ilişkin temel prensiplerin belirlenmesinde esas alınan temel görüşler şunlardır:

1- Finansal sektörde gözetim ve denetim işlevinin temel amacı istikrarı ve güveni temin etmek ve böylece ödünç alan ve ödünç verenlerin maruz kalacakları riskleri en aza indirmektir.

2- Gözetim ve denetim otoritesi, iyi yönetimi teşvik etmeli ve finansal piyasalarda şeffaflığın ve denetimin artırılmasını sağlamak suretiyle piyasa disiplinin oluşturulmasını ve sürdürülmesini desteklemelidir.

3- Gözetim ve denetim otoritesi taşıdığı sorumlulukları yerine getirmek ve görevlerini etkin olarak sürdürebilmek için faaliyetlerinde bağımsız olmalı, finansal kurumlardan gerekli bilgilerin temin edilmesi ve aldığı kararların uygulanması konusunda gerekli yasal yetki ve araçlara sahip olmalıdır.

4- Gözetim ve denetim otoritesi bir finansal kurumun yaptığı işi tam olarak anlamalı ve taşıdığı risklere ilişkin etkin risk yönetimi yapmasını sağlamalıdır.

5- Etkin gözetim ve denetim her bir finansal kurumun risk profilinin bilinmesini ve denetime ilişkin kaynakların uygun olarak dağılımını gerektirir.

6- Gözetim ve denetim otoritesi finansal kurumların taşıdıkları riskler için yeterli kaynak bulundurmalarını (sermaye, güvenilir yönetim, etkin kontrol sistemi, muhasebe kayıtları gibi) temin etmelidir.

Finansal sektörde gözetim ve denetim sistemi, uygun maliyet ve yüksek kalitede finansal hizmet sunan etkin ve rekabete açık bir sistemini teşvik etmelidir. Gözetim ve denetim otoritesinin sağladığı güven ve koruma seviyesi ile finansal aracılık yapmanın maliyeti arasında bir ilişki olduğu bilinmelidir. Bankalara ve finansal sisteme tanınan risk taşıma toleransının azaltılması ve daha zorlayıcı ve maliyeti daha yüksek olan bir denetim sisteminin öngörülmesinin yeni kaynakların yaratılması ve dağıtılmasında ters yönlü bir etki yaratması aşikardır.

İyi denetlenen bir finansal sistem tasarrufların daha etkin dağılımında da imkan verecektir. Denetim otoritesinin görevi herhangi bir kurumu da korumak veya diğerlerine zarar vermesini engellemek değildir, otorite bir bütün halinde finansal sistemin sağlığı ve etkinliği ile tasarruf sahiplerinin ve finansal sektöre yatırım yapan hissedarların haklarının korunması ile ilgilidir.

Finansal sektörde yetkili otoriteler kendi yetki alanlarında yer alan ve finansal sektörde faaliyetinde bulunan tüm kurumların gözetim ve denetiminde benzer prensipleri uygulamalıdırlar.

Finans sektörü ekonomik faaliyetler için anahtar bir sektördür, fakat aynı zamanda kendisi de ticari bir sektördür; üstelik siyasi, ekonomik, teknolojik ve her alandaki gelişmeden ilk ve en çok etkilenen sektörlerin başında gelmektedir.

Finansal sektörde faaliyet göstermek doğal olarak risk almayı gerektirmektedir. Finansal kurumların faaliyetlerinden dolayı maruz kaldıkları risklerin başlıcaları ana gruplar altında toplanabilir. Bunlar, kredi riski, ülke ve transfer riski, piyasa riski, faiz riski, likidite riski, faaliyet riski, yasal risk ve itibar riskidir.

Gözetim ve denetim otoritesi ile finansal kurumların yöneticileri finansal kurumların maruz kaldığı risklerin tanınması, izlemesi, ve kontrolünün yapılması konusunda önemli bir rol oynar. Gözetim ve denetim işlevinin en önemli kısmı yetkili otoritece, söz konusu bu risklerin yönetiminde uyulması gereken sermaye yeterliliği, kredi karşılıkları, aktif yoğunluğu, likidite yönetimi, risk yönetimi ve iç denetim gibi ihtiyati düzenlemelerin geliştirilmesi ve uygulanmasını sağlamaktır. Bazen kantitatif, yani ölçülebilen zaman zaman zaman da kalitetif özellikte olan bu düzenlemeler finansal kurumların sınırsız riskler almasını sınırlandırmak içindir. Öte yandan bu düzenlemeler zorunluluk göstermediği sürece finansal kurumların yönetimine ait kararların önüne geçmemeli ancak bu kurumların uygun şekilde faaliyette bulunmaları için gerekli asgari standartları zorunlu kılmalıdır.

Finansal sektörün dinamik yapısı, finansal sektörde faaliyet gösteren ihtiyati kurallara uyulduğunun denetlenmesi ve bu kurallara uyumun sürdürülmesi hususlarını olduğu kadar yeni koşullar altında da gerekli kurallara uyulacağı hususunun değerlendirilmesini gerektirir.

Mali sektörde mesleki ve ahlaki yüksek standartların gelişmesi ve bankacılık faaliyetleriyle bilerek ya da bilmeyerek kötüye kullanımların engellenebilmesi için risk yönetiminde bankaların uygun politikalarının ve uygulamaları olmalıdır.

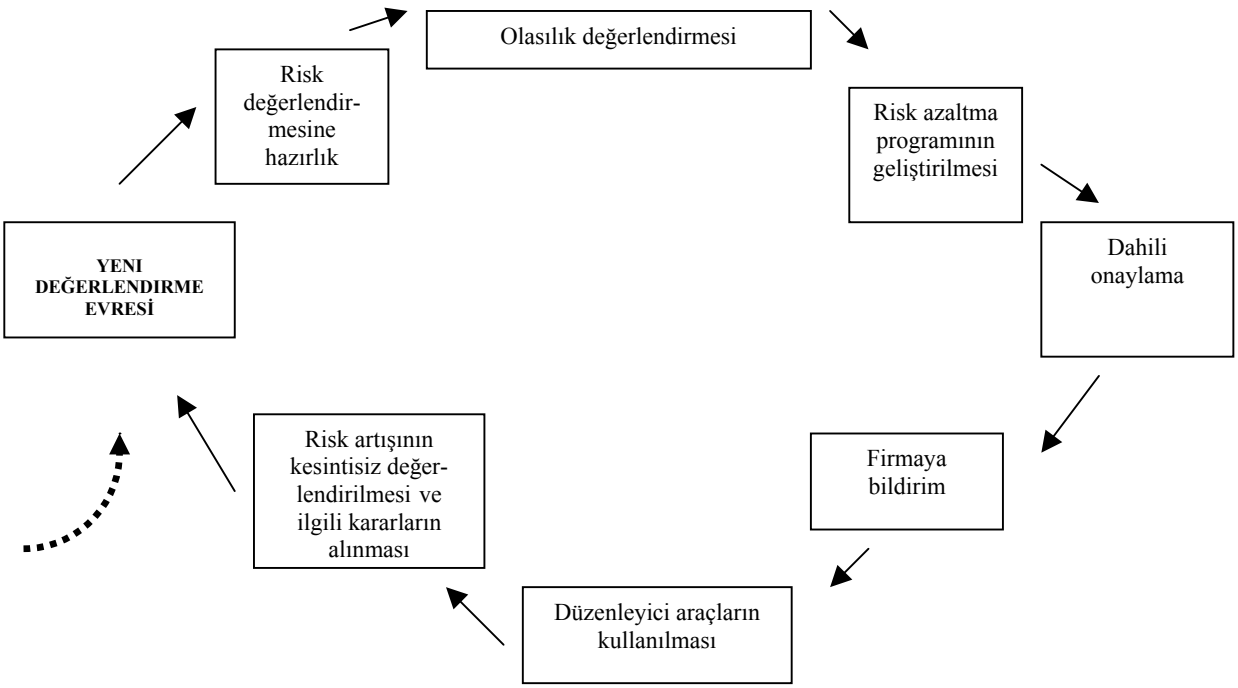
İlerideki gelişmeler ne yönde ve nasıl olursa olsun, düzenleme/denetimin ve finansal kurumların iki konuya ağırlık vermesi gerekmektedir, bunlar risklerin iyi yönetilip yönetilmediğinin denetlenmesi ve denetimin etkin olmasıdır. Finansal sektörde artan küreselleşme içerideki denetim ve düzenlemenin uluslararası uyumunu da önemli hale getirmektedir. Bu nedenle finansal sektörü yakından ilgilendiren gelişmeler hususunda gerekli ve uygun adımlar zamanında atılmalıdır.

Türkiye Bankalar Birliği

1. Risk değerlendirme çerçevesine genel bakış

1.1. Firma risk değerlendirme çerçevesi, denetim otoritesinin önem verdiği ve bir risk azaltma programı geliştirilmesine yön verecek riskler üzerinde yoğunlaşarak oluşturulan bir dizi yapısal aşamadan oluşmaktadır. Bu aşamalar Şekil 1'de gösterilmektedir.

Şekil 1: Firma Risk Değerlendirme Çerçevesi



1.2. Risk değerlendirme çerçevesinin 9 temel özelliği bulunmaktadır.

- Üzerinde yoğunlaşacağımız riskler; yasal hedeflerimizin gerçekleştirilmesi karşısında risk oluşturan risklerdir ki, bu bir firmanın yönettiği risklere normal bakış açısından farklı bir bakış açısıdır. Dolayısıyla, bu dokümanda kullanılan "risk" kavramına bu farklı anlam yüklenmektedir.
- Riskler tanımlarken ve değerlendirirken, yasal hedeflerimiz üzerindeki etkileri ve gerçekleşme olasılıklarını dikkate alırız.
- Firmanız düşük etkili olarak değerlendirildiyse, firmada firma bazlı risk değerlendirme ya da risk azaltma programı bulunmuyor demektedir. Bu tür firmalar, temel izleme, bu bilgi ile tanımlanan risklere karşı aksiyon gerçekleştirme ve sektör genelinde incelemenin bir parçası olarak sektör ve iş kolunda uyum standartlarının izlenmesine yönelik uygulamalar esas alınarak izlenmektedir. İzleme işlevi aynı zamanda bir firmanın düşük etki (low impact) kategorisi dışına çıktığının fark edilmesine ve firma bazlı risk değerlendirme ve risk azaltma programına ihtiyaç duyulmasına imkan sağlayacaktır.
- Risk değerlendirme bir denetim değil yüksek düzeyde bir inceleme ya da el kitabımızla uyumu kontrol edecek detaylı testleri içeren bir süreçtir.

- Risk değerlendirme firmayı etkileyen dış risklerle birlikte iş (business) ve kontrol risklerinin tanımlanmasını içeren süreçtir. Bu riskler, yedi çeşit düzenleyici risk altında firmanın yasal (statutory) hedeflerini ne şekilde etkilediğine bakılarak değerlendirilir. Söz konusu riskler "hedeflere yönelik risk grupları"(Risk to objectives groups-RTO groups) olarak tanımlanmıştır ve yasal hedeflerle ne şekilde ilişkilendirildiği Ek 1'de açıklanmaktadır.
- Beklentilerimizde bir firmanın kontrolünün bu dokümanda açıklanan özelliklere tamamen uygunluk göstereceği yaklaşımında değiliz, daha çok bir firmanın yaptığı işin özellikleri ve ölçeği ile ilişkilendirmeye çalışıyoruz.
- Risk değerlendirmenin çıktısı firmanızın taşıdığı risklere ilişkin incelemenin ortaya konulduğu bir mektuptur. Bu mektup aynı zamanda teşhis edilen konuları açıklayan ve bu konulara işaret etmek üzere alınacak önlemleri belirleyen bir risk azaltma programını da içermektedir.
- Risk azaltma programına yaklaşımımız, etkin iç kontrollerin oluşturması ve sürdürmesi ile firmanın düzenleyici kural ve yükümlülüklere uyum içinde faaliyet göstermesinde üst düzey yönetimin sorumluluklarına dikkat çekmektir.
- Firmanız, risk profiline bağlı olarak bir zaman çizelgesine göre yeniden değerlendirilecektir. Eğer firmanın taşıdığı riskler, risk azaltma programında maddi değişiklik yapılmasına dikkat çekiyorsa değerlendirmemizi yeniden inceleyeceğiz.

2. Risk değerlendirme çerçevesini nasıl kullanırız?

2.1. İlgili aşamalar aşağıda sıralanmış ve takip eden bölümlerde açıklanmıştır.

a. Risk değerlendirmesi için hazırlık
b. Olasılık değerlendirmesi
c. Risk azaltma programının geliştirilmesi
d. Dahili onaylama
e. Değerlendirmeye ilişkin sonuçların, - risk azaltma programı hakkında bilginin- firmaya bildirilmesi
f. Risk artışının kesintisiz değerlendirilme ve yanıt verilmesi

a. Risk değerlendirmesi için hazırlık

Etki değerlendirmesi

2.2. Risk değerlendirmesine hazırlık aşamasındaki ilk adım firmanızın etkisinin değerlendirilmesidir. Bu değerlendirme, firmanızın düzenleyici yükümlülüklere göre yaptığı raporlamanın bir parçası olarak daha önceden sağladığı nicel bilgi (örneğin, yıllık brüt gelir, toplam aktifler/pasifler) kullanılarak yapılmaktadır. Firmanızın faaliyet gösterdiği sektöre (bankacılık, sigortacılık, aktif yönetimi gibi) bağlı olarak değişen etki sınırları (eşikleri) karşısında değerlendirilen bu bilgiler kullanılarak bir dereclendirme (puanlama) sistemi geliştirdik. Halihazırda, düzenleyici otoritenin özel dereceleri geçersiz kılmak üzere karar yetkisini kullanabilmesine rağmen bir firma tüm yasal hedefler karşısında genel bir etki derecesi alabilir. Dört yasal hedefle ilgili olarak farklı etki dereceleri kullanmaktayız. Böylece gelecekte firmanız her bir hedef için farklı etki dereceleri alabilir.

2.3. Ek 2'de mevcut etki sınırlarına ve derecelerine örnekler verilmiştir. Bunlar sektördeki her bir firma için yüksek, orta yüksek, orta düşük ve düşük dereceleri tanımlamak için kullanılmıştır.

2.4. Tek bir firma ya da bir çok firmanın bir araya gelmesinden oluşan bir grubun farklı sektörlere ilişkin faaliyetleri bulunuyorsa, sektör ölçümlerinden işletme ya da grup etki derecesini bulmak için "bir araya getirme işlevi"nden yararlanırız. Ancak , bu dokümanda bir araya getirme yönteminden bahsedilmemiş, temel odak noktamız olasılık değerlendirmesinin firma için ne anlama geldiği olmuştur.

2.5. Bir grubun parçası olup ta birden fazla firma için yapılan müşterek değerlendirme hariç olmak üzere, düşük etki grubu altında oluşturulmamış tüm firmalar tek tek risk değerlemesine tabi olacaklardır. Ayrıca, düşük etki oluşumuna rağmen ve yasal hedefler karşısında sürekli risk özelliği taşımadığı halde bir risk değerlendirmesi yapılan bazı özel durumlar da bulunmaktadır. Örneğin, brüt prim geliri olmadığı için düşük etki grubunda bulunan ve yeni bir faaliyet alanına açık olmayan bir sigorta firması için risk değerlendirmesi yapılabilir. Risk değerlendirmesine tabi olması durumunda firmanızın alacağı etki derecesini bildiren bir mektup sürecin sonunda tarafınıza gönderilecektir.

Grupların değerlendirilmesine yönelik tanımlama birimleri

2.6. Bir diğer hazırlık aşaması, değerlendirilecek birimlerine karar vermek için firmanın yasal, faaliyet ve yönetim yapısının incelenmesidir. Değerlendirmenin temel birimi tek bir firmadır. Bunun nedeni, çoğu zaman bir firmanın yapısının, risk değerlendirme çerçevesinin firma geneline uygulanmasına imkan verecek ölçüde basit olmasıdır. Dolayısıyla, risk değerlendirme çerçevesi, düzenlemeye tabi faaliyetlere bakılmaksızın, firmanın maruz kaldığı tüm riskleri kapsayacak şekilde düzenlenir.

2.7. Ancak, çoğu durumda bu yaklaşım uygun olmayabilir; örneğin birçok firmanın yer aldığı bir grubun olması ve bu grubun yasal, yönetim ve/veya organizasyon yapısının karmaşık olması. Bu durumda değerlendirmeye tabi olmak üzere seçilecek birim ya da birimler grubun organizasyon yapısından ve yönetiminden etkilenecektir. Bu da, grubun fiziki iş birimlerinin tanımlanmasıyla yapılmaktadır. Bunlar organizasyonda farklı yönetim yapısı olan birimlerdir, gelir sağlayan faaliyetleri sürdürmekte ve grubun genel riski açısından tek başlarına önem taşımaktadırlar. Grup bazında kontrol ve destek fonksiyonları (örneğin risk yönetimi, iç denetim ve enformasyon teknolojisi sistemleri-IT sistemleri) da ayrıca değerlendirilecektir.

2.8. Bir firmada fiziki iş birimlerinin nerede tanımlanacağına dair durumlar bulunmaktadır; örneğin firmanız çok büyük ölçekliyse ve birçok farklı iş aynı firmada yapılıyorsa fiziki iş birimlerinin olması risk değerlendirmesine yardımcı olacaktır.

2.9. Fiziki iş birimlerini yüzde 10 eşik aralığını kullanmak suretiyle hesaplayarak, tüm önemli iş birimlerinin değerlendirmeye dahil edilmesini sağlamış oluruz; örneğin gelir, vergi öncesi kar ya da firma veya grup sermayesinin yüzde 10'u ya da fazlası gibi. Ayrıca, firmanız ya da bir denetçi (supervisor) bir birimin fiziki birim olduğunu, ancak yüzde 10 eşik aralığı ile yakalanamayacağını düşünürse, bu birim fiziki iş birimi olarak dahil edilebilir.

2.10. Bu sürecin anlamı, çok daha karmaşık yapıdaki organizasyonlar için birden fazla firmayı kapsamak üzere fiziki iş birimlerinin değerlendirilmesidir. Bununla birlikte birden fazla firma için müşterek değerlendirme yapılması durumunda sorunların çıkacağı bazı tüzel kişilikleri tanımlayabiliriz.

Fiziki iş birimi örnekleri

1. Bir sigorta grubunda üç temel iş birimi bulunmaktadır. Birçok yetkili firma bu temel iş birimlerinin kapsamına girmektedir. Bunlar hayat sigortası, genel sigorta ve reasürans'dır. Grup, sermaye dağılımına ilişkin etkin ve gelişmiş önlemlere sahip değildir, ancak bir karlılık dağılımı söz konusudur. Buna göre birimler firmanın vergi öncesi karının sırasıyla yüzde 45, yüzde 30 ve yüzde 7'sini temsil ederler, ancak denetim otoritesi reasürans biriminin önemli risklere maruz kalabileceğinin farkındadır. Ancak denetim otoritesi hayat ve genel sigorta birimleri toplamı yüzde 10'luk karlılık sınırını geçtiğinden ve reasürans biriminde 10 olarak belirlenen sınırın alınan riskleri karşılayamayacağına bağlı olarak bu üç birimi de fiziki iş birimi olarak tanımaya karar verir.

2. Bir yatırım bankası grubunda iki iş birimi bulunmaktadır.; menkul kıymetler ve aktif yönetimi; bu birimlerin her birinde bir dizi yetkili firma bulunmaktadır. İş birimleri bağımsız olarak yönetilmektedir ve grubun vergi öncesi karındaki payları sırasıyla yüzde 70 ve yüzde 30'dur. FSA'nın farklı departmanları menkul kıymet ve aktif yönetimi şirketleriyle ilgilidir. İlgili denetim otoritesi menkul kıymetlerin tek başına bir iş birimi, aktif yönetiminin ise başka bir iş birimi olduğuna karar verebilir. İlgili denetim otoritesi risk değerlendirmesini yetkili firmalar üzerinden değil bu iki maddi iş birimi üzerinden yürütebilir.

Hukuki konular

2.11. Risk değerlendirmesi başlamadan önce, hedeflerimize ilişkin bölgesel kapsamı ve sınır ötesi denetim otoriteleri ile nasıl çalışabileceğimizi dikkate almalıyız. Hedeflerimizin özellikleri, bazı firmaların uluslararası olma özelliği, AB direktiflerinin etkisi ve bunların değerlendirmenin nasıl uygulanacağı üzerindeki etkilerine bağlı olarak hukuki sorunlar ortaya çıkmaktadır.

2.12. Piyasa güveni ve kamuoyunun farkında olduğu hedefler İngiltere finansal sistemince bilinmekte ve güvencesinde olmasına karşın Finansal Hizmetler Piyasalar Kanunu'nda diğer yasal hedefler büyük ölçüde coğrafik olarak bağlayıcı değildir. Bununla birlikte dokümanda, İngiltere'deki piyasalar ve tüketiciler üzerinde durulmuştur. Bunun nedeni, sınır ötesi piyasalar ve düzenleyici sistemler üzerinde doğrudan kontrol yetkimizin bulunmamasıdır. İyi düzenleme prensipleri gereği, diğer konularla birlikte kaynaklarımızın etkin ve verimli olarak kullanımını ve yaklaşımlarımızın uygunluğunu sağlamamız gerekmektedir.

2.13. Ancak, sınır ötesi faaliyetlerden kaynaklanan risklerin firmalar üzerindeki etkilerini dikkate almalı ve AB direktifleriyle tanımlanan sorumluluklarımız kapsamında daha geniş sorumluluklar üstlenmeliyiz; örneğin konsolide denetim otoritesi olarak ya da ev sahibi ülke düzenleyici otoritesi olarak ihtiyati düzenlemelerden sorumluyuz. Bu durumda sınır ötesi ülkenin denetim ve düzenleyici otoriteleriyle olabildiği ölçüde birlikte çalışacağız.

2.14. Kendi sorumluluklarımızı yerine getirmek için sınır ötesi ülke düzenleyici otoriteleri ile birilikte çalışırken, etkinliklerine göre yaptığımız değerlendirmelere bağlı olarak söz konusu otoriteler arasında bir ayrıma gidebiliriz. Değerlendirmelerde genel kabul görmüş uluslararası düzenleyici standartlara ve muhasebe standartlarına bağlılık gibi (örneğin Basel Komite'nin Temel İlkeleri) dikkate alınan çeşitli kriterler bulunmaktadır. Sizin firmanız açısından bunun anlamı; tüm diğer koşullar eşit olduğu takdirde sınır ötesi düzenleyici otoritenin daha az etkin olduğu yargısının olduğu durumlarda, bizim daha fazla çalışma yapmamız ve firmaların İngiltere'deki faaliyetlerinin güvence altına alınması hususunu araştırmamız demektir.

Hukuki konulara örnekler

1. Bir Avrupa bankası İngiltere'de bir şubesi aracılığıyla faaliyet göstermekte, ayrıca perakende aracılık faaliyetleri ve toptancı tahvil piyasasında iş birimleri bulunmaktadır. AB Bankacılık Konsolidasyon Direktifine göre bu banka diğer AB ülkelerinde, ihtiyati sorumluluk menşe ülkede olmak üzere, faaliyet gösterebilmekte olduğundan, bizim bu firma üzerinde ihtiyati denetim yetkimiz bulunmamaktadır. Ne var ki şubenin likiditesi, İngiltere'deki tüketicilere düzenlenmiş ürünlerin satışının yapılması, İngiltere'de piyasanın kötüye kullanımı, finansal yenilikler, şube aracılığıyla karaparanın aklanmasının önlenmesi gibi konularda sorumluluklarımız bulunmaktadır. Örneğin, bu firmanın risk değerlendirmesinde uygulanabilir "hedeflere yönelik risk grupları" (Risks to objectives groups-RTO groups); yanlış davranış/kötü yönetim, piyasanın kötüye kullanımı, tüketici bilinci, hile veya sahtekarlık, karapara aklanmasıdır (Ek 1). Ayrıca, bu firma İngiltere'de tahvil piyasasında önemli bir oyuncu olduğundan menşe ülkedeki düzenleyici otoritenin ihtiyati denetiminden ve ihtiyati riskler açısından doğrudan sorumlu olmamamıza rağmen piyasa güveni hedefimize yönelik riskleri (söz konusu firmanın finansal başarısızlığı nedeniyle ortaya çıkabilecek sorunlar nedeniyle) yeterli şekilde işaret ettiğinden emin olmalıyız.
2. Avrupa Ekonomik Alanında ikamet eden bir banka, şubesi aracılığıyla İngiltere'de faaliyet göstermektedir. Teknik olarak buradaki ihtiyati sorumluluğumuz, yasal bir varlık olarak tüm bankayı kapsamaktadır. Bu firmanın risk değerlendirmesinde uygulanacak olan hedeflere yönelik risk grupları içinde sadece finansal başarısızlık risk grubu tüm banka düzeyinde, diğerleri İngiltere'deki şube düzeyinde uygulanır. Bankanın tümden değerlendirilmesinde, etkin olduğuna inandığımız menşe ülke düzenleyici otoritesine daha fazla itimat ederiz (dolayısıyla daha az çalışma yaparız), daha az etkin olduğuna inandığımız menşe ülke düzenleyici otoritesine daha az itimat ederiz (dolayısıyla daha fazla çalışma yaparız).

b. Olasılık değerlendirmesi

2.15. Olasılık değerlendirmesinin iki amacı bulunmaktadır. Birincisi, hem bizim yasal hedeflerimizi hem de firmanızı etkileyecek ya da firma içinde oluşacak risklerin gerçekleşme olasılığının değerlendirilmesini isteriz. İkinci olarak, bu risklerin tespit edilmesine yönelik bir risk azaltma programı geliştirilmesinde yaptığımız bu değerlendirmeyi kullanırız.

2.16. Olasılık değerlendirmesine firmanıza ilişkin bir risk haritası geliştirilmesi de dahildir. Söz konusu risk haritasında, harici olaylar ve tehditler dikkate alınır, firmaya ait özel riskler tanımlanır ve bu riskler basit bir şekilde derecelendirilir (skorlama).

2.17. Olasılık değerlendirmesi, firmanız tarafından sağlanan yeni bilgiler ve mevcut veriler ışığında oluşan riskleri değerlendirdiğimiz bir masa başı çalışmayı da içermektedir.

Çevresel değerlendirme

2.18. Firmanıza ait bir risk haritası oluşturmanın ilk adımı çevresel değerlendirmedir. Bu değerlendirme, firmanıza yönelik harici riskleri, doğrudan ya da dolaylı olarak firmanızın faaliyetlerini etkileyen riskleri kapsar ya da kontrol eder. Bir kez tanımlanmış olması durumunda çevresel riskler olasılık değerlendirmesinin diğer temel aşamalarında da dikkate alınır.

2.19. Çevresel riskler altı temel kategoride toplanmaktadır; siyasi/yasal, sosyal-demografik, teknolojik, ekonomik, rekabet ve piyasa yapısı.

Çevresel risklere örnekler

1. Perakendeci bir firma, kendi ürünlerini üretmek ve kendi müşterilerine dağıtmak suretiyle, uzun vadeli tasarruf işinde yer almaktadır. Önemli çevresel faktörlerin (örneğin polarizasyon rejimindeki değişiklikler, hissedarlar için ürünlerin piyasaya girmesi ve diğer firmaların yarattığı rekabet) firmanın işini ve risklerinin kontrolünü nasıl etkileyeceğini bilmek isteriz. Aynı zamanda, söz konusu çevresel koşullara bağlı olarak firmanın stratejisindeki değişikliklerden kaynaklanabilecek riskleri anlamaya çalışırız, özellikle de herhangi bir değişikliğin müşterilerin yönetimini ve kontrol yapısını nasıl etkileyeceğini bilmek isteriz.

2. Finansal Risk Genel Görüntüsüne göre önemli sayıda müşterinin borçlarını döndürmekte zorluk çektiği görülmektedir. Perakendeci ipotek piyasasında yer edinmiş önemli bir firmanın, bizim müşteri araştırmamız ışığında, portföyüne nasıl bir stres testi uyguladığını anlamak ve ipotek portföyünün müşteri geri ödemelerinde yaşanacak daha ileri boyuttaki zaafiyetlere karşı ne kadar kırılgan olduğunu görmek isteriz.

Firmaya özel risklerin tanımlanması

2.20. Risklerin tanımlanmasının iki yönü bulunmaktadır; riskler nasıl oluşur? ve hangi yasal hedefleri etkiler? Risk değerlendirme çerçevesinin sorunlara göre belirlenmesi amaçlanmıştır. Ne var ki, denetçilerin risklerin nelerden kaynaklandığını tanımlamalarına yardım etmek için 4 temel iş grubu ve 5 kontrol risk grubu altında yer alan 45 ayrı risk unsuru bulunmaktadır. Bu risk grupları şunlardır:

- İş riski (business risk)
  - strateji
  - piyasa, kredi, sigorta ve faaliyet riski

- finansal sağlık
- müşterilerin kullanıcıların ve ürünlerin/hizmetlerin özellikleri

- Kontrol riski (control risk)
  - müşteri/kullanıcı yönetimi
  - organizasyon
  - dahili sistemler ve kontroller
  - yönetim kurulu, üst yönetim ve personel
  - iş ve uyum kültürü

2.21. Her risk grubu, tanımlanmış risklerin derecelendirilmesi için farklı risk unsurlarına göre ayrılmıştır. Bu unsurlar firmanızın değerlendirilmesinde dikkate alınan bir kontrol listesi değildir. Bu unsurlar, firmanızın maruz kaldığı iş ve kontrol risklerinin nasıl ve ne ölçüde değerlendirileceği konusunda denetim otoritesinin dikkate aldığı alanlar hakkında daha fazla bilgi vermektedir. Aynı zamanda bir risk azaltma programı hazırlanmasının alt yapısını oluşturmaktadır. Söz konusu risk unsurları Ek 3'de verilmiştir.

2.22. Tanımladığımız iş ve kontrol risklerini yasal hedeflerimizle ilişkilendirmek isteriz. Bunun için de 7 ayrı risk grubundan (RTO groups) bir ya da birkaçını etkileyip etkilemediğine bakarız (Ek 1). Bunlar:

- Finansal başarısızlık: (Firmanın finansal başarısızlığı nedeniyle ortaya çıkabilecek piyasa güveni ve tüketicinin korunması hedeflerine ilişkin risklerdir.) Yüksek etki firmaları/grupları için finansal başarısızlık nedeni olacak düzeyde olmayan ancak bazı piyasalarda firma/grubun ölçeği nedeniyle piyasa güvenini olumsuz etkileyecek derecede önemli olan olası finansal zararları içermektedir.
- Yanlış davranış/ kötü yönetim: (Firmalarca ürünlerinin yanlış tanıtımı ya da satışı nedeniyle tüketicinin korunması ve piyasa güveni hedeflerine yönelik riskler)
- Tüketici bilinci: (Firmalarca satılan ürünler hakkında tüketicinin eksik bilgisi olmasından kaynaklanan piyasa güveni ve kamuoyu bilinci hedeflerine ilişkin riskler)
- Hile ya da sahtekarlığın yansıması: (Firmalarda hile ve sahtekarlığın yansımasından kaynaklanan finansal suçların engellenmesi ve piyasa güveni hedeflerine ilişkin riskler)
- Karaparanın aklanmasının yansıması: (Firmalar aracılığıyla karaparanın aklanmasından kaynaklanabilecek finansal suçların engellenmesi ve piyasa güveni hedeflerine ilişkin riskler)
- Piyasa özellikleri: (Bir piyasanın etkin olarak çalışmasına engel olan bozukluklardan kaynaklanan, piyasa güveni ve tüketicinin korunmasına yönelik riskler). Bu hedeflere yönelik risk grupları sadece İngiltere piyasalarının çalışmasında önemli olan belli başlı yetkili firmalara ve yetkili teşekküllere ilişkindir.

2.23. Risklerin tanımlanması süreci firmanız hakkındaki mevcut bilgilerin kullanılmasıyla başlayacaktır. Gerekirse bu süreçte yerinde çalışmalar yapılarak (özellikle yüksek etkili firmalar için) risklerin tanımlanması ve doğrulanması desteklenecektir. Firmanızı ziyaret etmeden önce daha fazla bilgi talep edilebilir. Bu bilgiler sayesinde yerinde çalışmaların, bilgi eksikliği olan, iş ya da kontrol yapısının değiştiği ya da doğrulamaya ihtiyaç duyulan alanlarda yoğunlaştırılması sağlanacaktır.

2.24. Risk değerlendirme çerçevesinin bu aşamasına ait sonuçlar ise 7 risk unsuru ya da hedeflere yönelik risk gruplarıyla ilgili bir dizi riskin tanımlanması olacaktır.

Risklere örnekler

Yüksek getirili ürünlere ilişkin olarak tüketicilerden çok sayıda şikayet aldık. Bu şikayetleri yerinde yaptığımız çalışmalarda daha detaylı araştırdık ve sonuç olarak satış esasına dayalı eğitimlere ilişkin prosedürlerin zayıf olduğunu, piyasa materyalleri üzerindeki kontrollerin açık olmadığını ve satış işlevinin izlenmesi ne yönelik uyum işlevi için yeterli düzeyde personel ayrılmadığını tespit ettik.

Bu kontrol başarısızlıklarının satış esasına dayalı eğitim ve istihdam, finansal tanıtım, kamuoyuna bilgi verilmesi/ürün literatürünün yeterliliği, uyum, kültürüne ait konular ve iş kültürü risk unsurları açısından birçok bileşeni bulunmaktadır. Bu bileşenler yanlış davranış/kötü yönetim ve tüketicilerin korunması hedeflerine yönelik risk grupları üzerindeki etkileri açısından değerlendirilmeli ve risk azaltma programında ele alınmalıdır.

2.25. Tek bir risk değerlendirme çerçevemizin olmasına rağmen sektörler ve piyasalar arası farklılıklar, uyguladığımız şekilde bu çerçeve içine adapte edilmiştir. Bu, prensip olarak farklı risk unsurları ve hedeflere yönelik risk grupları yapısının farklı bölümleri kullanılmak suretiyle yapılmıştır.

Sektörel uygulama örnekleri

1. Bir piyasa altyapısı sağlayıcısı başvuracağı belli risk unsurlarına sahip olacaktır, ancak bunları diğer firmalara uygulayamayabilir. Bu unsurlar, piyasanın yanlış çalıştığı (piyasa etkinliği, piyasanın temizliği, ve takas-mutabakat düzenlemeleri dahil olmak üzere) durumlar üzerinde yoğunlaşmaktadır. Diğer risk unsurları, örneğin müşteri yönetimine dair unsurlar, uygulanabilir olmayabilir.
2. Sadece toptancı piyasalarda mevduat toplayan ve kurumsal bankacılık alanında faaliyet gösteren bir bankanın başvurduğu genel bir müşteri/kullanıcı risk grupları yönetimi (müşteri aktif portföyleri tutulması hariç) ya da müşterilerin hedeflere yönelik risk gruplarına dair bilinçlendirilmesi politikası olmayabilir.
3. Dahili denetim fonksiyonunun olması zorunlu olmayan küçük bir firma bu özel risk unsurunu uygulamayacaktır.

Risklerin derecelendirilmesi ve toplanması

2.26. Tanımlanmış ticari riskler (iş riskleri) ve kontrol risklerinin yasal hedeflerimizle ilişkilendirilmesini istediğimiz için risk unsurlarını, etkileyebilecekleri hedeflere yönelik risk gruplarına göre derecelendiririz. Derecelendirme sürecinde yüksek, orta yüksek, orta düşük, düşük, bilinmiyor ve veri mevcut değil olmak üzere 6 ayrı derece kullanılır.

- Veri mevcut değil: Risk unsuru ve hedeflere yönelik risk grupları arasında ilişki bulunmamaktadır.
- Bilinmiyor: Yetersiz bilgi- eğer ilgili ise daha ileri bir araştırma yapılmalıdır.
- Düşük: Temerrüt derecesi-reaksiyon yok
- Orta düşük: İşaretlenmiş risk-seçime bağlı eylem
- Orta Yüksek: Önemli risk-azaltılmadıysa eylem beklenir.
- Yüksek: Yüksek risk-azaltılmadıysa eylem gereklidir.

2.27. Yukarıda bahsedildiği gibi derecelendirme risk unsuru seviyesinde yapılır, örneğin; bahsedilen risk unsurunun hedefe yönelik risk gruplarından birisini temsil etmesi durumundaki risk. Yukarıdaki örnekte olduğu gibi bir çok bileşenden oluşması halinde bu derecelendirmede tek bir sorun çok sayıda risk unsuruna karşılık gelen bir derecelendirmeye yol açabilir. Bu derecelendirmede ayrıca ticari riskler grubunu derecelendiririz, yani riskler üzerinde kontrollerin etkilerini dikkate almadan derecelendirme yaparız.

2.28. Her bir yasal hedef karşısında genel olasılık derecesini bulmak için detaylandırılmış derecelerin hepsini bir araya getiririz. Derecelerin toplanmasında temel prensip kontrol risklerinin ticari riskleri azaltabilir ya da artırabilir olmasıdır. Ayrıca, derecelerin toplanması sürecinin herhangi bir seviyesinde sonucun bir risk kararını yeterli yansıtmadığının düşünülmesi halinde denetim otoritesinin toplama yöntemini geçersiz kılma yetkisi bulunmaktadır.

Risk derecelerinin toplanmasına örnek

FATF üyesi olmayan ülkelerden çok sayıda sınır ötesi yerleşik müşterilerin yer aldığı bir müşteri tabanına sahip olan bir firmanın önemli boyutta nakit işlemleri içen bankacılık işleri bulunmaktadır. Sonuç olarak karaparanın aklanmasının önlenmesiyle ilgili hedeflere yönelik risk grubu ile ilişkili olarak ticari riskleri "yüksek" olarak değerlendirilmiştir. Ne var ki, firma karaparanın aklanmasının önlenmesi konusunda kapsamlı ve iyi test edilmiş kontroller (iyi personel eğitimi, etkin hesap açma prosedürleri, etkin hesap izleme programları, ispatlanmış eskalasyon prosedürleri, bu alanda güçlü kontrollere bağlı bir üst yönetim dahil olmak üzere) yapmaktadır. Sonuçta karaparanın aklanmasının önlenmesine ilişkin kontrol riskleri "düşük" derece olarak değerlendirilmiştir.

Karaparanın aklanmasının önlenmesi konusundaki söz konusu ticari riskler ve kontrol riskleri karaparanın aklanmasının önlenmesi hedefine yönelik risk grubu için "genel" derece, göreceli olarak yüksek ticari risk üzerindeki güçlü kontrollerin etkisini yansıtmak için "orta" derece olarak bulunmuştur. Firma diğer finansal suçlarla ilgili hedefin (piyasanın kötüye kullanımı ile hile veya sahtekarlığın tekrarlanması) diğer bileşenleri için ise "düşük" risk grubunda değerlendirilmiş, böylece yasal hedef karşısındaki genel olasılık derecesi "orta düşük" olmuştur.

2.29. Bu dokümanda derecelerin toplanması yöntemimiz hakkında detaylı bilgi verilmemektedir. Bunun nedeni ise firma bazlı risk unsuru derecelerinin risk azaltma amaçlarımızın konusu olması ve firmanızın bu konuya kendi dikkatini yoğunlaştırmasını istememizdir.

2.30. Ek 4'de detaylı derecelendirme matrisine bir örnek verilmiş, ek 5'de ise derecelere ilişkin bir özet yer almıştır. Her bir yasal hedef karşısındaki genel olasılık derecesi, firmanıza gönderilen etki derecesi ile birlikte Ek 5'in sonunda gösterilmektedir.

c. Risk Azaltma Programının Geliştirilmesi

2.13. Yerinde ziyaretlerimiz de dahil olmak üzere olasılık değerlendirme sürecinin tamamlanmasını takiben firmanız içim bir risk azaltma programı geliştirmek için çalışmaya başlayacağız. Risk azaltma programları sonuçlarına yönelik olarak tasarlanan düzenleyici eylem programlarıdır. Bunun anlamı; risk değerlendirme süresince tanımladığımız sorunlara ilişkin olarak ulaşmak istediğimiz sonuçlara göre bir dizi düzenleyici araç seçmemizdir.

2.32. Risk azaltma programı, firmanızın risk değerlendirmenden hareketle ve tanımlamış olduğumuz sorunlara işaret etmek üzere tasarlanır. Seçeceğimiz düzenleyici araçların türü riskin derecesine, yapısına ve aradığımız sonuçlara bağlıdır. Birçok durumda bu araçlar bizim harekete

geçmemizden ziyade özel bir sonuca erişilmesi için firmanızın harekete geçmesini gerektirecektir ki bu da bizim üst yönetimin taşıdığı sorumluluklara yaklaşımımızla uyumludur.

2.33. Amaçlarına göre (bazı araçlar birden fazla amaca hizmet edebilmekle birlikte) düzenleyici araçlar aşağıdaki gibi sınırlandırılır:

- Teşhis : Risklerin tanımlanması ve/veya ölçümü için kullanılan araçlar.
- İzleme : Risklerin izlenmesi için kullanılan araçlar.
- Önleme : Risklerin azaltılması için kullanılan araçlar.
- Çözüm : Kesinleşmiş risklerin işaret edilmesi için kullanılan araçlar.

Yüksek ya da Orta Yüksek olarak nitelenen riskler, özellikle de kontrol alanındakiler için genellikle firmanız ya da bizim tarafımızdan alınacak azaltıcı önlemelere ihtiyaç vardır ve bu önlemler normal olarak önleyici ya da çözüm getirici araçların kullanımını içerir. Orta-Düşük riskler için düzenleyici eylemde izleme araçlarının kullanımını yer alabilir, örneğin özel bir riske ait herhangi bir değişikliğin izlenmesi amacı ile bilgilerin masa başında gözden geçirilmesi. Bir risk hakkında daha fazla bilgi edinmek için teşhis amaçlı araçlar kullanılacaktır. Düşük olarak nitelenen riskler genellikle daha ileri çalışmaları gerektirmeyecektir.

2.34. Yüksek etkili yetkili firmalar için risk profilindeki değişiklikleri tanımlamak için bize yardımcı olacak ilave bir risk azaltma programı unsuru olması muhtemeldir ki bu;

- iş birimleri içinde ortaya çıkan risklerin tanımlanmasına ve
- firmanızın üst düzey yönetim ve kontrol yapısına olan güvenimizin devam etmesine imkan verir.

Bunu yapmak için, kontrol yapısının temel özelliklerinin (özellikle risk yönetimi, uyum ve iç denetim) etkinliğini ölçmek için teşhise ve izlemeye dayalı araçlar kullanılacaktır. Bunlar aynı zamanda daha maddi ve/veya yüksek riskli olan iş birimlerinin risk profillerindeki değişikliklerden haberdar olmamıza yardımcı olacaktır.

2.35. Risk azaltma programı geliştirirken, özellikle de kaynakların etkin ve ekonomik kullanımını sağlamak için, iyi düzenleme prensiplerini unutmayız. Bunun anlamı programın genel maliyeti dikkate alınırken aynı zamanda özel konulara işaret etmek için en etkin araçların kullanılmasıdır. Maliyet konusunda, risk azaltma programının uygulanmasına ilişkin dahili maliyetlerimiz ve firmalar tarafından maruz kalınacak önemli harici maliyetler dikkate alınır.

2.36. Risk azaltma programının genel yoğunluğunun firmanızın hem etki hem olasılık açısından taşıdığı risklerle orantılı olmasını sağlamayı amaçlarız. Aynı zamanda çalışmalarımız daha çok iç fonksiyonlara (iç denetim ya da risk yönetimi gibi) dayandırılmakta, gerek ziyaretlerimiz gerek donanımlı personel kullanımı ve risk azaltma programının genel olarak yoğunluğu bakımından firmanıza ek yük getirilmesi ise daha az tercih konusudur.

3.37. Aynı zamanda tarafımızca düzenleyici bir süre de tespit edilecektir. Bu süre, resmi risk değerlendirmeleri arasındaki dönemdir ve aynı zamanda risk azaltma programının sürdüğü dönemdir.

Düzenleyici araçların seçimine örnekler

1. Bir sigorta firmasının iç denetim departmanına ait risk değerlendirmesi sürecinde; denetim evresinin son denetim ile iş yönetimlerinden gelen talepler arasında geçen zamana dayalı olduğunu saptadık. Denetim eylem noktalarını izlemek için somut hale getirilmiş bir süreç yoktur. Buradan hareketle tanımlanmış risk konusu; firmanın departmanlarına ait risk değerlendirmelerine dayalı bir risk tabanlı denetim planının olmaması ve eylem noktalarının izlenmesine ilişkin zayıf prosedürleri içermek üzere iç denetim prosedürlerindeki zayıflıktır. Yönetimin kendi başına bu risk konusunu işaret edip etmeyeceğine baktık, ancak zayıflığın yapısı ve iç denetimde başka zayıflıkları gösteren olasılık koşulu altında seçilen düzenleyici araç donanımlı bir personelden Finansal Hizmetler ve Piyasalar Kanunu (FSMA) bölüm 166' ya göre iç denetim metodolojilerinin ve prosedürlerinin değerlendirilmesine ilişkin bir raporlama istenmesiydi. Bunun, iç denetiminin etkin olmasını sağlamak üzere firmanın üst düzey yönetimince niyet edilen sonuca ulaşmak için gerekli olduğuna karar verdik.

2. Bir bağımsız finansal danışmalık zincirinin iç denetim departmanına yapılan bir risk değerlendirme ziyaretinde yapılan saptama; departmanın tepkisel çalışma üzerinde yoğunlaştığı ve etkin bir uyum izleme programı bulunmamasıydı. Bu olayda risk konusu ise firmanın uyuma ilişkin ortaya çıkan problemleri tanımlama zaafiyetiydi. Seçilen düzenleyici araç firmadan kapsamlı bir uyum izleme programı geliştirmesi, bize göndermesi ve uygulanmasının talep edilmesi ve ilerlemenin gözden geçirilmesi için altı ay sonrasında bir denetim ziyaretinin yapılması olmuştur. Bu eylem, firma üst yönetimince niyetlenen uyum işlevinin etkinliğini sağlama sonucuna ulaşmak üzere tasarlanmıştır.

d. Dahili onaylama

2.38. Risk değerlendirme sürecini tamamlandıktan sonra bir risk azaltma programı geliştirildiğinde sonuçları size göndermeden önce bir dahili onay çalışması yürütürüz.

2.39. Yüksek etki firmaları için onay süreci, ilgili müdürlük ya da en azından bir departman müdürü tarafından başkanlık edilen bir komitenin resmi incelemesinden oluşmaktadır. Düşük etki firmaları için onay çalışması ise en azından firma ile ilgili günlük sorumlulukları olmayan bir müdür tarafından izlenir ve bir komite tarafından denetlenir.

2.40. Bu inceleme;
- Özel bir firma için risk konuları ışığında denetim grubu için bir eleştiri mekanizması sağlar.
- Riske dair sektör karşılaştırmaları yapılmasına yardımcı olur.
- Bizim maliyetlerimiz ve firmanın yüklendiği önemli dış harcamalar dahil olmak üzere risk azaltma programının orantısal olup olmadığı kontrol edilir.
- Genel kaliteyi ve tutarlılık kontrolünü sağlar.

e. Değerlendirme sonuçlarının bir mektup ile firmanıza bildirilmesi

2.41. Dahili onaylamayı takiben değerlendirme sonuçlarımızı bir mektupla firmanıza bildiririz. Mektupta, tanımladığımız riskler ile firmanız ve bizim tarafımızdan bu konulara işaret etmek üzere alınacak önlemler ortaya koyan bir risk azaltma programı eşliğinde firmanızın risk vaziyetine ilişkin görüşümüzü beyan ederiz.

f. Değerlendirmenin devam etmesi ve risk eskalasyonuna (artışına) yanıt verme

2.42. Düzenleyici süre 12 aydan daha uzun olduğunda normal olarak ara risk değerlendirmesi yaparız. Bu genellikle bir denetçinin masa başı değerlendirmesidir ve tüm risk faktörlerinin, konula-

rının ve kullanılan düzenleyici araçların incelenmesini kapsar. Bundan sonra olasılık değerlendirmesi ve risk azaltma programındaki herhangi bir maddi değişiklik hakkında size bildirim yapılacaktır. Yüksek etkili firmalar için ara değerlendirme en az yılda bir kez yapılır. Diğer firmalar için düzenleyici süre normal olarak düzenleyici sürenin yarısı kadardır (24 aylık bir düzenleyici süre için 12 ay ya da 36 aylık düzenleyici süre için 18 ay gibi).

2.43. Firmanızı etkileyen özel gelişmelerin sonucu olarak risk değerlendirmesinin güncellenmesi ihtiyacı doğduğunda yeniden inceleme yapılır.

- Dış çevrede maddeten firmanızı etkileyen değişiklikler,
- Firmanızın faaliyetlerinde, stratejisinde, altyapısında ya da yönetiminde gerçekleşen ya da niyet edilen değişiklikler,
- Diğer tüm koşullar eşit tutulduğunda risk profilinde iyileşme sağlayacağı niyet edilen sonuçlara başarıyla ulaşılması.

Ek olarak, özel risk sorunlarına ilişkin düzenleyici araçların gözden geçirilmesi ihtiyacı olabilir, örneğin; aranan sonucu vermeyen bir aracın olması durumunda. Bu gibi durumlarda ve özel gelişmeler firmanızı ters yönde etkilediğinde yeniden gözden geçirme risk değerlendirmesi ve risk azaltma programında değişikliklerin yapılmasına yol açabilir. Bunlar ayrıca firmanıza bildirilecektir.

2.44. Tanımlanmış risklerin, diğer çözüm getirici araçların kullanılması ihtiyacını doğuracak noktaya kadar yükselmesi durumu söz konusu olabilir. Bu muhtemel olarak eşik koşullarının, tanımış kriterlerin, kuralların ya da diğer ilgili düzenlemelerin ihlal edildiği durumlarda gerçekleşir.

2.45. Düzenleyici süre boyunca risk azaltma programınızı izleyecek ve belirlenen zaman diliminde niyet edilen sonuçlara ulaşılması için program çerçevesinde alınan önlemleri takip edeceğiz.

3. Bir firma risk değerlendirme ve risk azaltma sürecinden neler beklemelidir?

Zaman çizelgesi

3.1. Şekil 1'de firmanız için risk değerlendirmesi ve risk azaltma işlevine ilişkin açıklayıcı bir zaman çizelgesi verilmektedir.

3.2. Bu aşamada risk değerlendirmesi tamamlandıktan sonra firmanıza nihai mektubun ne zaman gönderileceği gösterilmemiştir. Bunun nedeni ise halihazırda bir çok açıdan düzenleyici çalışmalarımız için hizmet seviyesi standartlarımız üzerinde çalışmamızdır; 2002-2003 Yıllık Raporumuzda detaylar yer almaktadır.

Grup konuları

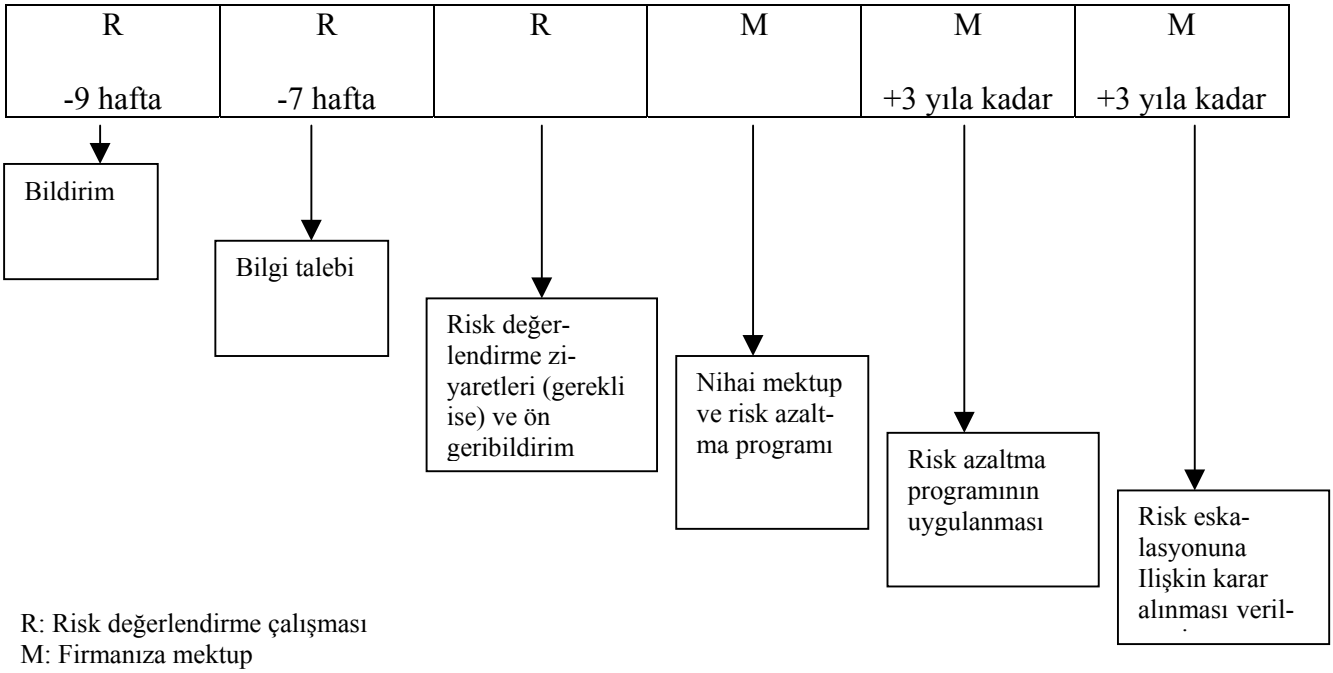
3.3. Düzenleyici sorumluluğun gruplara (bir dizi firmadan oluşan) aktarılmasının yöntemi; bir grubun, FSA'nın bir departmanı ile aynı anda ya da ayrı olarak yürütülen fakat farklı FSA departmanlarının koordineli risk değerlendirme çalışmasından oluşan müşterek bir risk değerlendirmesinin olup olmamasını etkiler. Buna ilişkin açıklama şöyledir:

- Bir sektördeki firmalardan oluşan gruplar (örneğin; genel sigorta ve hayat sigortası alanındaki yetkili firmalardan oluşan bir grup) normal olarak FSA'nın söz konusu sektörden sorumlu departmanın yönetiminde olacaktır. Tüm firmaları kapsayan bir müşterek risk değerlendirme ve risk azaltma programı ancak grubun birleşik bir yönetim ve/veya kontrol yapısı olduğuna karar vermemiz durumunda sürdürülecektir. Grup bu şekilde birleşmemiş ise daha bağımsız bir şekilde yönetilen ya da kontrol edilen bölümler üzerinde birebir değerlendirmelerimizi sürdüreceğiz.

- Farklı sektörlerdeki firmalardan oluşan gruplar, faaliyet alanları, yürüttükleri risk değerlendirme ve risk azaltma programlarına bağlı olarak farklı FSA departmanlarının (Sigorta Firmaları Yatırım Firmaları Departmanları gibi) çeşitli firmaları denetlediği "kılavuz denetim modeli" kullanılarak yönetilecektir. Ancak, sektör alanlarından birisi, grup bazında sorunlar için tek bir iletişim noktası olacak olan ve grup bazında risk incelemesi ve bireysel risk azaltma programlarının koordinasyonunu geliştirecek olan kılavuz denetçi olarak hareket edecektir. Bu durumda farklı firmalara ilişkin risk değerlendirmeleri farklı zamanlarda yapılabilir.

- Bazı gruplar ise grup denetimi modelinde yönetilecektir. Burada çoklu disiplinli bir takım, tek bir grup denetçisi sorumluluğu altında grup (örneğin menkul kıymetler, bankacılık ve aktif yönetimi faaliyetleriyle uğraşan firmalardan oluşan grup) içindeki tüm düzenlemeye tabi firmaları düzenleyecektir. Bu model ancak çeşitli kriterler (ölçek, karmaşıklık, faaliyet yelpazesi, yönetim ve kontrol yapılarındaki birleşmenin düzeyi dahil olmak üzere) karşılandığında kullanılacaktır. Bu modelde grup içinde yer alan tüm firmaları kapsamak üzere müşterek risk değerlendirme ve risk azaltma programı yürütülecektir.

Şekil 1: Risk değerlendirme aşamaları ve firmanız için gösterge zaman çizelgesi



R: Risk değerlendirme çalışması
M: Firmanıza mektup

Bildirim ve bilgi talebi

3.4. Bu raporun daha önceki bölümlerinde belirtildiği üzere firmanız için risk değerlendirme süreci tarafımızca gönderilen bildirimle başlamaktadır. Bundan sonra masa başı değerlendirme çalışmasını başlatacağız. Zaman zaman ön çalışmayla aynı zamanda yapılmakla birlikte risk değerlendirme çalışması için talep edilen ek bilgiye ilişkin detayları vereceğiz. Aynı zamanda daha fazla bilgi edinmek amacıyla yerinde risk değerlendirme ziyaretlerine ihtiyaç duyulması halinde bunu da firmanıza bildireceğiz.

3.5. Elbette elimizde olan bilgileri talep etmeyeceğiz ancak ihtiyaç duyacağımız türdeki bilgilere ilişkin bazı örnekler şunlar olabilir:

- Güncel iş birimleri, yasal yapı ve yönetim yapısına ilişkin grafikler,
- Temel komitelere ilişkin referans kavramlar-örneğin yönetim kurulu ya da komite tutanaklarına örnekler, ancak rutin olarak olmamak üzere.
- Mevcut strateji dokümanları,
- Yönetim hesapları,
- Risk raporları (uygun kredi, piyasa, faaliyet ve sigorta riskleri dahil olmak üzere)
- Uyum raporları,
- Karaparanın aklanmasının önlenmesi çerçevesinde raporlar,
- İç denetim planı ve metodolojisi- İç denetimin niteliği ve kapsamını değerlendirmek amacıyla iç denetim raporları ve denetim komitesi tutanaklarına örnek talep edebiliriz, ancak rutin olarak tüm iç denetim raporlarını talep etmeyeceğiz.
- Dış denetim yönetiminden mektup.

Risk değerlendirme ziyaretleri

3.6. Firmanızın risk haritasını tamamlamamıza yardımcı olacak daha fazla bilgiyi sağlamak için risk değerlendirme ziyaretleri yapabiliriz. Diğer bir ifadeyle, firmanızın iş ve kontrol yapısı hedeflerimize yönelik maddi riskler ortaya çıkarıyorsa bunları tanımlamak için bu ziyaretlerden faydalanırız. Değerlendirmeyi tamamlamak için yeterli bilgiye sahip olmamız durumunda bu ziyaretleri yapmayabiliriz.

3.7. Yerinde risk değerlendirme ziyaretleri aşağıdakilerden herhangi birisini kapsayabilir:

- Tarafımıza düzenli gönderilen bilgiler de dahil olmak üzere elimizde halihazırda bulunan bilgilerdeki bilgi açıklarının kapanması (örneğin; geribildirimler, şikayet bilgileri), önceki risk değerlendirmeleri, özel alanlara ilişkin incelemeler ve firmanızın sağladığı paragraf 3.5'de bahsedilen bilgiler.
- Önceki çalışma ya da bilgilere dayandırılarak tanımlanan konuların takibi.
- Firmanızın kontrol yapısı hakkında çeşitli yönlerine ilişkin görüşlerimizi çeşitlendirmek üzere bazı kontrollerin gözden geçirilmesi.

3.8. Bu ziyaretler firmanızın kilit noktalarındaki kişilerle görüşmeleri da kapsamaktadır. Görüşmeyi tahmin ettiğimiz kişi sayısı ve tüm yerinde ziyaretlerin toplamı için geçirilecek süre firmanızın ölçeğine, faaliyet alanına ve ön çalışmamızda tanımladığımız konulara bağlı olarak değişebilir. Ancak, görüşme yapmak isteyeceğimiz kişiler (muhtemelen kilit kontrol noktalarındaki onaylanmış kişileri kapsayacak, ancak bununla sınırlı kalmayacaktır) için örnekler Şekil 2'de belirtilmektedir; burada bazı firmalarda tek bir kişinin tanımlanmış fonksiyonların birden fazlası için çalıştığı kabul edilmektedir. Ayrıca, Şekil 3'de söz konusu kişilerle yapılacak görüşmenin kapsayacağı temel risk grupları da belirtilmektedir (bunlar sadece örnek teşkil etmesi amacıyla verilmiştir).

3.9. Firmanızın denetim konusunda iletişim kurulan firma yöneticileri (iletişim müdürleri) normal olarak risk değerlendirme ziyaretlerini de yürütecektir. Çalışma ekibine, özel uzmanlık gerektiren konular olması durumunda, uzman personel tarafından destek verilecektir; örneğin Risk İnceleme Departmanı uzmanlarımız, kredi türevleri ile ilgili işlerin içerdiği riskleri müzakere edeceklerdir.
.

Şekil 2: Risk değerlendirme ziyaretlerinde görüşme yapılacak kişilere ve tartışılacak risk gruplarına örnekler

	Strateji	Piyasa, kredi, sigorta ve faaliyet riskleri	Finansal yapının sağlığı	Müşteri /kullanıcı ve ürün/hizmet özellikleri	Müşteri/ kullanıcı yönetimi	Organizasyon	Dahili sistemler ve kontroller	Yönetim kurulu, yönetim ve personel	İş ve uyum kültürü
Başkan	➨						➨	➨	➨
Baş yönetici	➨						➨	➨	➨
Denetim komitesi başkanı							➨		➨
İdari olmayan müdür	➨					➨	➨	➨	➨
Baş finansal yönetici		➨	➨			➨	➨		➨
Risk yönetimi müdürü		➨					➨		➨
İş birimi müdürü	➨	➨			➨		➨	➨	➨
Baş yatırım yöneticisi	➨	➨		➨	➨		➨	➨	➨
İç denetim müdürü				➨			➨		➨
Baş aktüer		➨			➨		➨		➨
Uyum müdürü					➨	➨	➨		➨
Operasyon müdürü							➨		➨
Bilgi işlem müdürü				➨			➨		➨
İnsan kaynakları müdürü					➨			➨	➨
Düzenleme müdürü (yetkili organ)	➨	➨			➨		➨	➨	➨

Risk değerlendirme ziyaretlerine örnek

1. Bilgi eksiklikleri: Bir yatırım bankasının kredi türevlerinin alım-satımı olmak üzere kendine yeni bir iş alanı kurduğunu biliyoruz. Ancak firmanın risk değerlendirmesi sürerken, firmanın söz konusu yeni faaliyetleri hakkında çok az bilgimiz bulunmaktaydı. Bu nedenle ilgili faaliyet alanındaki firma yetkilisine bir risk değerlendirme ziyareti yapılmasına karar verdik. Ziyaret süresince, iş alanıyla ilgili planlar, karşı tarafların seçimi, ön ofis kontrolleri ve risk alma istekliliği ele alınacaktır. Aynı zamanda risk kontrolleri hakkında kredi ve piyasa riski yöneticilerinden ve sistem konularına ilişkin bilgi işlem yöneticisinden, teminat yönetimine ilişkin operasyon yöneticisinden ve belgeleme konularında uyum yetkilisinden bilgi alınır. Aynı zamanda bu yeni iş alanının firmanın genel stratejisi ile uyumu konusu da üst düzey yönetim ile müzakere edilecektir.

2. Özel konuların takibi: Bir menkul kıymetler şirketinde risk yönetimi fonksiyonu hakkındaki önceki çalışmalarda kredi riskine yönelik stres testleri ve senaryo analizinde zayıflıklar olduğu ve firmanın yönetim komitesinin bu konuda bir eleştirisi/açıklama beklentisi olmadığı belirlenmiştir. Bu konuyu takip etmek amacıyla prosedürlerde iyileştirme sağlanması için risk yönetimi yöneticisine bir risk değerlendirme ziyareti yapılmasına karar verilmiştir. Yönetim komitesinin diğer üyeleri ile eleştiri yapılmasında etkinliğin düzeyinin ne olması gerektiği müzakere edilmiştir.

3. Kontrollerin sınırlı düzeyde incelemesi: Bir süre önce firmanın karaparanın aklanmasının önlenmesi konusundaki sorumlu yetkili raporlarında, ilgili konuda emsal grup ile mutabık kalınmadığının farkına varılmıştır. Risk değerlendirme ziyaretimiz sırasında bu alandaki firma kontrollerine ilişkin sınırlı sayıda inceleme yapılmasına; bu amaçla karaparanın aklanmasının önlenmesinden sorumlu yetkiliye sunulan dahili raporlardan bir örnek incelenmesine ve şüpheli işlem raporlarına ilişkin personelin eğitim kayıtlarının incelenmesine karar verilmiştir.

Ön geribildirim

3.10. Ön geribildirimin amacı, firmanız için risk azaltma programı oluşturmadan önce risk değerlendirmesiyle ilgili önemli bulguları sizinle paylaşmaktır. Bu ön geribildirim genellikle sizinle yapacağımız bir toplantı şeklinde olacaktır ve yerinde risk değerlendirme çalışmasının tamamlanmasını takiben yapılacaktır. Ne var ki, önemli bulgulara ilişkin sonuçlarımızı oluşturmak amacıyla zamana ihtiyaç duyacak olmamız durumunda ön geribildirim toplantısı daha ileri bir zamanda da yapılabilir

3.11. Ön geribildirim toplantıları her durumda yapılmayabilir. Risk değerlendirme süresinde sadece önemli birkaç sorunun ortaya çıktığı durumlarda ya da önemli sorunların olması durumunda bulgularımızı size bildirmeden önce konunun daha resmi olarak ele alınmasının gerektiği durumlarda ya da sorunların başka yollarla ele alındığı (telefon görüşmesi gibi) durumlarda söz konusu ön geribildirim toplantıları yapılmayabilir.

3.12.Ön geribildirim toplantılarının maddi hatalar sonucu yapılan yorumların tartışılmasından ziyade firmanızın bu maddi hataları düzeltmesine olanak vereceği hususu önem taşımaktadır. Söz konusu toplantıyı takiben geliştireceğimiz risk azaltma programındaki konuların temelini oluşturan bazı olguları denetlemek isteyebiliriz.

3.13. Yerinde çalışmanın sonuna doğru bir ön geribildirim toplantısı olup olmayacağı, eğer olacak ise yerinde çalışmanın sonunda mı yoksa daha ileri bir tarihte mi yapılacağı konusu açıklanacaktır.

Nihai mektup ve risk azaltma programı

3.14. Bu rapordaki 2.38, 2.39, 2.40'ıncı paragraflarda tanımlandığı üzere risk değerlendirme sonuçları ve risk azaltma programı resmi bir mektup ile firmanıza bildirilmeden önce dahili bir incelemeye tabi olacaktır. Bu iletişim süreci 2 bölümden oluşmaktadır:

- Nihai mektupta şu hususlar belirtilmektedir;
  - Her bir yasal hedef karşısında firmanızın etki ve olasılılık dereceleri,
  - Firmanızın karşı karşıya bulunduğu temel çevresel ya da harici riskler hakkındaki görüşlerimiz; uygun olması durumunda bu görüşler firma bazlı özel sorunlara ilişkin kapsam ve koşulların oluşturulmasını sağlayacaktır.
  - Yüksek ya da Orta Yüksek olasılık derecelerine yol açan temel bulgular,
  - Risk azaltma programının temek noktaları,
  - Düzenleyici sürenin uzunluğu.

- Risk azaltma programında şu hususlar belirlenmektedir;
  - Tarafımızca tanımlanan sorunlar ve bunlarla ilgili yetkili firmalar,
  - Her bir sorun ile ilgili olarak aradığımız sonuçlar,
  - Beklenen sonuca ulaşmak için alınacak önlemler, bu önlemlerin kim tarafından alınacağı (firmanız ya da FSA),
  - Önlemlere ilişkin zaman çizelgesi.

Risk azaltma programına yönelik bir örnek Ek 6'da yer almaktadır.

3.15. Firmanız için düzenlenen mektup yönetim kurulu ya da eşdeğeri bir organa gönderilecektir. Bunun nedeni etkin iç kontrollerin oluşturulması ve sürdürülmesi ile firmanız faaliyetlerinin düzenleyici yükümlülüklere uygun olarak sürdürülmesinde üst düzey yönetimin taşıdığı sorumluluğa verdiğimiz önemi belirtmektir. Bu yaklaşıma paralel olarak beklenen özel sonuçlara ulaşılması amacıyla bizim yerimize firmanız tarafından alınacak önlemler için risk azaltma programlarında ve söz konusu önlemlerin alınmasını temin etmekle sorumlu üst yönetimde bir taraflılık olacaktır. Ayrıca, mektubun bir kopyası firmanızda iletişim kurduğumuz anahtar noktalardaki kişi veya kişilere gönderilecektir.

3.16. Firmanızın, sınır ötesi faaliyet gösteren bir kuruluşun bir şubesi ya da iştiraki olması durumunda risk değerlendirme mektubu ve risk azaltma programı aşağıdaki şekilde gönderilecektir:

- Firmanız, Avrupa Ekonomik Alanındaki bir ülkeden pasaport girişi olan bir şirketse risk değerlendirme mektubu, firmanızın genel merkezindeki İngiltere şubesinden sorumlu kişiye de dikkatini çekmek üzere gönderilecek bir kopyayla beraber firmanın İngiltere'deki Genel Müdürüne ya da muadiline gönderilir.
- Firmanız, Avrupa Ekonomik Alanında olmayan bir ülkeden pasaport girişi olan bir şirketse risk değerlendirme mektubu, firmanızın İngiltere'deki genel müdür ya da muadiline dikkatini çekmek üzere gönderilecek bir kopyayla beraber firmanın genel merkezindeki İngiltere şubesinden sorumlu kişiye gönderilir.
- Firmanız bir şube ya da iştirak ise mektubun bir kopyası merkezin bulunduğu ülke ya da konsolide denetim otoritesine gönderilir.

3.17. Taslak mektuplar yetkili firmalar için kullanılmayacaktır. Bunun nedeni firmanızın taşıdığı risklere ilişkin görüşümüzde olduğu gibi nihai mektubun müzakere edilmesi uygulamamız bulunmamaktadır. Durumlara ilişkin sorunlarda önemli değişiklikler olması durumunda beklentimiz bunların, ön geribildirimde ya da risk azaltma programı geliştirirken sorunlara neden olan temel faktörleri kontrol amaçlı çalışmalarımız sırasında çözülmüş olmasıdır. Ne var ki firmanız istediğimiz sonuçlara ulaşılması için bize alternatif araçlar önerebilir ve bu araçların daha etkin ya da verimli olduğuna karar vermemiz durumunda risk azaltma programını iptal edebiliriz.

3.18. Firmanızdan, nihai mektubu risk azaltma programının takip edeceğini teyit eden resmi bir yanıt isteriz. Mektup firmanız adına gizlidir ancak firmanızın profesyonel danışmanlarına (denetçiler ve aktüerler) bir kopyasının gönderilmesini isteyebiliriz.

3.19. Firmanız, olaylara dayanan hatalarla ilgili düşüncelerimizi ya da paragraf 3.17'de tartışılan konuları takiben risk azaltma programında hala çözümlenmemiş olayları de içermek üzere risk değerlendirme bulgularına ihtilaf etmek isterse resmi olarak bunu denetçinizle (supervisor) görüşmeniz gerekmektedir. Denetçi ihtilaf bulunan konulara ilişkin olarak firmanızı yanıtlayacaktır. Firmanız, denetçinin gerçekçi yanıtlar vermediğini düşünürse ilk merci olarak denetçinin yöneticisi ya da departman müdürü ile iletişim kurmalısınız.

3.20. Firmanız risk azaltma programındaki çalışmaların gerçekleştirilmesinden uzaklaşırsa diğer düzenleyici araçların (örneğin yetkili bir firma bölüm 166' ya bir uzman raporunun talep edilmesi ya da Finansal Hizmetler ve Piyasalar Kanunu bölüm 165'e göre resmi bilgi talep edilmesi) kullanımını dikkate alırız. Eğer sorunun halihazırda işaret edilmediğini düşünürsek firmanızın herhangi bir kuralı ya da eşik koşulunu (yetkili organlar için yetki koşulu) ihlal edip etmediğini ya da diğer formal çalışmanın yapılıp yapılmadığını (örneğin, yetkili firmalar için icra/uygulama eyleminin kullanılması) dikkate alırız. Formal çalışmanın yapılmasına, içinde temyiz mekanizmalarının da yer aldığı olağan karar alma sürecimiz kullanılarak karar verilecektir.

Risk azaltma programının uygulanması

3.21. Risk azaltma programı, düzenleyici süre olarak tanımladığımız bir zaman çizelgesine göre uygulanacaktır. Bu süre resmi risk değerlendirmeleri arasında bir zaman dilimidir ve tam süresi firmanızın taşıdığı risklere bağlı olmakla birlikte 12-36 ay arasında değişmektedir. Örneğin; düşük ve orta düşük olasılık derecesindeki firmalar için düzenleyici süre normal olarak 24-36 aydır, yüksek ve orta yüksek olasılık dereceli firmalar için ise bu süre 12-24 aydır.

3.22. Düzenleyici süre içinde, firmanız yatay ve konusuna göre yapacağımız çalışmaya tabi olabilir. Buna neden olan sorunlara aşağıda değinilmiştir;

- Birçok firmayı etkileyen ve tek bir firmanın risk azaltması yerine bir dizi firma karşısında yatay olarak riskin azaltılmasına işaret edilen bir sorun; öyle ki bu sorun özel bir firmanın risk azaltma programında yer alan ve akabinde yatay olarak işaret edilmesi gerektiğine karar verilen ya da o firmaya özel risk azaltma programında tanımlanmayıp diğer firmalar ile çalışılırken tanımlanmış olabilir.
- Firmaya özel değil de bir tüketici, bir ürün ya da bir piyasayla ilgili olan, ancak riski değerlendirmek ve düzenleyici cevabımıza karar vermek için tüm firmalara yönelik bir çalışma yapmamız gerektiren bir sorun.

3.23. Böyle bir çalışmayı yaparken, firmanızın risk azaltma programında yer alan firmanıza özel çalışmayla da eşgüdüm sağlama gayreti içinde olacağız.

Kesintisiz değerlendirme ve risk değişikliğine yanıt

3.24. Paragraf 2.42'de açılandığı üzere düzenleyici süre 12 aydan daha uzun ise firmanıza yönelik bir geçici inceleme yürütürüz. Bu inceleme masa başı değerlendirmeyi içermektedir ve olasılık değerlendirmesindeki her türlü maddi değişikliği ya da düzenleyici süreyi hatırlatmak üzere risk azaltma programı firmanıza bildirilecektir.

3.25. Her zaman firmanızdan risk değerlendirmemizi etkileyecek türden olayları bize bildirmesini bekleriz. Gerçekte, firmanızın gelişmeler hakkında bizi bilgilendirme konusundaki yaklaşımı ve performansı ileride risk değerlendirmemizde mümkün olduğunca dikkate alınacaktır. Bu olaylar ayrı bir kitapçıkta tanımlanmakla birlikte aşağıda da birkaç örnek verilmiştir.

- Firmanızın çalışanlarından birinin bir müşterinize karşı hileli bir eylem gerçekleştirdiğinin farkında olunması,
- Firmanızın sistemleri veya kontrollerinde herhangi önemli bir bozukluğun olması,
- Firmanızın yeni bir ürün ya da hizmet sunumuna başlaması,
- Önemli bir kural ihlali olması.

3.26. Bu olaylar risk değerlendirmemizi güncelleştirmemize yol açabilir. Risk değerlendirmemizi diğer faktörlere bağlı olarak da değiştirebiliriz, örneğin firmanızın faaliyet gösterdiği çevre koşullarında değişiklik olması ya da bir çok firma üzerinde yürütülen yatay çalışmanın sonucu olarak bu güncellemeyi yapabiliriz. Benzer durumlarda, risk azaltma programında herhangi bir maddi düzeltme yapılmasına ilişkin size bir açıklama göndermeden önce risk değerlendirmesine konu değişiklikleri önce sizinle tartışırız.

Risk eskalasyonuna örnek

Kurumsal ve perakende piyasalara aktif yönetimi alanında hizmet vermek üzere faaliyet gösteren bir firma 4 yasal hedefimiz dikkate alındığında orta yüksek etki ve orta düşük olasılık derecesinde değerlendirilmiş ve 2 yıllık düzenleme süreci verilmiştir. Bu düzenleyici süreye 9 ay kala firma uyum yönünden zayıf olduğuna dair bir geçmiş bilginin bulunduğu büyük rakiplerinden biriyle birleşerek perakende piyasasındaki faaliyetlerini genişletmeyi planladığını bildirmiştir. Firmanın genişleme planları, birleşme olacak şirketin faaliyetlerinin kendi IT perakende platformuna kaydırılmasını içermektedir. Bu durum muhtemelen firmanın kapasitesini genişletecek ve firmaların birleşen geri ofislerinde önemli maliyet tasarrufu sağlanacak, yeni yönetim grubu her iki firmanın temsilcilerinden oluşacaktır.

Bu birleşme için gerekli olan kontrol uygulamaları sürecindeki değişikliğe paralel olarak biz de risk değerlendirmemizi güncelleştirmek durumunda kalacağız. Sonuç olarak, piyasa güveni ve müşteri korunması için olasılık derecelerinin, IT ve geri ofislerin birleştirilmesine bağlı olacak artacak riskler ve birleştirilen şirket yapısında kontrollerin nasıl etkin olarak uygulanabileceğine dair belirsizlikler nedeniyle orta düşükten orta yükseğe değiştirilmesi gerekmektedir. Risk azaltma programı revize edilerek firmaya gönderilecek ve ekinde IT ve geri ofislerin birleşmesine dair detaylı bir planın eklenmesi ve bu plana ilişkin gelişmelerin tarafımıza düzenli olarak rapor edilmesi istenecek, ayrıca firmanın iç denetim fonksiyonundan yüksek düzeydeki kontrollere ilişkin düzenlemelerin yeterliliği konusunda bir rapor talep edilecektir.

4. Firmalarca sıkça sorulan sorular

Soru	İlgili paragraf
1. Risk değerlendirme çerçevesinin amacı nedir?	Giriş 4
2. Risk değerlendirme çerçevesinin önemi nedir?	Giriş 6
3. FSA'ya göre risk ne anlama gelir?	1.2
4. Etki ve olasılık ne anlama gelir?	1.2
5. Hangi firmalar risk değerlendirme çerçevesini uygular?	2.5
6. Risk değerlendirme çerçevesinin genel yapısı ve öngördüğü zaman çizelgesi nasıldır)	Paragraf 2.1-Şekil 2
7. FSA, firmamız üzerinde risk değerlendirme çerçevesi uygulayacağını ne zaman bildirir?	3.3
8. FSA faaliyette bulunduğumuz dış çevreyi nasıl dikkate almaktadır?	2.18-2.19
9. FSA riskleri nasıl tanımlamaktadır?	2.20-2.25
10. Risk değerlendirmesinin bir parçası olarak FSA firmalardan bilgi ister mi?	3.4
11. Risk değerlendirme sürecinde FSA firmada çalışan kişileri ziyaret eder mi? Eğer öyleyse kimleri?	3.6- 3.8-Şekil 3
12. Söz konusu ziyaretlere FSA'dan kim katılmaktadır)	3.9
13. Bu ziyaretlerde FSA neyi araştıracaktır)	3.7
14. Bir firma birçok birimden oluşmakta ise FSA bunu ne şekilde dikkate alacaktır?	2.6-2.10
15. Bir çok yetkili firmadan oluşan bir grup olmamız durumunda FSA bu yapıyı nasıl dikkate alacaktır?	2.6,-2.10-3.3
16. Sınır ötesi bir organizasyonun bir parçası olmamız durumundaki özel sorunlar nelerdir?	2.11-2.14
17. Risk değerlendirme sonuçlandırılmadan önce FSA'dan herhangi bir geri bildirim olabilir mi?	3.10-3.13
18. FSA risk değerlendirme işlevinde yaklaşımında tutarlılığı nasıl sağlar?	2.38.2.40
19. FSA risk değerlendirme sonuçlarını nasıl iletir?	3.14
20. Risk değerlendirmesi sonuçlarını bildiren nihai mektubun taslak halini görebilir miyiz?	3.17

21. Mektupta etki ve olasılık dereceleri nasıl kullanılmıştır ?	2.26-2.30
22. Risk azaltma programı nedir?	2.31.2.34
23. Risk azaltma programında niyet edilen çıktı (sonuç) ile ne anlatılmaktadır)	2.31
24. Düzenleyici dönem nedir?	2.37-3.21
25. Risk azaltma programının uygulanmasında FSA maliyetlerimiz dikkate alacak mı?	2.35-2.36
26. Sonuç mektubu kime gönderilecek? Mektubun kopyası başka kime gönderilecek?	3.15-3.16
27. Mektup denetçilerimize ve diğer profesyonel danışmanlarımıza gönderilecek mi?	3.18
28. Risk yönetim programı uyguladığımızı teyit etmeli miyiz?	3.18
29. Mektubun içeri ve risk azaltma programını sorgulayabilir miyiz?	3.17-3.19
30. FSA mektubun sonuçlarını takip edecek mi?	2.45
31. FSA tarafından yapılan herhangi bir karşı firma çalışması risk azaltma programımızdaki çalışmayla etkileşim içinde olur mu?	3.22-3.23
32. Risk azaltma programında öngörülen önlemleri almazsak sonucu ne olur?	3.20
33. FSA gelecek resmi değerlendirme tarihinden önce risk değerlendirmesini güncelleyecek mi?	2.42-3.24
34. Gelecek değerlendirme öncesinde risklerimiz değişir ise ne olacak?	2.43-2.44-3.26
35. Mektup sonrasında FSA'yı gelişmelerden haberdar etmek için neler yapmalıyız?	3.25

Ek 1:

Yasal Hedefler, Hedeflere Yönelik Riskler" (RTO's), Hedeflere Yönelik Risk Grupları (RTO groups)

Risk çizelgesinde, değerlendirmekte olunan firmalara yönelik *yasal risklerin*, *hedeflere yönelik riskler* içindeki temel risklerden oluştuğu ve yasal hedeflerimizle ne şekilde ilişkili olduğu görülmektedir.

Çizelgede 15 adet *hedeflere yönelik risk* tanımlanmıştır; bunların 13'ü belirli yapıdaki firmaların risklerinin değerlendirilmesine ilişkindir, diğerleri (5 ve 6) ise firmaya özel olmayıp, tüketici/ürün/işkoluna (sanayi) ilişkin riskleri göstermektedir.

Olasılık değerlendirmesi, çizelgede yer alan 7 yasal riske *(hedeflere yönelik risk grupları*) karşılık bir risk unsuru taşıyan bir firmanın ticari riskleri ile denetim risklerinin belirlenmesi ve derecelendirilmesini içermektedir.

Yasal Hedefler	**Piyasaya Güveni Sarsan Unsurlar**				**Kamu Bilinci**	**Tüketicinin Korunması**					**Finansal Suçlar**		
Hedeflere Yönelik Riskler	Yayılma özelliği ya da paralel özellikler gösteren finansal başarısızlıklar	Yaygın biçimde firmaların yanlış davranışlarda bulunmaları ya da yanlış yönetilmeleri	Finansal suçlar	Piyasanın çalışamaması	Tüketicilerin özel ürün ya da hizmetlere dair yeterli bilgi sahibi olmaması bilgiye dayalı karar vermenin önünde bir engel oluşturur. (finansal kazanç ya da kayıp üzerindeki doğrudan ya da çabuk etkileri hesaba katılmaksızın	Yayılma özelliği ya da paralel özellikler gösteren finansal başarısızlıktan kaynaklanan fırsat kaybı da dahil tüketici zararları	Firmaların yanlış davranışlarda bulunmaları ya da yanlış yönetilmelerinden kaynaklanan fırsat kaybı da dahil mevcut ve geçmiş alımlara dair tüketici zararları	Piyasanın kötüye kullanımından kaynaklanan fırsat kaybı da dahil mevcut ve geçmiş alımlara dair tüketici zararları	Piyasanın çalışamamasından kaynaklanan fırsat kaybı da dahil mevcut ve geçmiş alımlara dair tüketici zararları	Tüketicilerin özel ürün ya da hizmetlere dair yeterli bilgi sahibi olmamasından kaynaklanan fırsat kaybı da dahil mevcut ve geçmiş alımlara dair tüketici zararları	Hile ve sahtekarlık tekrar etme oranı (doğrudan kayıplara yol açan sonuçları hesap edilmeksizin)	Yanlış yönetim ya da finansal piyasalara ilişkin bilginin yanlış kullanımının tekrar etme oranı (doğrudan kayıplara yol açan sonuçları hesap edilmeksizin)	Suç işlenmesine dair usullerin ele alınmasının tekrar etme oranı (doğrudan kayıplara yol açan sonuçları hesap edilmeksizin)

Hedeflere Yönelik Risk Grupları	Finansal Başarısızlık	Yanlış Davranış/ Kötü Yönetim	Karapara Aklanması	Piyasa Kalitesi	Tüketici Bilinci	Finansal Başarısızlık	Yanlış Davranış/ Kötü Yönetim	Piyasanın Kötü Kullanımı	Piyasa Kalitesi	Tüketici Bilinci	Hile ya da Sahtekarlık	Piyasanın Kötü Kullanımı	Karapara Aklanması

Piyasanın Kötü Kullanımı
Hile ya da Sahtekarlık

Hedeflere Yönelik Risk Grupları

Finansal Başarısızlık	Yanlış Davranış/ Kötü Yönetim	Piyasa Kalitesi	Tüketici Bilinci	Hile ya da Sahtekarlık	Piyasanın Kötü Kullanımı	Karapara Aklanması

Ek 2:
Etki Sınırları

Aşağıda yer alan etki dereceleri farklı kategorilerdeki firmalara ilişkin örnek göstergelerdir.

Banka ve yapı kooperatifleri		Kredi birlikleri	Hayat sigortası ve yardım vakıfları	Yardım vakıfları	Genel konular	Acenta olarak danışma, düzenleme ve muamele						
						Öz varlıklar ve türev ürünler				Emekli fonları ve diğer finansal ürünler	Yatırım yönetimi firmaları	
T. aktifler/ T. yükümlülükler (milyon£)	Sektör ağırlıklı mevduat (milyon£)	Üye sayısı	T. aktifler/ T. yükümlülükler (milyon£)	Üye sayısı	Brüt prim geliri (milyon£)	T. aktif./ T. yüküm. (milyon£)	Finansal kaynak gerekleri (milyon£)	Günlük ticaret hacmi (milyon£)	Günlük ticaret hacmi (milyon£)	Yıllık ciro	Yönetimdeki fonlar (milyon£)	***Etki aralıkları***
18.000	6.500		36.000	2.000.000	2.000	36.000	750	25.000	15.000	250	80.000	***Y/OY***
1.800	650		3.600	200.000	200	3.600	75	2.500	1.500	25	8.000	***OY/OD***
90	32,5	5.000	180	10.000	10	180	5	125	75	1,25	400	***OD/D***

Not:

Etki dereceleri; yüksek (Y), orta-yüksek (OY), orta-düşük(OD), düşük(D).

Ek 3:
Risk Unsurları

İçerik

Risk Grubu: Strateji (İş Riski)

1. Stratejinin niteliği
2. Ticari yapı

Risk Grubu: Piyasa, Kredi ve Faaliyet Riski (İş Riski)

3. Kredi riski
4. Sigorta riski
5. Piyasa riski
6. Faaliyet riski
7. Yasal risk

Risk Grubu: Finansal Sağlamlık (İş Riski)

8. Sermaye yeterliliği
9. Likidite
10. Kar

Risk Grubu: Müşteri/Kullanıcı/Ürün ve Hizmet Yapısı (İş Riski)

11. Müşteri/ kullanıcı/üye çeşidi
12. Kaynak ve dağıtım kanalları
13. Ürün/hizmet çeşidi
14. Piyasa verimliliği
15. Uygun piyasalar

Risk Grubu: Müşteri/Kullanıcıya Yönelik Davranışlar (Kontrol riski)

16. Satış esasına dayalı personel eğitimi ve istihdamı
17. Satış esasına dayalı personel ücretleri
18. Finansal promosyonlar (teşvikler)
19. Müşteri/kullanıcı/üyelere yönelik kabul, danışmanlık ve raporlama
20. Muamele ve yönetim
21. Müşteri/kullanıcı/üye aktiflerinin korunması
22. Kamuoyunun bilgilendirilmesi/ürün literatürünün yeterliliği
23. Üyelik düzenlemeleri

Risk Grubu: Organizasyon (Kontrol riski)

24. Yasal yapı/Mülkiyet yapısının beyanı
25. Denetçiler/Grup şirketlerinin özellikleri/yetkileri
26. Grubun geriye kalanıyla ilişkiler

Risk Grubu: Dahili Sistemler ve Kontroller (Kontrol riski)

27. Risk yönetimi
28. Politika, prosedür ve kontroller

29. Yönetime bilgi
30. Enformasyon teknolojisi sistemleri (IT)
31. Finansal ve yasal raporlama ve muhasebe politikaları
32. Uyum
33. İç denetim
34. Dış kaynak kullanımı (outsourcing)
35. Profesyonel danışmanlık
36. Ticari devamlılık
37. Karapara aklanmasının önlenmesi ile ilgili kontroller
38. Piyasanın temizliği ve düzgünlüğü
39. Takas ve saklama düzenlemeleri

Risk Grup: Yönetim Kurulu, Üst Yönetim ve Personel (Kontrol riski)

40. Şirket yönetimi
41. Yönetim sorunluluklarının tanımlanması ve dağılımı
42. Yönetim kalitesi
43. İnsan kaynakları

Risk Grup: Ticari Kültür (Kontrol riski)

44. Düzenleyicilerle ilişkiler
45. Kurum kültürüne ilişkin konular ve iş ahlakı

Not:
Her bir risk unsurunun altında kısa tanımlamalar yer almıştır. Ek 1'de gösterilen 7 adet yasal riske karşılık gelen risklere ilişkin konulara bakılacaktır. Böylece yasal hedeflerimize yönelik bir risk taşıyan konuların belirlenmesi sağlanacaktır.

Sadece yetkili kurumlara ya da piyasadaki diğer büyük firmalara (bunlar piyasa altyapısı sunucularıdır, yetkili firmalarla birlikte tanımlı piyasalardaki önemli oyuncular ya da likidite sağlayıcılardır) uygulanabilen riskler dışındaki risk unsurları tüm firmalara uygulanabilmektedir.

Risk Grubu	Risk Unsuru
Strateji (İş riski)	**1. Stratejinin niteliği**

Firmanın tüm stratejisinden kaynaklanan riskler; stratejik planlama süreçlerinin niteliği, stratejilerin gerçekleştirilebilirliği, stratejinin etkileri, özellikle riskler açısından ve uygulama deneyimi.

Stratejik planlama süreci

- Yüksek hedefler seçilmesi süreci, bu hedeflerin detaylı biçimde kısa vadeli işlere dönüştürülmesi ve faaliyet planları
- Ticari faaliyette bulunulan ortamda gerçekleşen değişikliklere nasıl tepki verileceğine ilişkin çerçeve
- Düzenlemelere ilişkin önceliklerin dikkate alınmasına ilişkin süreç

Gerçekleştirilebilirlik/stratejinin realitesi

- Yüksek düzeydeki hedeflerin yapısı
- Stratejinin eş düzeydeki gruplarla mukayese edilebilirliği
- Hizmet verilen piyasada, dağıtımı yapılan ürünlerde ve dağıtım kanallarındaki değişikliğin düzeyi ve yapısı
- Maliyet yapısındaki değişikliğin düzeyi ve yapısı
- Piyasa payındaki değişikliğin düzeyi ve yapısı

En etkili alanlarda stratejinin etkileri

- Risk alma isteği
- Birleşme, devir/tasfiye
- İnsan gücü/yetenek
- Finansal kapasite
- Enformasyon teknolojisi (IT)
- Kontroller
- Dış kaynak kullanımı (outsourcing)

Uygulama

- Değişik senaryo alternatiflerini de içermek üzere uygulama planlarının kalitesi
- Uygulamanın takip edilmesi süreci
- Stratejik değişikliklerin uygulanmasında yönetim deneyimi
- Gerçekleşen hedeflerin takip edilmesi

Risk Grubu	Risk Unsuru
Strateji (İş riski)	2. Ticari yapı

Firmanın faaliyet gösterdiği iş kolunun (ticari yapının) özelliklerinden kaynaklanan riskler; firma ürünleri, hizmetler, müşteriler ve/veya kullanıcılar/ üyeler ve aralarındaki ilişkilere bağlı riskler.

Stratejide hedef alınan müşteriler ve/veya kullanıcılar/üyeler

- Perakende müşteri çeşidi-yüksek sermaye, zenginlik, orta düzey pazar, daha alt pazar
- Toptancı müşteri çeşidi-küçük ölçekli ticaret, büyük ölçekli şirket, kurumsal
- yüksek sermaye, zenginlik, orta düzey pazar, daha alt pazar
- Başlıca piyasa şirketleri çeşitleri ve/veya kullanıcı/üye-nakit, on-line, profesyonel
- Farklı pazarların doğru olarak hedeflenmesi yeteneği, müşteri bağlılığı ve/veya kullanıcı/üye tabanı
- Hizmet sunma kapasitesi, hizmeti sürdürme kapasitesi, farklı piyasalar

Stratejideki hedef piyasalar

- Coğrafik çeşitlilik ve hizmet sunulan pazarların risk özellikleri (ulusal /yabancı, gelişmekte olan piyasalar /gelişmiş piyasalar vb.)
- Siyasi müdahale riski
- Sektörel çeşitlenme

Stratejide hedeflenen ürünler/hizmetler

- Ürün ve hizmet çeşitleri ve özellikleri
- Müşteri ve/veya kullanıcı/üye segmentlerinin seçimine ilişkin uygunluk
- Ürün ve hizmetlerin rekabet edebilirliği
- Ürün ve hizmet fiyatlaması

Risk Grubu	Risk Unsuru
Piyasa, kredi ve faaliyet riski (İş riski)	3. Kredi riski

Firmanın üstlendiği kredi riskinin türü ve yapısından kaynaklanan riskler; firmanın risk alma isteği, firma ürün ve hizmetleriyle ilgili karşı taraf risklerinin yapısı, portföy özellikleri ve yapısı, kredi riski azaltma düzeyi ve yapısı.

Risk alma isteği

- Risk yelpazesinde kredi kültürünün ve pozisyonun yapısı (muhafazakar/girişimci)
- Deneyimlere ve stratejik yönetime uyum
- Risk alma isteğinin yönetim kurulunun standart ve değerlerini ne ölçüde yansıttığı

Ürün özellikleri

- Bilançoda karşı taraf risklerinin yapısı (ölçek, özellikler, yapı, likidite);
- teminatlı ve teminatsız krediler
- yatırım menkul kıymetleri
- reasürans
- bankalararası pozisyon

- Bilanço dışı karşı taraf risklerinin yapısı (ölçek, özellikler, yapı);
- türev ürünler (döviz, faiz oranı, kredi, mal/ürün)
- yayılma riski (kullanılmamış taahhüt imkanları, garantiler, teminat akreditifleri)
- aracılık (kredi, menkul kıymetler)
- ödeme, saklama ve gün-içi maruz kalınan risk yapısı
- takas evleri ve sistemlerinin kullanımı

Portföy özellikleri

- Bölge, sektör, müşteri, reassürör ve/veya kullanıcı/üye bazında yoğunlaşma
- Diğer risklerle etkileşim, özellikle faiz riski ve döviz riski
- Bağlı riskler
- Hacim, sektörler ve yoğunlaşmalardaki eğilim
- Portföy kalitesinin eğilimi (karşı taraf sınıflandırması, ödemede gecikme, takipteki alacaklar)

Risk azaltma

- Teminatlar (tür, kalite, likidite, pazarlanabilirlik, değerleme sıklığı, dokümantasyon)
- Netleştirme ve mahsup etme düzenlemeleri
- Kredi türevleri
- Teminatlar
- Reasürans

Risk Grubu	Risk Unsuru
Piyasa, kredi ve faaliyet riski (İş riski)	**4. Sigorta riski**

Firmanın üstlendiği sigorta aracılık yüklenimi riskinden kaynaklanan riskler; firmanın risk alma isteği, firma ürün ve hizmetlerinde sigorta aracılık yüklenimi dolayısıyla maruz kalınan risklerin yapısı, portföy özellikleri, reasüransın yapısı ve kapsamı.

Risk alma isteği

- Reasürans alımını da içermek üzere risk yelpazesinde sigorta risk kültürünün ve pozisyonun yapısı (muhafazakar/girişimci).
- Deneyimlere ve stratejik yönlendirmeye uyum
- Risk alma isteğinin yönetim kurulunun standart ve değerlerini ne ölçüde yansıttığı

Ürün özellikleri

- Sigorta risklerinin yapısı (ölçek, vade, karmaşıklık, iptal hükümleri)
- emlak ve kaza (perakende ve ticari)
- hayat
- sağlık
- Alınan garantilerin yapısı

Portföy özellikleri

- Bölge, sektör, müşteri, aracı kurumlar ve reassürör bazında yoğunlaşma
- Hacim, sektörler ve yoğunlaşmalardaki eğilim
- İş kolu/sektör türüne göre alacakların tahsili (alacaklar/prim oranı, ödenen/borç alacakları oranı)
- Riziko ve olasılık çizelgesindeki değişikliklerin etkisi

Reasürans

- Reüsürans sigortasının kapsamı, yapısı (yoğunlaşma, risklerin karşılaştırılması, dokümantasyon)
- Sigortanın uygunluğu ve yeterliliği

Risk Grubu	Risk Unsuru
Piyasa, kredi ve faaliyet riski (İş riski)	**5. Piyasa riski**

Firmanın üstlendiği piyasa riskinin türü ve yapısından kaynaklanan riskler; firmanın risk alma isteği, firma ürün ve hizmetlerinde maruz kalınan piyasa riskinin yapısı ve portföy özellikleri.

Risk alma isteği

- Piyasa riski kültürünün yapısı ve risk ölçeği (muhafazakar/girişimci)
- Deneyimlere ve stratejik yönetime uygunluk
- Risk alma isteğinin yönetim kurulunun standart ve değerlerini ne ölçüde yansıttığı

Ürün/piyasa özellikleri

- Müşteri ve/veya kullanıcı/üye ile mülkiyet güdümlü
- Kullanılan piyasalar; tezgah üstü / döviz
- Ürün yapısı (karmaşıklık, volatilite, likidite)
- nakit (bono, mal, net varlık)
- türev ürünler (faiz oranı, döviz, mal, net varlık)
- Ticari hesapların (bilançonun) dışında kalan piyasa riski
- bankaların bilançolarında faiz riski
- sigorta şirketlerinin yatırım portföylerinde piyasa riski
- döviz riski (kur dönüşüm riskleri dahil)
- diğer saklanmış riskler

Portföy özellikleri

- Alınan pozisyonların büyüklüğü ve yapısı
- Portföy likiditesi ve likidite riskine açıklık
- Diğer risklerle etkileşim, özellikle kredi riski
- Yoğunlaşmalardaki eğilimler
- Alınan pozisyonlardaki eğilimler

Risk Grubu	Risk Unsuru
Piyasa, kredi ve faaliyet riski (İş riski)	**6. Faaliyet riski**

Firma faaliyetleri ile ilgili olarak firmanın maruz kalabileceği faaliyet risklerinin türü ve yapısından kaynaklanan riskler; yetersiz ya da başarısız kurum içi süreçlerden, çalışanlarda ve sistemlerden ya da dış etkenlerden kaynaklanabilecek doğrudan ya da dolaylı kayıplar. (not: kontrol çevresi ile ilişkili olarak faaliyet riski ilgili diğer kontrol bölümlerinde değerlendirilecektir.

Risk alma isteği
- Faaliyet riski kültürünün yapısı ve risk ölçeği (muhafazakar/girişimci)
- Mali kaynaklar ve itibar üzerindeki etkilere ilişkin kabul edilebilir sınırlar
- Stratejik yönetime uyum
- Risk alma isteğinin yönetim kurulunun standart ve değerlerini ne ölçüde yansıttığı

İnsan kaynaklı riskler
- Faaliyet riskleri hakkında Yönetimin bilinci
- Personelin eğitim ve denetiminin işin yapısına ve stratejilere uygunluğu
- Kaynak profili (örneğin; personel sayısı, geçici ve daimi personel, personel dönüşümü)

Süreç ve sistemlerden kaynaklanan riskler
- İşlemlerin karmaşıklığına ve hacmine göre manuel ve otomatik süreçlerin ve sistemlerin durumu ve uygunluğu
- Süreç ve sistem başarısızlıklarının sıklığı ve etkileri (örneğin; müşteri/kullanıcı şikayetleri, düzenleyici mükafatlar, sistemdeki kesintiler, uzlaşma aralıkları, işlem ve dokümantasyon hataları
- Süreç ve sistem başarısızlıklarının piyasa, kredi ve sigorta risk sistemleri ve kontrolleri ya da diğer yasal yükümlülükler üzerindeki etkileri

Değişimden kaynaklanan riskler

- Çevre değişiminin boyutu (yeni teknoloji, yasal çerçeve, piyasa yapısı vb.)
- Yeni personel, karşı taraf ve sunucuların düzeyi
- Mevcut süreç ve sistemlere yönelik önemli ya da yeni değişikliklerin boyutu
- Mevcut ürün ve faaliyetlere yönelik önemli ya da yeni değişikliklerin boyutu
- Önemli şirket faaliyetlerinin varlığı (örneğin; birleşme, satın-alma ya da tasfiyeler)

Firma yapısına bağlı riskler
- Bölümler ve personel arasındaki ilişkiler ve karşılıklı bağımlılıklar
- Ticari yapının karmaşıklığı (örneğin; çoklu ya da ayrı yerleşim, çok sayıda yasal varlık, grup şirketleri ile bağlı ilişkiler)
- Dış kaynak kullanımının karmaşıklığı ve güven (itimat)

Risk azaltma
- Sigorta kapsamı

Risk Grubu	Risk Unsuru
Piyasa, kredi ve faaliyet riski (İş riski)	**7. Hukuki/yasal risk**

Firmanın yapmış olduğu sözleşmelerin türü ve yapısından kaynaklanan riskler; mevcut yasalara göre sözleşmelerin uygulanamaması ve ürün/hizmet yapısının firmayı özellikle hukuki risklere (davalara) maruz bırakması.

Riskin kaynağı-genel

- Faaliyette bulunulan iş koluna ilişkin yasaların açık olmaması ya da belirsizlik bulunması
- Firmanın müşteri ve/veya kullanıcı/üye ile ilgili hukukta yasaların açık olmaması ya da belirsizlik bulunması
- Ürün, müşteri ve/veya kullanıcı/üye sözleşmelerin belgelerin yetersizliği
- Hedef piyasalara ilişkin yasal çerçeve (coğrafik ve ürün) ile müşteri ve/veya kullanıcı/üye yasal pozisyonlarında değişiklik

Riskin kaynağı-diğer risklere bağlı olan

- Kredi riski (örneğin; kredi sözleşmesinin vadesi, yasal güvence uygulanabilme yetisi)
- Sigorta riski (örneğin; alacaklara ilişkin dava)
- Piyasa riski (örneğin; karmaşık türev ürün sözleşmelerinde tetikleyen hükümlerin bulunması)
- Faaliyet riski (örneğin; dış kaynak kullanımı sözleşmeleri, farklı hukuk alanlarında koruyucu alt düzenlemelerin uygulanabilirliği)

Geçmiş eğilimler

- Firmaya ile ilgili mevcut hukuki davalar
- Hukuki davalara bağlı kayıpların kayıtları ve kayıp türleri

Risk azaltma

- Sigortanın yapısı ve yeterliliği

Risk Grubu	Risk Unsuru
Finansal yapı (İş riski)	**8. Sermaye yeterliliği**

Firmanın sermaye durumundan kaynaklanan riskler; firmanın sermaye planlama çerçevesi, sermayenin kompozisyonu ve niteliği, mevcut ve hedeflenen faaliyetlerin sürdürülmesi için sermayenin yeterliliği, rezervlerin yeterliliği ve ilave sermaye imkanı.

Sermaye planlama çerçevesi

- Mevcut ve hedeflenen faaliyetler ve bunlara ilişkin risklere bağlı olarak sermaye gereğinin değerlendirilmesi süreci
- Stres ve senaryo testlerinin kullanılması

Kompozisyon ve nitelik

- Sermayenin unsurları
- Daha düşük nitelikli sermaye türlerinin kullanımı (örneğin; ikincil, geri ödenebilir, melez, örtülü unsurlar)
- Bir grup yapısı içinde sermeyenin yerleştirilmesi

Sermaye yeterliliği

- Sermaye yeterliliği hesaplanırken dikkate alınacak unsurlar:,
- bilanço içi ve bilanço dışı büyümede eğilimler ve projeler,
- tüm risk çeşitlerinin dahili değerlendirmeler,
- düzenleyici sermaye gerekleri,
- sermaye geri ödemesi ve kar payı dağılımlarına ilişkin planlar,
- stres ve senaryo testleri
- Birleşme gibi firma yapısıyla ilgili gelişmelerin etkileri

Rezerv yeterliliği

- Kredi kayıp karşılıkları
- Sigorta alacak karşılıkları
- Piyasa riski değerleme ve likidite karşılıkları
- Hukuki karşılıklar

Sermaye erişimi

- Geçmişte ilave sermaye ihtiyacının doğmasına ilişkin kayıtlar
- Mevcut ya da yeni hissedarlardan ilave sermaye edinebilme
- Sermaye artırımı için piyasa koşullarının uygunluğu (ev sahibi ülke ortamı)

Risk Grubu	Risk Unsuru
Finansal yapı (İş riski)	**9. Likidite**

Firmanın aktif/pasif kompozisyonundan ya da likidite yapısından kaynaklanan riskler; firmanın likidite yönetim çerçevesi ile günlük bazda ve kriz anında firmanın faaliyetlerini ve finansal yükümlülüklerini yerine getirmesi için gerekli fon akışını sağlamak üzere likidite kompozisyonu.

Likidite yönetimi çerçevesi

- Likidite politikasının yapısı
- Fonlama maliyetlerinin yönetimi ve likiditenin sürdürülmesi arasındaki uygunluk
- Düzenleyici yükümlülükler karşısındaki seyrin izlenmesi
- Farklı ve en kötü durum senaryoları için beklenmedik durum planlaması

Likidite kompozisyonu

- Fonlama yapısı ve çeşitlendirme – toptancı/perakendeci, vade yapısı, grup kaynaklarına güvenme, çekilmemiş taahhütlerin yapısı
- Fonlama kaynaklarının volatilitesi
- Likit aktiflerin niteliği (aktiflerin bağlı aktif olup olmadığı da değerlendirmek üzere)
- Fonlama maliyetleri
- Fon sağlayıcıların yoğunlaşması (toptancı/perakendeci)

Likidite erişimi

- Piyasanın ve derecelendirme kuruluşlarının görüşü
- Ana şirket ya da diğer grup şirketlerinden destek sağlayabilme durumu
- Kaynak sağlayıcıları ile ilişkilerin gücü

Likidite gereklerine ilişkin projeksiyonlar

- Kaynak, güvenirlilik, verilerde zamanlılık
- Projeksiyonlara ilişkin geçmiş kayıtlar
- Beklenmedik durum planlarının test edilmesine ilişkin aralıklar ve deneyimler

Risk Grubu Müşteri/kullanıcı ve ürün/hizmet yapısı (İş riski)	Risk Unsuru 12. Kaynaklar ve dağıtım kanalları

Firmanın faaliyette bulunduğu iş için erişebileceği mevcut kaynakların yapısı ve firma tarafından kullanılan dağıtım kanallarından kaynaklanan riskler; mevcut müşteri ve/veya kullanıcı/üye girişleri, aracı kullanımı ve sınır ötesi müşterileri kaynakları.

Doğrudan

- Farklı dağıtım kanallarının kullanılması (örneğin; şube ağı, internet)
- Mevcut müşterilere yenilenen ve artan ürün satışlarının düzeyi
- Yenilenen ve artan ürün satışlarını sağlamak için yöntemler
- Yeni müşteri ve/veya kullanıcı/üye edinilmesi için yöntemler
- Mevcut müşteri ve/veya kullanıcı/üyeler ile yeni müşteri ve/veya kullanıcı/üyelerden yeni işler çıkarılması için yöntemler
- Mevcut ve yeni müşteri ve/veya kullanıcı/üyelere satışları etkileyecek yeni kanalların geliştirilmesi

Aracılar

- Aracıların ne ölçüde kullanıldığı
- Aracılara yönelik kullanılan pazarlama metotları
- Aracılar ile ilişkilerin yapısı

Sınır-ötesi

- Sınır-ötesi müşterilerin kapsamı
- Sınır-ötesi müşteri ve/veya kullanıcı/üyelerin yerleşim yerleri
- Sınır-ötesi müşteri ve/veya kullanıcı/üye sağlanması için yöntemler
- Mevcut ve yeni müşteri ve/veya kullanıcı/üyelere satışları etkileyecek yeni kanalların geliştirilmesi

Risk Grubu	Risk Unsuru
Müşteri/kullanıcı ve ürün/hizmet yapısı (İş riski)	**13. Ürün/hizmet**

Firmanın sunduğu ürün ve hizmetlerin özelliklerinden kaynaklanan riskler; ürünlerin karmaşıklığı, seyri ve performansı.

Karmaşıklık

- Karmaşık ve açık olmayan yapıların kullanımı
- Piyasa, bölge, risk faktörleri ve karı taraf riskleri arasındaki ilişkilerin düzeyi
- Performans için diğer grup şirketlerine güven
- Teminatlar ve diğer güvencelerin yapısı
- Ürünlere bağlı finansal suçlardan kaynaklanan riskler (örneğin; piyasa manipülasyonları, karapara aklanması , hile karşındaki eğilimler)

Performans

- Uzun vadeli bankacılık, sigorta ve yatırım ürünlerinin yapısı ve boyutu
- Erken sonlandırma koşulları
- Esneklik (örneğin; müşterilerin vade değişiklikleri yapabilme yetisi)
- Müşterilerin bazı koşulları karşılayamaması durumunda firmanın sözleşmeleri sonlandırma olanağı
- Muhtemel volatilite
- Müşterilerin performans beklentilerini karşılamada ürünlere ilişkin geçmiş kayıtlar

Yasal yetki alanları

- Sınır-ötesi yatırım planları, satılan diğer ürünler ya da hizmetler
- Sınır-ötesi yatırım planları, satılan diğer ürünler ya da hizmetlere ilişkin hukuki yetki alanları

Müşteri ve/veya kullanıcı/üye

- Kontrol edilen ya da elde tutulan müşteri ve/veya kullanıcı/üye aktiflerinin yapısı ve boyutu
- Üçüncü kişiler ya da firma tarafından elde tutulan müşteri ve/veya kullanıcı/üye aktiflerinin boyutu

Hizmetler

- Danışmanlık hizmetlerinin kapsamı
- Sadece hizmet edimlerinin kapsamı
- Yönetilen hesapların kapsamı
- Araştırma koşullarının kapsamı

Risk Grubu Müşteri/kullanıcı ve ürün/hizmet yapısı (İş riski)	Risk Unsuru 14. Piyasa verimliliği (Piyasadaki başlıca firmalar)

Fiyat oluşturma süreçlerinden kaynaklanan riskler; yeterli likidite koşulları, önceki ve geçmiş ticari şeffaflık düzeylerinin uygunluğu.

Likidite

- Likidite destek ve teşviklerine ilişkin düzenlemeler
- Piyasa yapıcılığına ilişkin taahhütler

Şeffaflık

- Fiyat oluşturma düzenlemeleri
- Önceki ve geçmiş ticari şeffaflık için düzenlemeler
- Ticaretin adil ve düzenli yapılması için düzenlemeler
- Uygun olmayan ticari faaliyetlerin önlenmesi için taahhütler (örneğin; ikamet, temizlik ile ilgili ticaret)
- Müdahalelere ilişkin düzenlemeler
- Ticari bloke etme kuralları, uygulama ve uyum
- Geçmiş yayınlara ilişkin düzenlemeler

Risk Grubu	Risk Unsuru
Müşteri/kullanıcı ve ürün/hizmet yapısı (İş riski)	**15. Uygun piyasalar (Sadece kabul edilmiş yatırımların mübadelesi)**

Kabul edilmiş yatırımların mübadelesi yoluyla yapılan yatırım sözleşmeleri için piyasa özelliklerinden kaynaklanan riskler.

Piyasa özellikleri

- Belirli bir yatırımı elinde tutan ya da sözleşme yapmayı isteyen yatırımcıların dağılımı
- Yatırımı elde tutan ya da elde tutulabilen miktarlarda alış veriş yapanlara yönelik sınırlamalar
- Yatırım işlemi için sözleşme yapılması ya da teslimi için araçlar
- Ticareti yapılan yatırımların hacmi ya da içerdiği riskler hakkında doğru karar vermelerini sağlamak üzere kamuoyunda piyasa katılımcılarına sunulan bilgilerin yapısı

Risk Grubu	Risk Unsuru
Müşteri/kullanıcılara yönelik davranış (Kontrol riski)	**16. Satışı esasına dayalı eğitim ve istihdam**

Satış esasına dayalı eleman alımı ve eğitim prosedürlerinden kaynaklanan riskler.

Eleman alımı

- Amaca uygun seçilen muhtemel elemanların yetenekleri ve bilgilerinin dikkate alınmasına yönelik prosedürlerin uygunluğu
- Önceki faaliyetler ve eğitimler hakkında yeterli bilgi sağlanmasına yönelik prosedürlerin uygunluğu

Eğitim

- Etik uygulamalar ile hedeflenen satışların gerçekleşmesi arasındaki dengenin sağlanması
- Eğitilenlerin müşterinin risk alma isteğini ve bilgisini değerlendirmesine imkan verecek eğitimler
- Uygun aralıklarda çalışanların eğitim ihtiyaçlarının belirlenmesine yönelik prosedürlerin uygunluğu
- Faaliyetlerle ilgili olarak eğitimlerin planlaması, yapılandırılması ve değerlendirilmesinin uygunluğu

Beceri kazanılması

- Satış görevi için kişilerinin becerilerinin değerlendirilmesine yönelik prosedürlerin uygunluğu
- Çalışanın uygun sınavlardan geçirilmesine ya da uygun muafiyetler tanınmasının sağlanmasına yönelik prosedürlerin uygunluğu

Becerilerin yönetimi

- Teknik bilgisi, becerileri ve piyasa, ürünler, yasal mevzuat ve düzenleme değişiklikler dikkate alınarak belirli görevler için kişilerin ehil olup olmadıklarının değerlendirilmesini sağlayacak prosedürlerin uygunluğu

Denetim yetkisi

- Denetimlerin yeterliliğini sağlayacak düzenlemelerin uygunluğu
- Çalışanların eğitim ve yetkilere ilişkin düzenlemelerin bilincinde olması

Risk Grubu Müşteri/kullanıcılara yönelik davranış” (Kontrol riski)	Risk Unsuru 7. Personel ücret esasları

Firma çalışanları için ücretlendirme planının yapısından kaynaklanan riskler.

Politika

- Personel ücret politikasının açıklığı
- Ücret politikasının olası hileli davranış ya da yetkinin yanlış kullanımını üzerindeki etkilerinin dikkate alınma derecesi
- Ücret politikasından kaynaklanan hileli davranış ya da yetkinin yanlış kullanımına yönelik risklerin azaltılması için kullanılan araçlar

Uygulama

- Satış esasına dayalı farklı uygulamalara ilişkin maaş, komisyon ya da prim arasında ücretlendirmenin ayrımı
- Firmanın diğer alanlarında oluşabilecek hileli davranış ya da yetkinin kötüye kullanımına karşı maaş, komisyon ya da prim arasında ücretlendirmenin ayrımı
- Hile ya da yetkinin kötüye kullanımı hakkındaki geçmiş bilgiler ve ücretlendirme politikalarıyla ilişkisi

Risk Grubu	Risk Unsuru
Müşteri/kullanıcılara yönelik davranış (Kontrol riski)	**18. Finansal promosyon (teşvik)**

Firmanın reklam ve promosyon uygulamalarının yapısından kaynaklanan riskler.

Politika ve prosedürler

- Reklam politikasının yapısı ve varlığı
- Politika onayları için sorumluluk
- Politikalarla uyum sağlanmasına ilişkin prosedürlerin yeterliliği
- İlgili sektör standartları ve FSA kuralları ile uyum sağlanmasına ilişkin prosedürlerin yeterliliği
- Uyum sorumluluğu

Kayıtlar/Deneyim

- İç politikalara bağlılık
- FSA prensip ve kuralları ile diğer sektör standartlarına bağlılık
- Yanlış yönlendiren reklamlar hakkında müşteri şikayetlerinin yapısı ve sayısı

Risk Grubu Müşteri/kullanıcılara yönelik davranış (Kontrol riski)	Risk Unsuru 19. Müşteri ve/veya kullanıcı/üye kabulü, danışmanlık ve raporlama

Firmanın müşteri sınıflaması ve dokümantasyon prosedürlerinin işleyişi, danışmanlık kalitesi (örneğin, risk ve değişiklikleri müşterinin anlaması, uygunluk) ve müşteri ve/veya kullanıcı/üye raporlamalarının işleyişinden kaynaklanan riskler.

Müşteri kabulü

- Müşteri ve/veya kullanıcı/üye sözleşmelerinin bağıtlanmasına ilişkin prosedürlerin yeterliliği
- Müşterini tanı prensibini içermek üzere müşteri ve/veya kullanıcı/üye uygunluğunun değerlendirilmesi ve firma tarafından sunulan hizmetlerin müşteri ve/veya kullanıcı/üye tarafından anlaşılmasına ilişkin prosedürlerin yeterliliği
- Çıkar çatışmasıyla ilgili konuların (aracı kuruluşlardan kaynaklananlar da dahil olmak üzere) incelenmesinin yeterliliği
- Özel müşteri ya da özel müşteri statüsüyle korumadan feragat edilmesine ilişkin prosedürlerin yeterliliği
- Aracı kuruluşların değerlendirilmesine ilişkin prosedürlerin yeterliliği
- İşin (ticaretin) kalitesinin değerlendirilmesine ilişkin prosedürlerin yeterliliği

Danışmanlık

- Tavsiyelerin uygunluğunun sağlanmasına ilişkin aşamaların yeterliliği
- Danışmalık için doğru dokümantasyon kayıtlarının yeterliliği
- Müşterinin riskleri anlamasına ilişkin aşamaların yeterliliği
- Mevcut sözleşmelerin yenileri ile değiştirilmesi sırasında uygun olmayan tavsiyelerde bulunulmasından kaçınılmasına ilişkin aşamaların yeterliliği
- Stabilizasyona tabi olabilecek menkul kıymetlere ilişkin uygun açıklama yapılamasının yeterliliği
- Firmanın işlemlerdeki herhangi bir maddi çıkarının deklare edilmesinin sağlanmasına ilişkin prosedürlerin yeterliliği
- Makul komisyonların kamuya açıklanmasına ilişkin prosedürlerin yeterliliği (Firmanın ücretlendirmesi ve aracı kuruluşlarca uygulanan komisyonlar da dahil kamuya eksiksiz açıklama yapılmasını içermek üzere)

Raporlama ve şikayetlerin yönetimi

- Sözleşme notlarının zamanında düzenlenmesine ilişkin prosedürlerin yeterliliği
- Periyodik hesap özetlerinin sağlanmasına ilişkin prosedürlerin yeterliliği
- Geçmiş satışlardaki değişiklikler hakkında iletişimin yeterliliği
- Alınan şikayetlerin değerlendirilmesine ilişkin prosedürlerin yeterliliği
- Alınan şikayetler ders çıkarılmasına ilişkin sistemlerin yeterliliği

Kayıtlar/Deneyim

- FSA prensipleri, kuralları ve diğer sektör standartlarına bağlılık
- Kabul, danışmanlık ve raporlama konusundaki müşteri şikayetlerinin sayısı ve yapısı

Risk Grubu	Risk Unsuru
Müşteri/kullanıcılara yönelik davranış (Kontrol riski)	**20. İşlem ve yönetim**

Müşteri varlıklarına ilişkin işlemler ve yönetiminden kaynaklanan riskler.

Yönetim

- Aşağıdaki kuralları da içermek üzere iş kurallarına uygun olarak göre yönetimin yapılanmasına ilişkin prosedürlerin yeterliliği;
- müşterinin yatırım kriterlerine uygunluk
- maddi çıkarlar
- firmanın kendi pozisyonu ve diğer çıkar çatışması alanları dikkate alınarak müşterilere eşit muamele yapılması
- komisyonlar
- komisyonları artırmak için gereksiz yere işlem miktarının artırılması

İşlem

- Müşteri varlıklarına ilişkin aşağıdaki işlemleri içermek üzere işlem prosedürlerinin yeterliliği;
- çıkar çatışması
- zamanında icraat
- en iyi icraat
- zamanında tahsisat
- adil tahsisat
- yayınlanmış araştırma/analiz/tavsiyelerin işlem görmesi
- müşteri emirlerinin önceliği
- şarta bağlı yükümlülük işlemleri
- ertelenen ya da kota 4edilmemiş yatırımlar
- piyasanın kötüye kullanımı ve müşteri borçlanması
- içeriden işlem
- stabilizasyon
- aracılık yüklenimi
- yatırımlarda işlemlerin düzenlenmesi
- kolektif yatırım planlarının oluşturulması, operasyonu ve tasfiye edilmesi

Kayıtlar/Deneyim

- FSA prensipleri, kuralları ve diğer sektör standartlarına bağlılık
- İşlemler ve yönetim konusundaki müşteri şikayetlerinin sayısı ve yapısı

Risk Grubu Müşteri/kullanıcılara yönelik davranış (Kontrol riski)	Risk Unsuru 21. Müşteri/kullanıcı/üye varlıklarının güvenliği

Firma tarafından tutulan ve/veya kontrol edilen müşteri ve/veya kullanıcı/üye varlıkları ve paralarından kaynaklanan riskler

Saklama

- Aşağıdaki işlemler için prosedürlerin yeterliliği;
- ayırma
- kayıt ve belgeleme
- muhafaza etme
- saklanan yatırımların transferi
- saklama hizmeti verenlerin uygunluğu
- risklerin kamuya açıklanması
- hesap belgelerinin hazırlanması, içeriği ve gönderilmesi
- saklama anlaşması
- stok borç verme ve geri alım anlaşmaları
- hesap mutabakatı

Müşteri parası

- Aşağıdaki işlemler için prosedürlerin yeterliliği;
- müşteri parasının tespiti
- müşteri banka ve aracı kurum hesapları (kurumun değerlendirmesi dahil olmak üzere)
- nün Banka ve aracı kurumun statü onayı
- takas bankası ve aracı kurum hesapları
- ayırma
- müşteri para hesabına ve başka hesaba ödeme
- faiz tahsisi ve ödemesi
- hesap mutabakatı

Kayıtlar/Deneyim

- FSA prensipleri, kuralları ve diğer sektör standartlarına bağlılık
- Varlıkların güvenliği konusundaki müşteri şikayetlerinin sayısı ve yapısı

Risk Grubu Organizasyon (Kontrol riski)	Risk Unsuru 26. Grubun diğer bölümüyle ilişkiler

Firmanın grubun diğer bölümleriyle arasındaki ilişkilerden kaynaklanan riskler; düzenlemelerin yönetimi, merkezi fonksiyonlara uyum, finansal yapının durumu ve grubun faaliyetleri, diğer grup şirketlerine finansal ve diğer bağımlılıklar.

İlişkinin yapısı

- Tüzel kişiliğin yönetim yapısı
- Raporlama akışı
- Grubun herhangi bir bölümü tarafından resmi ya da garı resmi olarak uygulanan kontrol ve etkinin düzeyi
- Matris yönetim düzenlemelerinin açıklığı ve şeffaflığı

Merkezi fonksiyonlar

- Yerleşim (örneğin; off-shore operasyonları)
- Firmanın faaliyetleri ile ilgili olarak grubun kontrol fonksiyonlarının etkinliği; risk yönetimi, uyum, iç denetim, finans, ürün kontrolü, yatırım stratejisi
- IT bağlantıları
- Grup içindeki farklı firmalar arasındaki karşılıklı bağlantıların açıklığı

Finansal ilişkiler

- Karşılıklı ilişkilerin yapısı; sermaye, fonlama likidite, iş ilişkileri
- Grubun ve karşılıklı ilişki içinde olan grup şirketlerinin finansal durumu
- Grup şirketlerinin karşılıklı yükümlülükleri ya da istekleri yerine getirme kabiliyeti üzerindeki kısıtlamalar

Ürün/pazarlama ilişkileri

- Firmanın grubun diğer bölümleri adına sattığı ürün ve hizmetlerin yapısı
- Grup şirketlerince paylaşımı yapılan müşteri ve/veya kullanıcı/üyelere hizmet ve ürün dağıtımında etkinlik
- Grup şirketlerine satılan ürün ve hizmetlerinden kaynaklanan finansal yükümlülükler ya da yanlış satışlara ilişkin tecrübe ve kayıtlar

Grubun faaliyetleri

- Grup şirketleri arasındaki çıkar çatışmalarının yönetimi
- Özel amaçlı araçların kullanımı
- Grup içindeki olayların ve faaliyetlerin etkileri (finansal suç, finansal zayıflık, müşteriye yanlış satış ve kontrol zaafiyetleri)

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	27. Risk yönetimi

İşle ilgili risklerin zamanında ve doğru biçimde tanınması, ölçümü, izlenmesi ve kontrolüne yönelik sistem ve prosedürlerin etkinliği ve yapısından kaynaklanan riskler; kredi riski, sigorta ve aracılık riski, piyasa r,ski, operasyonel risk, yasal risk ve yeni ürün riski.

Yüksek düzeyde risk politikası

- Risk alma isteğinin oluşturulması ve risk yönetim işlevinin yönetiminin delegasyonunda Yönetim Kurulunun işlevi
- Özel risk türleri, karşı taraf riski ve firma faaliyetlerine ilişkin maruz kalınabilecek riskler için kabul edilebilir sınırların oluşturulmasını içeren risk stratejisinin uygulanmasına yönelik üst düzey yönetimin işlevi
- Risk kültürünün sürdürülmesi ve iletişimin etkinliği
- Firmanın faaliyetleriyle ilgi risklerin hangi boyutta risk yönetimine tabi olacağı
- Sermaye dağılımı, uygun karşılıkların ve rezervlerin ayrılmasıyla ilgili politikalara ilişkin sorumluluklar
- Çalışanlara yönelik ödül mekanizması ve risk kültürü arasındaki uyum

Risk tanıma

- Risk tanınmasına ilişkin sorumluluklar
- İş risklerinin tanınması işlevi
- İş ile ilgili risklerdeki değişikliklerin düzenli olarak gözden geçirilmesi
- Yeni ürün onaylanmasına ilişkin işlevin yapısı ve etkinliği

Risk değerlendirmesi/ölçümü

- Risk ölçüm ve değerlendirmesi sürecinin uygunluğu, yeterliliği ve sıklığı
- Kullanılan verinin ve zaman kesitinin kaynakları (örneğin; piyasa fiyatları, pozisyon bilgisi, doğru veri, kredi temerrüdüne düşme olasılıkları, operasyonel zararlar)
- Risklerin boyutu, karmaşıklığına göre kullanılan modelleri içermek üzere risk değerlendirme ve ölçümü ile ilgili Araçların uygunluğu ve sağlamlığı
- Kullanılan risk değerlendirme ve ölçüm araçlarının değerlendirilmesinin sıklığı ve doğruluğu
- İşlem, portföy, departman ya da firma düzeyinde piyasa riski, kredi riski, sigorta ve operasyonel risklerin ölçümü ve değerlendirilmesi yeteneği

Risk izleme

- Tüm tanımlanmış risklerin izlenmesini temin edecek metodoloji
- İzleme raporlarının açıklığı, doğruluğu, zamanlılığı ve sıklığı
- Yönetim ve çalışanlara raporların dağıtımı
- Risk pozisyonlarının önceden belirlenmiş sınırlarla karşılaştırılması (karşı tarafta yer alan bireyler ve gruplar karşında maruz kalınacak riskleri içermek üzere)

Risk kontrol ve risk yönetimi işlevi

- İşe ilişkin risklerin tanınması işlevi
- Risk kontrol ve risk yönetim fonksiyonunda çalışanların deneyimi, yetenekleri ve özellikleri
- Risk kontrol ve risk yönetim fonksiyonu ile ilgili üst yönetime raporlama akışı
- Risklerin önceden belirlenmiş sınırlar içinde yönetilmesinin temini için yapılanlar
- İstisnai raporların yapısı, takip ve eskalasyonun geçerliliği

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	**28. Politikalar, prosedürler ve kontroller**

Politikalar, prosedürler, kontroller ve bunların uygulamalarından kaynaklanan riskler.

Politika, prosedür ve kontrollerin niteliği ve uygunluğu

- Finansal yapının doğruluğu ve sağlığı, müşteri aktiflerinin güvence altında olduğu ve piyasanın kötüye kullanımı (karapara aklanmasıyla ilgili kontroller ayrı tutulmak üzere) ve hilelere karşı korunduğunu ve manuel kayıtların güvenliğini (elektronik kayıtlar ayrı değerlendirilmek üzere) temin etmek üzere politika, prosedür ve kontrollerin yeterliliği
- İşin yapısı, örgütlenmesi ve yönetim şekli ile uygunluk
- İşin büyüklüğü, özellikleri, hacmi ve işlemlerin karmaşıklığıyla uygunluk

Fonksiyonların ayrılması

- Piyasanın kötüye kullanımı ve hile için fırsatlar ve çıkar çatışmalarından kaynaklanan risklerin azaltılması amacıyla fonksiyonların ayrılması ve etkinliği

Finansal kontroller

- Gelir ve maliyet politikalarının tarafsızlığı ve tutarlılığı
- Farklı enstrümanlar için muhasebe politikalarının ekonomik amaçlarla uygunluğunun sağlanmasına yönelik prosedürler (örneğin yatırım, ticaret, riskten korunma)
- Firmanın muhasebe ve işlem verilerin doğru ve eksiksiz olmasını sağlamak üzere politika ve prosedürler
- Her türlü riskten kaynaklanabilecek muhtemel zararların karşılanması için makul düzeyde karşılık ayrılmasına yönelik politika ve prosedürler

Operasyonel kontroller

- Hileye karşı fırsatların azaltılması ve işlem kayıtların doğru ve tam olmasının sağlanmasına ilişkin prosedürler (örneğin; bağımsız uzlaşma, bağımsız teyitler, ödeme ve menkul kıymet hareketleri için bağımsız yetkilendirme prosedürleri)

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	**29. Yönetime bilgi verilmesi**

Yönetime sunulan bilginin yapısından kaynaklanan riskler; bilginin doğruluğu, ilgisi, yeterliliği, zamanındalığı ve dağıtımının etkinliği ve verimliliği.

Genel uygunluk
- İşin yapısı ve türüne
- Coğrafik temsile
- Firmanın faaliyetleriyle ilgili risklere

Bilginin yönetim kurulu ve üst yönetimce kullanılması
- İşin gözden geçirilmesi, stratejik ve operasyonel kararların alınmasında bilgilerin yönetim kurulu ve üst yönetimce kullanımı

Zamanlılık, doğruluk ve dağıtım
- İşin gereklerine göre raporlama dönemleri ve uygunluğu
- Üretim ve kaliteye ilişkin sorumluluk
- Manuel çalışmaları da içermek üzere değerlendirme işlevlerinin ve kullanılan sistem kaynaklarının kapsamı
- Kayıp veri, uzlaşılamayan konuların takibi gibi konuları içermek üzere doğruluk ve eksiksizliğin sağlanması için kalite kontrol işlevi
- Raporlama hiyerarşisi

Kalite
- Finansal bilginin yeterliliği, örneğin;
  - kar-zarar bilgisi (örneğin; iş, coğrafik dağılım, ürün ve tüzel kişilik bağlantılarıyla ilgili ayrıntılı hesaplar)
  - bilanço ve sermaye bilgisi (örneğin; likidite, iç ve dış likidite uygunluğunun analizi, büyük riskler ve sermaye yükümlülükleri)
- Bütçedeki büyük hareketler ve değişimlerin açıklanması
- Ekonomik sermaye ve ekonomik karlılık ölçümleri
- İş göstergelerinin yeterliliği, örneğin;
  - müşteri ve/veya kullanıcı/üye bilgileri (örneğin; kazanç ve zarar verisi, memnuniyet ölçümleri, şikayet bilgileri)
  - emsal grup karşılaştırmaları (örneğin; piyasa payı bilgileri)
- Risk bilgilerinin yeterliliği, örneğin;
  - kredi riski (örneğin; limitlere göre karşı taraf riski, bilanço dışı riski, geciken ve takibe alınan bilgilerin analizi, karşılık ayırma)
  - sigorta riski (örneğin; limitlere göre maruz kalınacak değerler, yoğunlaşmalar, alacak performansı)
  - piyasa riski (örneğin; hassasiyet testleri, VAR limitleri ve ürün/lokal ayrıma göre kullanım)
  - faaliyet riski (temel performans göstergeler, örneğin; işlevsel hatalar, işe ait kesintiler-müdahaleler, hile, yasal dokümantasyon hataları, istatistik temin edilmesine ilişkin haklar

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	**30. IT Sistemleri**

IT (Enformasyon Teknolojisi) altyapısına ilişkin kontrollerden kaynaklanan riskler; kaynakların yeterliliği, uygulama ve erişim prosedürleri, güvenlik çerçevesinin etkinliği, vb. ve IT altyapısının işin yürütülmesi için yeterli bir platform olup olmadığının değerlendirilmesi.

Kurum yapısı ve organizasyon
- Sorumlulukların ve raporlama süreçlerinin açıklığı
- Yüksek düzeyde raporlama gerekleri
- IT kaynaklarının yeterliliği
- IT görevlerinin ayrımının yeterliliği
- Yönetim yapısı (örneğin; danışma komiteleri, teknik standart forumları)

Proje yönetimi
- Teklif edilen projelerin geçerliliğini değerlendirme yöntemi
- Proje onayı ve onay işlevi
- Proje yönetim araçları, izleme ve raporlama işlevi
- Çoklu ve birbirinden bağımsız projelerin yüksek düzeyde kontrolü işlevi

IT uygulaması
- Uygulama sürecinde iş alanının yapısı
- Yetenek ve standartların erişimi, tasarımı ve gelişiminin yapısı
- Tanıma sistemlerinin entegre olması ihtiyacına yaklaşım
- Test, doğrulama, eğitim kullanımı ve destek sistemlerine yaklaşım

Bilgi güvenliği
- Güvenlik politikası ve standartlarının oluşturulması ve politikanın kullanıcılar tarafından anlaşılması
- Bilgi güvenliğiyle ilgili teknik uzmanlığın yeterliliği
- Güvenlik olaylarının raporlanması ve gerekli kararların alınmasına yaklaşım
- Güvenlik politikasıyla uygunluğun sağlanmasına yaklaşım
- Son kullanıcıya yaklaşım
- Virüs yönetimine yaklaşım
- IT güvenlik testine yaklaşım (örneğin; etik "hacking", güvenlik denetimleri)

Performans
- Hayat/üretim ortamındaki problemlerin tanınması ve çözümüne ilişkin yöntemler
- İstenilen hizmetleri tanımlamak üzere hizmet seviyeleri düzenlemelerinin yapısı
- Kapasite gereklerinin tahmini için yöntemler
- Problemli alanların belirlenmesi için eğilim analizinin kullanımı
- Problem teşhisi için test uygulaması

Risk Grubu Dahili sistemler ve kontroller (Kontrol riski)	Risk Unsuru 31. Finansal ve yasal raporlama ve muhasebe politikaları

Finansal ve yasal raporlamanın yapısından kaynaklanan riskler; finansal ve yasal raporlamanın yeterliliği, doğruluğu, ilgisi ve zamanın uygun oluşu, muhasebe politikalarının uygun şekilde uygulanması

Finansal raporlama

- Hissedarlara ve ilgili piyasalara yapılan finansal raporlamanın açıklığı ve zamana uygun oluşu
- Gelişmiş ve uygun muhasebe politikalarının oluşturulmuş muhasebe standartlarına bağlı kalınarak uygulanmasında tutarlılık
- Muhasebe politikalarının belgelenmesi için uygulanan standartlar
- Raporlamanın iç ve dış gelişmelere paralel olarak yapılanmasını temin edecek mekanizmalar
- Risklerden kaynaklanabilecek muhtemel kayıplar için yeterli karşılık ayrılmasının sağlanmasına ilişkin politikaların uygunluğu (örneğin; ticari operasyonlara ilişkin likidite rezervleri, kredi zarar karşılıkları)

Yasal raporlama

- FSA ve diğer düzenleyici otoritelerce talep edilen verilerin doğru biçimde raporlanması yeteneği
- Raporlamanın zamanında yapılması yeteneği
- Yasal raporlama için sorumlulukların açıklığı

Risk Grubu	Risk Unsuru
Dahili sistemler ve Kontroller (Kontrol riski)	32. Uyum

Uyum fonksiyonunun yapısı ve etkinliğinden kaynaklanan riskler; uyum yapısı, yönetim, emirler, personel, metodoloji ve verimlilik.

Yönetim/referans süreleri

- Referans süreleri ve hedefler, onaylanma düzeyleri
- Risk ve kontrol işlevindeki rolü
- İşe ve ilgili kayıtlarına erişim

Yapı, raporlama sırası ve kaynaklar

- Grup ve iş akışı arasındaki ilişkilerin uyum fonksiyonlarının yapısını içermek üzere uyum yapısı
- Raporlama sırası ve hesap verme fonksiyonu, firmanın yönetim organına erişim
- Kaynak, kalite ve uyum personelinin deneyimi
- Uyum, iç ve dış denetimler arasındaki bağlar
- Dış kaynak kullanımı
- İş ve üst yönetime layık olma

Metodoloji

- Belgelenmiş politika ve prosedürlerin geniş kapsamı
- Uyum için personele verilen eğitimin süresi ve sıklığı
- İşlemlere ilişkin danışmanlık kullanımı
- Aşağıdakiler de içermek üzere iç ve dış kurallara uyumun sağlanmasında uyum izleme işlevinin yeterliliği
  - iş birimleri ve ticaret masaları incelemeleri
  - ticaret gözetimi
  - çıkar çatışması prosedürleri (örneğin; kontrol odası, fiziki ayrım, çin duvarları vb.)

İzleme

- İstisna ve tavsiyelerin zamanında işaret edilmesi sürecinin yeterliliği
- Önemli istisna ve tavsiyelerin izlenmesi sürecinin yeterliliği
- İşaret edilmemiş sorunların eskalayonu

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	33. İç denetim

İç denetim fonksiyonunun yapısı ve etkinliğinden kaynaklanan riskler; uyum yapısı, vekalet, e-mirler, personel, metodoloji ve verimlilik.

Yönetim/referans süreleri

- Referans süreleri ve hedefler, onaylanma düzeyleri
- Risk ve kontrol işlevindeki rolü
- Tüm hesap ve kayıplara sınırsız erişim olanağı
- Bağımsız denetçiler ve hesap denetçileri ile ilişkiler

Yapı, raporlama sırası ve kaynaklar

- Sorumlulukların açıklığı
- Denetim Komitesine erişim sağlanmasında raporlama akışının ve doğrudan erişimin kullanılması ve bağımsızlığı; Yönetim Kurulu Başkanına ve CEO'ya erişim ve bu erişimin kullanımının düzenliliği
- Uyum fonksiyonu ve uyumun denetimi arasındaki ilişki
- İç denetim elemanlarının denetim planını uygulamak için kalite, tecrübe ve yeterliliği
- Üst yönetim, denetim komitesi ve bağımsız denetçilerin kredibilitesi
- Teknik deneyim ve kapasite düzeyi, eğitim kullanımı
- Dış kaynak kullanımı

Denetim planı

- Onay süreci
- İş ve altyapı alanlarının kapsamına karar verme süreci
- İşin kendi değerlendirme sürecinin güvenirlilik düzeyi
- Diğer sorumlulukların dahil edilmesi, özel projeler, hileli yeni ürün onayı

Metodoloji

- Riske dayalı metodoloji kullanımı
- Derecelendirme sistemi için tanımlar ve rasyonel sayılar
- Otomatik araçların kullanımı
- Yüksek riskli alanlara ilişkin yönetim değişikliği işlevi
- Olaylara karşı tepki verilmesi ve iç denetimce izin verilmiş soruşturmaların açılması

Denetim raporları

- Yönetimle iletişim ve uzlaşma işlevi
- Sorunların tanınması ve öncelik verilmesi

- Raporların zamanlılığı ve denetim puanlamasının kullanımı
- Raporların uygun üst yönetime dağıtımı

İzleme

- İstisna ve tavsiyelerin zamanında işaret edilmesi sürecinin yeterliliği
- Önemli istisna ve tavsiyelerin izlenmesi sürecinin yeterliliği
- Denetçi ya da diğerlerinden alınan dış kaynaklı tavsiyelerin dahil edilme düzeyi
- Tanımlanmamış konulardaki eskalayon işlevi

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	34. Dış kaynak kullanımı

Dış kaynak kullanımı ya da üçüncü kişi sunucuların kullanımından kaynaklanan riskler; dış kaynak ya da üçüncü kişilere güven ve kontroller.

Politika ve sorumluluk

- Firmadaki onay seviyesini içermek üzere dış kaynak ya da üçüncü kişi sunucuların kullanımına ilişkin politikaların uygunluğu
- Dış kaynak ya da üçüncü kişi sunucularla ilişiklere ilişkin sorumlulukların tüm yönleriyle açıklanması

Sunucu (Sağlayıcı) seçimi

- Sunucunun yetenekli, saygın, finansal açıdan güçlü ve uygun bilgi ve deneyime sahip olması için düzenlemeler

Sunucu ile anlaşma

- Firma ve sunucu arasında uygun bir hizmet anlaşmasının olması
- İlişkilerin düzenli olarak gözden geçirilme sıklığı ve özelliği
- İç ve dış denetçilere erişimin kullanımı ve yeterliliği, sunucuların denetçileri tarafından raporların kullanımı
- FSA bilgilerine erişimin yeterliliği
- Sunucudaki her hangi bir konudan firmanın haberdar olmasını sağlamak üzere sunucu ile firma arasındaki raporlama akışının yeterliliği

İzleme

- Sağlanan hizmetin firmanın ihtiyaçlarını karşılamaya ve mevcut stratejik amaçlarıyla uygun olmasının değerlendirilmesine ilişkin düzenlemeler
- Sistemin bütünlüğü ve kontrollerin devamlılığını sağlamak üzere sunucu ile ilişkilerin izlenmesine yönelik düzenlemeler

Beklenmedik durum planları

- Sözleşmenin sonlandırılması ya da sunucunun beklenen hizmeti sağlayamaması durumunda yeni düzenlemelerin yapılmasına ilişkin planların yeterliliği

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	**35. Profesyonel danışmanlık**

Profesyonel danışmanlık kullanımından kaynaklanan riskler; profesyonel danışmanların seçimine ilişkin kontroller ve ilişkilerin izlenmesi.

Danışman seçimi

- Seçim işlevi
- Mevcut işler için profesyonel danışmanların uygunluğu
- Profesyonel danışmanların itibarı
- Firma ile profesyonel danışmanları arasındaki ilişkilerin devamlılığı
- Danışmanların rotasyonuna ilişkin politika

Danışmanların rolü

- Profesyonel danışmanların firmadan bağımsız oluşu
- Çıkar çatışmalarının yönetimi
- Yönetimin tavsiyeye göre hareket düzeyi

Risk Grubu	Risk Unsuru
Dahili sistemler ve Kontroller (Kontrol riski)	**36. İş sürekliliği**

İş sürekliliğine ilişkin düzenlemelerin yapısı ve etkinliğinden kaynaklanan riskler; planlama sürecinin yeterliliği, iş sürekliliği planının niteliği ve test süreci.

Strateji geliştirme

- Tüm maddi iş birimlerini ve faaliyetlerini kapsamak üzere bir firmanın iş sürekliliği risk değerlendirme ve azaltma planının kesintisiz olarak geliştirilmesi ve güncellenmesine ilişkin sorumlulukların açıklığı
- Planların geliştirilmesi ve onaylanmasına yönetimin katılım düzeyi
- Düzenlemelere başvurmada sorumlulukların açıklığı
- Alternatif düzenlemelerin FSA, piyasalar, müşteri ve/veya kullanıcı/üyelere iletilmesine yönelik stratejinin yeterliliği

Planın niteliği

- Firmanın işi ve risklere duyarlılığının dikkate alınmasına ilişkin planın uygunluğu (örneğin; fiziki yerleşim, esneklik sağlayan sistemler, piyasadaki rol ve takas mekanizmaları)
- Temel personel ve ekipmanının alternatif yerleşimlerine ilişkin düzenlemelerin yeterliliği
- Yedekleme ve kurtarma sistemlerine ilişkin düzenlemelerinin yeterliliği
- Mevcut piyasa pozisyonlarının oluşturulması ve uygun zamanlama ile çözülmesine ilişkin prosedürler

Testler

- Test etme sıklığı
- Test kapsamı
- Testlerden çıkarılan dersler

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	**37. Karapara aklanmasının önlenmesi ile ilgili kontroller**

Karaparanın aklanmasının önlenmesi ile ilgili kontrollerin yapısı ve etkinliğinden kaynaklanan riskler; raporlama görevlisinin etkinliği, eğitim, müşteri ve/veya kullanıcı/üyenin tanınması, işin tanınması, iç ve dış raporlama düzenlemeleri ve kayıt tutma düzenlemeleri.

Politika
- Dahili politikalara ilişkin klavuzun yeterliliği
- Klavuzun dağıtımı
- Daha yüksek riskli yargı alanlarına ilişkin güncel bilgilerin dahil edilmesi işlevi
- Karaparanın aklanmasının önlenmesine ilişkin yasal düzenlemelerdeki değişikliklerin dahil edilmesi işlevi
-

Karaparanın aklanmasının önlenmesi ile ilgili raporlama görevlisi
- Organizasyon yapısı içindeki düzeyin uygunluğu
- Görev ve sorumlulukların açıklığı
- Nitelik ve deneyim
- Kayıtlara erişim

Eğitim
- Eğitim verilen personelin deneyimi
- Sıklık
- Kullanılan materyalin niteliği ve bütünlüğü
- Eğitim alan personelin kapsamı

"Müşterini tanı" prosedürleri
- Ad ve adreslerin doğrulanmasına ilişkin prosedürlerin yeterliliği
- Müşteri profili politikasının yeterliliği
- "Müşterini tanı" işlevinin uygunluğu

Şüpheli işlemelerin tanınması
- Şüpheli durum tanımı
- İncelenecek işlemlerin tanınmasına ilişkin sistem ve işlevler
- Şüpheli işlemlerin ele alınmasına ilişkin prosedürler
- Şüpheli işlemlerin raporlanmasına ilişkin prosedürler

Kayıt tutma
- Hesap açma belgelerinin yeterliliği
- Belgelerin saklanma süresi
- İşlem kayıtlarının ve denetim sürecinin yeterliliği

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	38. Piyasanın temizliği

Firmanın faaliyette bulunduğu piyasanın kötüye kullanımına karşı hassasiyetinden kaynaklanan riskler; kötü, haksız, hileli ve onursuz ticari işlemler ve piyasadaki uygulama sorunlarıyla işbirliği yapılması.

Yatırımcılar için genel koruyucu önlemler

- İmkanların kötü ve uygunsuz amaçlar için kullanımının önlenmesine ilişkin önlemler
- Hile ve kötü yönetim, cüretkar davranışlar, imkanların yetersizliği veya kullanıcılar tarafından ihmaline karşı yatırımcıların korunması
- Kullanıcıların imkanları ne şekilde kullandıklarını izlemelerini temin etmek üzere bilgi sağlanması
- Kullanıcıları araştırma yapmaya teşvik edecek düzenlemeler
- Kullanıcıların yasal ve düzenleyici yükümlülüklerle uyumlu hareket etmesini temin edecek düzenlemeler
- İmkanların yasal ya da düzenleyici yükümlülüklerin aksine kullanılması riskinin azaltılmasına ilişkin düzenlemeler

Finansal suç ve piyasanın kötüye kullanımı

- FSA ve İngiltere ya da sınır ötesinde finansal suçların ya da piyasanın kötüye kullanımının ortaya çıkarılması, önlenmesi, takip edilmesiyle ilgili diğer kurumların kamuya bilgi vermesine izin veren kurallar
- Normal olmayan ticari işlemler için imkanların kullanımının izlenmesi için düzenlemeler
- Finansal suç ya da piyasanın kötüye kullanımına ilişkin muhtemel örneklerle ilgili iletişimin sağlanmasına ilişkin düzenlemeler
- Finansal suçların önlenmesinde ilgili kurumlar arasınsa işbirliği

Standartların korunması ve yükseltilmesi

- Eşit rekabet koşullarında doğru ticaret yapılmasıyla ilgili yüksek standartların korunması ve yükseltilmesi için kurallar (örneğin, Piyasa Yönetim Kuralları)
- FSA ve diğer ilgili kurumların işbirliğine izin verilmesi ve uygun işbirliğinin düzeyi hakkında kurallar

Disiplin

- Uygulamanın kurallara uyumunun sağlanmasına ve izlemeye ilişkin düzenlemeler
- Takas düzenlemelerine uyumun uygulanması ve izlenmesi için düzenlemeler

Risk Grubu	Risk Unsuru
Dahili sistemler ve kontroller (Kontrol riski)	**39. Ödeme ve takas düzenlemeleri**

Döviz, takas evleri ya da diğer temel piyasa şirketlerine dair yapılan işlemlere taraf olanların hak ve yükümlülüklerinin zamanında yerine getirilmesine ilişkin düzenlemelerin işleyişinden kaynaklanan riskler.

Ödeme ve takas hizmetleri

- Takas ve/veya ödemeler ile ilgili kurallar ve uygulamalar
- Ticari eşleştirme düzenlemeleri
- Dağıtım ve ödeme düzenlemeleri
- Marj ve teminat düzenlemeleri
- Temerrüde düşme hallerinin belirlenmesi ve çözümü için düzenlemeler
- Üye ödemelerinin izlenmesi
- Ödeme kayıtlarının izlenmesi

Risk Grubu	Risk Unsuru
Yönetim kurulu, üst yönetim ve personel (Kontrol riski)	40. Yönetim yapısı

Firmanın yönetim yapısının özelliklerinden kaynaklanan riskler; yönetim kurulunun, icracı olmayan yöneticilerin ve komitelerinin rolü ve etkinliği.

Yönetim Kurulunun (ya da eşdeğeri olan idari organ) yapısı, rolü ve etkinliği

- Yönetim kurulu ve alt komitelerin yapısı ve başvurma koşulları
- Yönetim kurulunun ve alt komitelerin oluşumu, üyelerin yetkileri
- Toplantı sıklığı, bilginin niteliği ve zamanındalığı, toplantı kayıtlarının geçerliliği
- Yönetim, anlama, izleme ve firmanın faaliyetleri ile risklerin denetim düzeyi, idari yönetime eleştiri getirebilme
- Yetkilendirme veya tanıma yükümlülüklerine ilişkin asgari koşullarla (eşik koşullar) uygunluğun sağlanmasını temin edecek şekilde prosedürlerin yeterliliği
- İyi yönetişime ilişkin kurallara bağlılık
- Yönetime ilişkin düzenlemelerinin yapısı (yabancı sermayeli firmalar için tüzel kişilik yönetimini içermek üzere)

İdareci olmayan yöneticiler

- İdareci olmayan yöneticilerin icracı yöneticiler içindeki payı
- Atanma, terfi ve görev süresi tanımları
- Yetenek ve deneyim
- İdareci yönetime karşı uygun eleştirilerde bulunabilme ve bağımsız karar verme yeteneğinin kullanılması isteği ve yeteneği
- Atama, ücretlendirme ve denetim komitelerine katılım düzeyi
- İdari yöneticilerle ilişkilerin yapısı

Denetim ve Uyum Komitesi

- Yönetim ve referans koşulları
  - kuralların açıklığı, yönetim kurulu alt komiteleri ve başvuru koşulları gibi
  - iç denetim/uyum için öncelikli bir planın uygulanması ve geliştirilmesinin izlenmesindeki rolü
  - onaylanmış risk yönetim politikaları ve prosedürlerinin etkin olarak uygulanmasının ve iç denetimlerin yapılmasındaki rolü
- Raporlama akışı ve oluşum
  - iç denetim ve uyuma ilişkin raporlama akışının iç denetim ve uyum komitesinden bağımsız olması
  - denetim ve uyum komitesinin icracı olmayan başkanı
  - işin yapısına uygun olarak icracı olan ve olmayan diğer yöneticilerin deneyimleri ve yönetimdeki ağırlıkları

- **Operasyon**

– toplantıların sıklığı
– iç denetimden uyum biriminden yapılan raporlamanın niteliği
– toplantıların yönetimi, materyal konularla ilgilenilmesi ve idari yönetime üstünlük sağlayacak deliller sunulması
– idari yönetim olmaksızın bağımsız denetçilerle yıllık toplantılar yapılması
– tanımlanmış güçsüzlüklerle ilgili idari yönetimin hazırlıklı aksiyonları

Risk Grubu Yönetim kurulu, üst yönetim ve personel (Kontrol riski)	Risk Unsuru 41. Yönetim sorumluluklarının tanımı ve dağılımı

Yönetim sorumluluklarının tanımı ve dağılımından kaynaklanan riskler, sorumlulukların etkin biçimde delegasyonu

Yönetim yapısı

- Firmanın faaliyetlerinin izlenmesi, uygun sistem ve kontrollerin oluşturulması ve yönetiminin izlenmesi de dahil olmak üzere yönetim sorumluluklarının açıklığı, tanımı ve belgelenmesi
- Matris yapısı içinde sorumlulukların dağıtılması mekanizması
- Yasal kişiliğe ilişkin sorumlulukların etkin olarak yönetilmesinin temin edilmesine ilişkin araçlar
- İş birimleri ve fonksiyonel birimler arasındaki etkileşimin etkinliği
- İş prensiplerinin uygun olarak dağılımına göre sorumluluklara ilişkin yükümlülükler
- Kontrol fonksiyonundaki yetkili kişilerin doğruluk ve uygunluğuna ilişkin gerekliliklerin kesintisiz karşılanmasını teminen gerekli araçların ve rollerini uygun biçimde sürdürmelerini sağlayacak yetkilerin olması

Delegasyon

- Delegasyonun düzeyi
- Delege edilmiş yetkilerin belgelenmesi
- Üst yönetimin delege edilmiş kararları izlemesini temin edecek araçların olması
- Yetkisi olmayan kişilerin firma adına işlem yapma ya da karar almalarının engellenmesine yönelik araçların olması

İletişim

- Firma içinde yönetsel sorumluluklara ilişkin bilgi akışının ve bu bilgilerin anlaşılmasının sağlanmasına yönelik araçlar

Risk Grubu	Risk Unsuru
Yönetim kurulu, üst yönetim ve personel (Kontrol riski)	**42. Yönetimin niteliği**

Yönetimin niteliğinden kaynaklanan riskler; yönetimin deneyimleri, iş ve idari organın faaliyetleri ile uygunluk.

Deneyim ve bütünlük

- Deneyim, nitelikler ve teknik yetenek
- Kontrol fonksiyonundaki yetkili kişilerin doğruluk ve uygunluğuna ilişkin gerekliliklerin kesintisiz karşılanmasını teminen gerekli araçlar
- Geçmiş deneyim ve kayıtlar
- Etik standartlar üzerindeki pozisyon ve bütünlük
- Baskın bireylerin varlığını da içermek üzere liderlik biçimleri

İş ile uygunluk

- Sektörün yer aldığı piyasada önemli konuların anlaşılması
- Sorumlu oldukları iş ya da kontrol alanlarında temel konuların anlaşılması
- Yönetim, anlama, izleme ve firmanın faaliyetleri ile risklerinin denetim düzeyi, idari yönetime karşı eleştiri getirebilme

İdari organın işleyişi

- Yönetim kurulu ile ilişkiler (Yönetim kurulundan ayrı komite ise)
- Toplantıların sıklığı
- Üyeler arasında eleştiri yapabilme derecesi ve iş ile ilgili temel konularla ilgilenilmesi

Risk Grubu	Risk Unsuru
Yönetim kurulu, yönetim ve personel (Kontrol riski)	**43. İnsan kaynakları**

İnsan kaynakları ile ilgili konulardan kaynaklanan riskler, terfi, ücret, eğitim, disiplin prosedürleri ve kaynakları.

Politika

- Eğitim ve yeterlilik rejimine bağlı kalınması için prosedürler

Kaynakların yeterliliği

- İş stratejisi ile ilişkilendirilerek personelin yeterliliğinin değerlendirilmesine yönelik süreçler
- Kilit noktalardaki personele güven
- Personel kaynakları üzerinde baskı (part-time personel kullanımı dahil)
- Personel kaybına karşı acil durum planları

Personel alımı

- Personel alım politikası
- İl alanlarına bağlantılar

Eğitim

- İş ihtiyaçlarına bağlantı
- İç kurallar ve prosedürlerle uygunluğu temin etmek üzere eğitimlerin yeterliliği
- FSA kuralları ile uygunluğu temin etmek üzere eğitimlerin yeterliliği

Ücret politikası

- Personel ücret ve istihdam rejimi
- Ödüllendirmenin kullanımı ve ödüllendirmeden kaynaklanabilecek risklerin kontrol edilmesi ve izlenmesi
- Hisse opsiyon planlarının kullanımı

Disiplin

- Disiplin prosedürlerinin yeterliliği

Risk Grubu	Risk Unsuru
İş (ticari faaliyet) ve uyum kültürü	**44. Düzenleyicilerle ilişkiler**

Kurumun FSA ve diğer düzenleyici otoriteler ile ilişkilerinin yapısından kaynaklanan riskler; (düzenlemelere ilişkin yakın geçmişi içermek üzere)

Davranış-tutum

- Düzenlemelere karşı genel tutum
- FSA ve diğer düzenleyici otoritelerle ilişkilerin yapısı
- Düzenleyici ile iletişimin açıklığı, doğruluğu ve zamanındalığı
- Düzenleyici tarafından talep edilen bilgilerin sağlanmasındaki isteklilik
- Düzenleyici tarafından talep edildiğinde üst düzey personelin geri çekilmesi
- Düzenleyicilerin güncel konu ve gelişmelerden haberdar olmalarını sağlama yeteneği ve isteği

Düzenlemelere ilişkin geçmiş

- Düzenleyici tarafından ortaya çıkarılan konuların tanımlanmasındaki hız ve etkinlik
- Kuralların ihlal edilmesinin boyutu ve yapısı
- FSA ve diğer düzenleyici otoriteler tarafından alınan disiplin önlemleri

Risk Grubu	Risk Unsuru
İş (ticari faaliyet) ve uyum kültürü	**45. İş ahlakı ve kurum kültürü**

Firmanın faaliyette bulunduğu kültürel çevreden kaynaklanan riskler; uyum konusuna ve firmanın etik kurallara göre faaliyet gösteremeyeceği koşullara/risklere karşı yönetimin yaklaşımı.

Kurum içi kültür

- Kurum içi kültürün yapısı ve açıklığı
- Kültürün oluşturulmasına icracı yönetimin katılım derecesi
- Kültürün izlenmesi sürecine yönetim kurulunun katılım derecesi
- İş ahlakının görünümü ve etik politikaların yapısı
- Önemli kurumsal değişikliklerin takibi ve kurum kültürünün izlenmesi ve değerlendirilmesi süreci

Risk ve kontroller

- Risk ve kontroller arasındaki denge
- Düzenleyici kurallara, prensiplere ve klavuzlara uyum sağlamadaki tutum

Müşteri ve/veya kullanıcı/üye

- Finansal ürünlerin müşterilerce daha iyi anlaşılmasını sağlamak da dahil olmak üzere müşterilere karşı tutum
- Satış kültürü
- Müşteri ve/veya kullanıcı/üye şikayetlerine/ilgilerini cevaplandırmaya hazır olmak

Hissedarlar

- Hissedarlara karşı tutum
- Halka açıklık ve kamu hissedarlarının yönetimi

Ek: 3 Olasılık Derecelendirme Matrisi (Örnek Tablo)

Risk grupları	Risk unsurları	Finansal Başarısızlık (1 ve 8)		Yanlış Davranış/Kötü Yönetim (2 ve9)		Tüketici Bilinci (7 ve 12)		Yanlış Davranış/Kötü Yönetim (3 ve 13)		Piyasanın Kötüye Kullanımı (3,10,14)		Karaparanın aklanmasının önlenmesi (3 ve 15)		Piyasa Yapısı (4 ve 11)	
Strateji	Stratejinin niteliği	**D**		**D**		**VERI YOK**		**D**		**D**		**VERI YOK**		**D**	
	İşin yapısı	**D**		**D**		**VERI YOK**		**D**		**D**		**VERI YOK**		**D**	
Strateji derecesi		L		D		VERI YOK		D		D		VERI YOK		D	
Strateji derecesi-						VERI YOK						VERI YOK			
Piyasa, kredi, sigorta ve faaliyet riski	Kredi riski	D		VERI YOK		VERI YOK		D		VERI YOK		VERI YOK		D	
	Sigorta riski	D		D		VERI YOK		VERI YOK		VERI YOK		VERI YOK		VERI YOK	
	Piyasa riski	D		VERI YOK		D		VERI YOK		VERI YOK		VERI YOK		D	
	Faaliyet riski	D		D		VERI YOK		D		D		D		D	
	Yasal risk	D		VERI YOK		D		D		VERI YOK		VERI YOK		D	
Piyasa, kredi, sigorta ve faaliyet riski derecesi		D		D		D		D		D		D		D	
Piyasa, kredi ve faaliyet riski-															
Finansal yapının sağlığı	Sermaye yeterliliği	D		D		VERI YOK		D		D		D		D	
	Likidite	D		D		VERI YOK		D		D		D		D	
	Karlılık	D		VERI YOK		VERI YOK		D		D		D		D	
Finansal yapının sağlığına ilişkin derece		D		D		VERI YOK		D		D		D		D	
Finansal yapının sağlığı-															
Müşteri/kullanıcı ve ürün/hizmet yapısı	Müşteri/kullanıcı/üye çeşidi	VERI YOK		D		D		D		VERI YOK		D		D	
	İşin kaynakları ve dağıtım kanalları	VERI YOK		D		D		D		D		D		D	
	Ürün ve hizmet çeşitleri	VERI YOK		D		D		D		D		D		D	
	Piyasa etkinliği	VERI YOK		VERI YOK		D		D		D		VERI YOK		D	
	Uygun piyasalar	VERI YOK		VERI YOK		D		D		VERI YOK		VERI YOK		D	
Müşteri, ürün, hizmet derece		VERI YOK		D		D		VERI YOK		D		D		D	
Müşteri, ürün, hizmet derece								L							

D: düşük

Risk grupları	Risk unsurları	Finansal Başarısızlık (1 ve 8)	Yanlış Davranış/Kötü Yönetim (2 ve9)	Tüketici Bilinci (7 ve 12)	Yanlış Davranış/Kötü Yönetim (3 ve 13)	Piyasanın Kötüye Kullanımı (3,10,14)	Karaparanın aklanmasının önlenmesi (3 ve 15)	Piyasa Yapısı (4 ve 11)
Müşteri/kullanıcı yönetimi	Satış esasına dayalı eğitim ve istihdam	VERI YOK	D	D	VERI YOK	VERI YOK	VERI YOK	VERI YOK
	Satış esasına dayalı eğitim ve istihdamın temeli	VERI YOK	D	D	D	VERI YOK	VERI YOK	VERI YOK
	Finansal teşvik	VERI YOK	D	D	VERI YOK	VERI YOK	VERI YOK	VERI YOK
	Müşteri/kullanıcı kabulü, danışmanlık verilmesi ve raporlama	VERI YOK	D	D	VERI YOK	VERI YOK	VERI YOK	D
	İş ve yönetim	VERI YOK	D	D	D	D	VERI YOK	D
	Müşteri/kullanıcı aktiflerinin güvenliği	VERI YOK	D	D	D	VERI YOK	VERI YOK	D
	Ürün literatürünün yeterliliği, kamuoyuna açıklama	VERI YOK	D	D	VERI YOK	VERI YOK	VERI YOK	VERI YOK
	Üyelik düzenlemeleri	D	VERI YOK	D	D	D	VERI YOK	D
Müşteri/kullanıcı yönetimi derecesi		D	D	D	D	D	VERI YOK	D
Müşteri/kullanıcı yönetimi								
Organizasyon	Yasal/ mülkiyet yapısının açıklığı	D	VERI YOK	VERI YOK	D	D	VERI YOK	D
	Hukuk/kontrol edenlerin özellikleri/ Grup varlıkları	D	VERI YOK	VERI YOK	D	D	D	D
	Grubun geri kalanıyla ilişkiler	D	D	VERI YOK	D	D	D	D
Organizasyon derecesi		D	D	VERI YOK	D	D	D	D
Organizasyon								
Dahili sistemler ve kontroller	Risk yönetimi	D	VERI YOK	D	D	D	VERI YOK	D
	Politika, prosedür ve kontroller	D	VERI YOK	D	D	D	VERI YOK	D
	Yönetim bilgisi	D	D	D	D	D	VERI YOK	D
	IT sistemleri	D	D	D	D	D	VERI YOK	D
	Finansal ve düzenleyici raporlama, muhasebe politikaları	D	VERI YOK	D	VERI YOK	VERI YOK	VERI YOK	VERI YOK
	Uyum	D	D	VERI YOK	D	D	D	D
	İç denetim	D	D	D	D	D	D	D
	Dış kaynak kullanımı (outsource)üçüncü kişi sunucular	D	D	D	D	VERI YOK	VERI YOK	D
	Profesyonel danışmanlar	D	D	D	D	D	VERI YOK	VERI YOK
	İş sürekliliği	D	D	VERI YOK	VERI YOK	VERI YOK	VERI YOK	D
	Karaparanın aklanmasının önlenmesi kontrolleri	VERI YOK	VERI YOK	D	VERI YOK	VERI YOK	D	VERI YOK
	Piyasanın temizliği	VERI YOK	D	VERI YOK	D	D	D	D
	Mutabakat düzenlemeleri	D	VERI YOK	VERI YOK	VERI YOK	VERI YOK	VERI YOK	D
Dahili kontrol derecesi		D	D	VERI YOK	D	D	D	D
Dahili kontroller				D				
Yönetim kurulu, yönetim, personel	Kurumsal yönetim	D	D	VERI YOK	D	D	D	D
	Yönetim yetki ve sorumluluklarının tanımı ve dağıtılması	D	D	VERI YOK	D	D	D	D
	Yönetim kalitesi	D	D	D	D	D	D	D
	İnsan kaynakları	D	D	D	D	D	D	D
Yönetim kurulu, vb. derecesi		D	D	D	D	D	D	D
Yönetim kurulu, vb.								
İş ve uyum kültürü	Düzenleyici otorite ile ilişkiler	D	D	D	D	D	D	D
	İş etiği ve kültürel sorunlar	D	D	D	D	D	D	D
Kontrol kültürü derecesi		D	D	D	D	D	D	D
Kontrol kültürü derecesi								

Ek 5: Derecelendirme Özeti

Hedeflere Yönelik Risk Grupları	Finansal Başarısızlık (1 ve 8)	Yanlış Davranış/ Kötü Yönetim (2 ve9)	Tüketici Bilinci (7 ve 12)	Yanlış Davranış/ Kötü Yönetim (3 ve 13)	Piyasanın Kötüye Kullanımı (3,10,14)	Karaparanın aklanmasının önlenmesi (3 ve 15)	Piyasa Yapısı (4 ve 11)
Risk Grupları							
Strateji	**D**	**D**	**Veri yok**	**D**	**D**	**Veri yok**	**D**
Piyasa, kredi, sigorta ve faaliyet riski	**D**	**D**	**D**	**D**	**D**	**D**	**D**
Finansal sağlık	**D**	**D**	**Veri yok**	**D**	**D**	**D**	**D**
Müşteri/kullanıcı ve/veya ürün/hizmet yapısı	**Veri yok**	**D**	**D**	**D**	**D**	**D**	**D**
TOPLAM İŞ RİSKLERİNİN DERECESI	**D**	**D**	**D**	**D**	**D**	**D**	**D**
Müşteri/kullanıcı yönetimi	**D**	**D**	**D**	**D**	**D**	**Veri yok**	**D**
Organizasyon	**D**	**D**	**Veri yok**	**D**	**D**	**D**	**D**
Dahili sistemler ve kontroller	**D**	**D**	**D**	**D**	**D**	**D**	**D**
Yönetim kurulu, üst yönetim ve personel	**D**	**D**	**D**	**D**	**D**	**D**	**D**
İş ve uyum kültürü	**D**	**D**	**D**	**D**	**D**	**D**	**D**
TOPLAM KONTROL RİSKİ DERECESI	**D**	**D**	**D**	**D**	**D**	**D**	**D**
HER GRUP İÇİN OLASILIK DERECESI	**D**	**D**	**D**	**D**	**D**	**D**	**D**

D: Düşük

Yasal Hedeflere Göre Dereceler

Yasal hedef	Etki (drived impact)	Etki (impact override)	Öneri no. (override comment)	Olasılık (derived probability)	Olasılık (probability override)	Öneri no. (override comment)
Tüketicinin korunması				D		
Kamu bilinci				D		
Finansal suçların azaltılması				D		
Piyasa güveni				D		

Ek 6: Risk Azaltma Programı İçin Örnek (ABC Şirketi)

Sorunun yapısı	Sorunun ilgili olduğu firmalar	Beklenen sonuç	Eylem	Zaman çizelgesi
E-ticaret alanında firmanın uzmanlığı sınırlıdır. Bir web sayfasının açılmasıyla birlikte, etkin IT güvenliği sağlanmaması, firma ve müşterilerini etkileyecek olan sanal bir suç riskinin artmasına neden olacaktır.	ABC Şirketi	Müşterileri ve firmayı hile riskine karşı korumak üzere IT önlemleri alınması.	FSA, web sayfasının IT güvenlik kontrolleri ile ilgili daha fazla bilgi edinmek ve bu kontrollerin nasıl gerçekleştirildiğini test etmek ve dışardan ne tür danışmanlık alındığını görmek için web sayfası proje müdürünü ziyaret edecektir.	I/2003
Karapara aklanmasının önlenmesi konusunda raporlama yetkilisi yeni müşteriler için yetersiz müşteri sınıflandırma bilgisinin elde edildiğini belirtmiştir. Bu da firmayı karaparanın aklanmasına karşı kırılgan hale getirmektedir.	ABC Şirketi	Firma aracılığıyla karapara aklanması riskinin azaltılması için tüm müşterilere (eski ve yeni) ilişkin müşteri sınıflandırması hakkında yeterli bilgi edinilmesi	Firma hesap açma prosedürlerini inceleyecek ve bunlarla ilgili aksaklıkları işaret edecektir.	II/2003
Firma yeterli şekilde satışa yönlendirici eğitimleri izleyememekte ve uyum fonksiyonunun dışardan yürütülmesi, satış uygulamalarına ilişkin yetersiz uyum izlemesine neden olmaktadır. Sonuç olarak firma geliştirdiği daha karmaşık yatırım ürünlerinin hangi müşteri için uygun olacağına karar verme yeteneğinde değildir.	ABC Şirketi	Sadece uygun müşterilere karmaşık ürünlerin satılmasına dayalı satış eğitimi ve firmanın faaliyetine uygun politika ve prosedürlerin olması, uyum fonksiyonu için gerekli personelin sağlanması.	Firmanın satış esasına dayalı eğitimlerine ilişkin izleme sürecinin incelenmesi ve tanımlanan sorunlara işaret edilmesi sağlanacaktır. FSA, FSMA bölüm 166'ya göre uyum fonksiyonunun etkinliği, ilgili politika ve prosedürler hakkında bir uzman raporu talep etmektedir. Firmanın tanımlanan her türlü soruna işaret etmesi sağlanacaktır.	III/20003 III/2003
Firmanın risk tabanlı iç denetim fonksiyonu bulunmamakta, bu da daha yüksek riskli fonksiyonların zamanında incelenememesine yol açmaktadır.	ABC Şirketi	Firmanın karşılaştığı temel riskler için Yönetim Kurulu ve üst yönetime güvence verecek yapıda iç denetim fonksiyonunun olması.	Firma uygun olduğu ölçüde dışarıdan uzmanlar kullanarak risk tabanlı denetim metodolojisi oluşturacak ve uygulayacaktır. FSA uzman grubu, revize edilmiş metodolojilerin etkinliğini ölçmek için firmayı ziyaret edecektir.	IV/2003 I/2004
Firma içinde operasyonel riskin tanımlanması, izlenmesi ya da yönetimine dair sistematik bir çerçeve bulunmamaktadır.	ABC Şirketi	Yönetim kurulu/üst düzey yönetimin firmanın karşılaştığı temel faaliyet risklerinin farkında olması ve bunların azaltılması için gerekli kontrollerin yerleşmesinin sağlanması.	Firma operasyonel risklerin tanımlanması, ölçülmesi ve izlenmesi için uygun işlevleri oluşturacaktır.	IV/2004