

Sermaye piyasası aracı kurumlarında bilgi sistemleri ve bu sistemlerden kaynaklı operasyonel riskler

Dr. İZZET GÖKHAN ÖZBİLGİN*

İş Geliştirme ve Analiz Grup Başkanı Sermaye Piyasası Kurulu

İzzet Gökhan Özbilgin 1998 yılında ODTÜ Elektrik-Elektronik Bölümü'nden şeref listesinde mezun olmuş, daha sonra aynı bölümde yüksek lisansını tamamlamıştır. Akademik çalışmalarına devam ederek ikinci yüksek lisansını işletme alanında tamamlamış, devamında iç kontrol, denetim, operasyonel risk alanlarında çalışarak doktor unvanını almıştır. Aynı yıl iş hayatına da katılan Dr. Özbilgin, çeşitli özel kuruluşlarda sistem mühendisi, ağ mühendisi, güvenlik uzmanı gibi görevlerde bulunduktan sonra 2002 yılında Sermaye Piyasası Kurulu Bilgi İşlem Dairesi'nde göreve başlamıştır. Halen bu birimde Grup Başkanı olarak çalışan Dr. Özbilgin'in uluslararası ve ulusal yayımlanmış birçok eseri bulunmaktadır.

Bilgi ve iletişim teknolojilerinde yaşanan bu hızlı değişim sağladığı yararların yanında bazı riskleri de beraberinde getirmiştir. Önceden yazılı gerçekleştirilen işlemler elektronik ortama taşındığından bu işlemlerin izlenmesi, kontrol altına alınması ve denetlenmesi güçleşmiş, sistemler daha karmaşık bir yapıya dönüşmüştür.

1. Giriş

Bilgi ve iletişim teknolojilerinde meydana gelen gelişmeler ile bu teknolojilere ilişkin maliyetlerdeki düşüşler sermaye piyasası faaliyetlerinin geleneksel yöntemlerin yanı sıra bilgi ve iletişim teknolojilerine dayalı gerçekleştirilmesine olanak sağlamıştır. Uzaktan erişim imkânı sonucunda borsa ve takas işlemlerinin hızları artmış, işlem maliyetleri gerilemiş, operasyonel işlemler otomatik hale getirilmiştir. Özellikle internetin yaygınlaşması ile bölgesel sınırlar ortadan kalkmış, yatırımcılar aracı kuruma gitmeden veya telefon etmeden işlemlerini gerçekleştirebilir hale gelmiş, herhangi bir aracıya ihtiyaç duymadan piyasa verilerine ve bu bilgileri analiz eden araştırma raporlarına, portföy analiz programlarına, kamunun aydınlatılmasına yönelik dokümanlara ulaşabilmişlerdir. İnternet aynı zamanda halka arzların elektronik ortamda gerçekleştirilmesine imkân tanımış, halka arzlarda internet üzerinden talep toplanabilmesini, böylece zamandan tasarruf edilmesini sağlamıştır.

Bilgi ve iletişim teknolojilerinde yaşanan bu hızlı değişim sağladığı yararların yanında bazı riskleri de beraberinde getirmiştir. Önceden yazılı gerçekleştirilen

işlemler elektronik ortama taşındığından bu işlemlerin izlenmesi, kontrol altına alınması ve denetlenmesi güçleşmiş, sistemler daha karmaşık bir yapıya dönüşmüştür. Bu durum işletmelerin bilgi ve iletişim teknolojileri ile ilgili risklerinin türlerini değiştirmiş, işlemlerini elektronik ortamda gerçekleştirmeye başlayan kuruluşların denetiminde sadece bu sistemlerden elde edilen veriler değil, aynı zamanda bu verileri oluşturan bilgisayar sistemlerinin, bu sistemler üzerindeki işlem ve uygulamaların düzenli ve güvenli bir şekilde çalışması gerekliliğini ortaya çıkarmıştır.

Finansal sistemin önemli kurumlarından bankaların bilgi sistemlerine ve bu sistemlerden kaynaklı operasyonel risklere ilişkin çalışmalar literatürde yer almaktadır. Buna karşın sermaye piyasalarında aracılık faaliyetini yerine getiren aracı kurumlar için benzer çalışmalara literatürde rastlanmamaktadır. Bu kapsamda sermaye piyasalarında bir güven kurumu olarak faaliyet gösteren aracı kurumların bilgi sistemlerine dayalı faaliyetlerinin düzenlenmesi önemlidir. Bu çalışma aracı kurumların bilgi sistemleri hakkında bilgi vermesi ve bilgi sistemlerine ilişkin operasyonel risklerin incelemesi bakımından yapılmış ilk

Bu çalışma aracı kurumların bilgi sistemleri hakkında bilgi vermesi ve bilgi sistemlerine ilişkin operasyonel risklerin incelemesi bakımından yapılmış ilk çalışmadır.

çalışmadır.

2. Aracı Kurumların Bilgi Sistemlerine Genel Bakış

Sermaye piyasalarında yaşanan gelişmeler, yeni bilgi ve iletişim teknolojileri, internetin artan kullanımı, finans piyasalarındaki ürün ve hizmetlerdeki değişimler aracı kurumları önemli ölçüde etkilemektedir. Özellikle internet üzerinden yoğun işlem yapan, merkez dışı birim sayısı ve işlem hacmi yüksek olan aracı kurumlarda bu etki daha çok görülebilmektedir.

Bilgi sistemlerindeki ilerlemeler ve internet

net üzerinden işlem süreçlerinin gelişmesi telefon aracılığıyla emirlerin aracı kuruma iletilmesi döneminde yaşanan yetersizlikleri, özellikle işlem hacminin arttığı dönemlerde yaşanan erişim sorunlarını büyük ölçüde ortadan kaldırmıştır. Herhangi bir müşteri temsilcisi ile muhatap olmaksızın doğrudan emirlerini iletmek isteyen ve yatırım tavsiyesi talep etmeyen veya ihtiyaç duymayan aktif yatırımcılar, internet üzerinden gerçekleştirilen işlemlerle büyük avantajlar sağlamıştır. Bu durum sadece müşteriler için değil, aracı kurumlar için de avantajlar sağlamış, aracı kurumların daha düşük bedellerle hizmet sunabilmelerini kolaylaştırmıştır.

dece müşteriler için değil, aracı kurumlar için de avantajlar sağlamış, aracı kurumların daha düşük bedellerle hizmet sunabilmelerini kolaylaştırmıştır.

Ülkemizde faaliyet gösteren aracı kurumların bilgi sistemleri hakkında genel bilgi vermeye bu kurumların bilgi işlem bölümleri ve bu bölümlerde çalışanlardan başlanabilir. Bu kapsamda, Tablo 1’de verilen veriler incelendiğinde 2007 yılında faaliyet göstermekte olan 99 aracı kurumun 65’inde bilgi işlem çalışanı bulunurken; 2009 yılında bu veri 89 aracı kurumun 62’si şeklinde değişmiştir. Ayrıca aracı kurumların içinde internet üzerinden emir alanların sayısı 2007 yı-

	2007	2008	2009
Toplam Aracı Kurum Sayısı	99	98	89
Banka Kökenli Aracı Kurum Sayısı	31	31	30
Banka Kökenli Olmayan Aracı Kurum Sayısı	68	67	59
İnternet Üzerinden İşlem Yapan Aracı Kurum Sayısı	68	69	64
Bilgi İşlem Çalışanı Bulunan Aracı Kurum Sayısı	65	62	62
Toplam Çalışanların Bilgi İşlem Departmanında Bulunma Oranı	%3,1	%3,6	%3,9
Aracı Kurumlarda Ortalama Bilgi İşlem Çalışan Sayısı	2,8	3	3

İşlem Hacmi (milyar TL)	2007	2008	2009	Değişim (2007-2009)
Toplam Hisse Senedi İşlem Hacmi	776	665	965	%24
İnternet Üzerinden Hisse Senedi İşlem Hacmi	55	62	137	%149
Toplam VOB İşlem Hacmi	211	378	587	%178
İnternet Üzerinden VOB İşlem Hacmi	24	73	151	%529

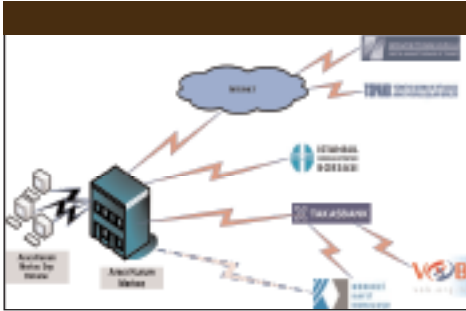
lında 68 iken; bu sayı 2009 yılında 64’e düşmüştür. Aracı kurum sektörünün bilgi işlem çalışanı bakımından durumu incelendiğinde ise 2009 yılında 62 aracı kurumda bilgi işlem çalışanı bulunduğu, bu sayının 2007 yılından bu yana neredeyse sabit bir seyir gösterdiği görülmektedir. Bir başka deyişle, teknolojinin çok önemli olduğu bu sektörde aracı kurumların üçte birinde bilgi işlem personeli bulunmamaktadır. Bilgi işlem personeli bulunmayan ve 1 tane bilgi işlem çalışanı olan aracı kurumlar birlikte ele alındığında ise bu rakam aracı kurumların yaklaşık %60’ını oluşturmaktadır. Aracı kurumlarda çalışanların 2009 yılı itibarıyla %3,9’u bilgi işlem bölümlerinde görev yapmakta ve bilgi işlem bölümleri ortalama 3 kişiden oluşmaktadır.

Aracı kurumların internet üzerinden gerçekleştirdikleri işlem hacimleri ile ilgili veriler ise Tablo 2’de sunulmakta olup, 2007 yılından itibaren toplam aracı kurum ve internet üzerinden işlem yapan aracı kurum sayısında azalma olmasına rağmen aracı kurumların internet üzerinden gerçekleştirdikleri işlem hacimlerinde çok büyük artışlar olmuştur. 2009 yılında Vadeli İşlem ve Opsiyon Borsası A.Ş. (VOB)’da yapılan işlemlerin yaklaşık dörtte biri, hisse senedi işlemlerinin de yaklaşık yedide biri internet üzerinden yapılmıştır. 2008 yılında toplam hisse senedi işlemlerinin %9’u, 2009 yılında ise %14’ü internet üzerinden gerçekleşmiştir. 2007-2009 yılları arasında toplam hisse senedi işlem hacmi %24 artarken, internet üzerinden gerçekleşen hisse senedi işlem hacmi

yaklaşık %149 oranında büyük bir artış göstermiş, böylece bölüm bazında en büyük artış bu kanaldan yapılan işlemlerde gerçekleşmiştir. Benzer süreç VOB işlemlerinde daha da yüksek yaşanmış ve vadeli işlemler ele alındığında bölüm bazında işlem hacmi gelişiminde en önemli değişim yine internet kanalıyla yapılan işlemlerde olmuştur. 2008 yılında internet üzerinden yapılan vadeli işlemlerin payı bir önceki yıla göre 8 puan artarak %19’a, 2009 yılında 7 puan artarak %26’ya yükselmiştir. İnternet üzerinden gerçekleşen VOB işlemleri 2007 yılından 2009 yılına kadar %529 oranında artmış, aracı kurumların bu işlemlerde her geçen yıl internete yöneldiği görülmüştür.

Aracı kurumların bilgi işlem bölümleri ve internet üzerinden gerçekleştirdikleri işlemler hakkında 2007-2009 yıllarını kapsayan bu verilerin yanında, bu kurumların bilgi sistemleri altyapılarının incelenmesi de ayrı bir önem taşımaktadır. Bu altyapıların iyi bir şekilde analiz edilmesi gerek yapılacak düzenlemelerin gerekse bu sistemleri de içine alacak kontrollerin doğru ve etkin olmasını sağlayacaktır.

Aracı kurumların bilgi sistemleri açısından en önemli süreçlerinden biri elektronik ortam kullanılarak alım satım işlemlerinin gerçekleştirilmesidir. Elektronik ortamda alım satım aracılığını kolaylaştıracak şekilde İstanbul Menkul Kıymetler Borsası (İMKB)’ye elektronik emir iletimi, ilk olarak 2000 yılında “Disketle Emir İletimi” uygulaması şeklinde başlamıştır. Disketle emir



iletimi, İMKB Hisse Senetleri Piyasasında (HSP) alternatif bir emir iletimi yöntemi olarak, yatırımcıların emirlerini disketle hızlı bir şekilde iletmelerine yönelik geliştirilen bir uygulamadır. Borsa tarafından bu uygulama ilk olarak 2000 yılında sadece 1. seans için yürürlüğe sokulmuş, 2001 tarihinden itibaren ise 2. seansa da disketle emir iletimi mümkün hale getirilmiştir. Daha sonra bu uygulamaya 2002 tarihinden itibaren geçerli olmak üzere “Express Application Program Interface (ExAPI)” yöntemiyle emir gönderimi dahil edilmiştir.

Ex-API, uzaktan erişim projesi kapsamında HSP Elektronik Alım Satım Sistemi ile üyelerin merkezi sistemlerini elektronik bir altyapı aracılığıyla bağlamak, üyelerin bu yapı vasıtasıyla emir işlemlerini elektronik ortamda yürütebilmelerini sağlamak için oluşturulmuş olan bir mesajlaşma arayüzüdür. Bu arayüz, üye sistemi ile HSP Temsilci Ekranı (İMKB ExAPI Bilgisayarı) arasındaki iletişim yöntemlerini ve mesaj yapılarını belirlemektedir. Bu yapı sayesinde üyeler, kendi bilgisayar sistemleri aracılığı ile İMKB Alım Satım Sistemi'ne doğrudan, İMKB Kullanıcı Terminalleri ile klavye ve ekranların kullanılmasına gerek kalmaksızın, kendi bilgisayar sistemleri aracılığı ile erişebilmektedir.

“Disketle Emir İletimi” aşaması ExAPI sisteminin dahil olmasıyla “Elektronik Emir İletimi” aşaması olarak değiştirilmiş, bu aşamanın uygulamaya alınmasıyla bir gün önceki ikinci seansın bitişinden itibaren birikmiş emirlerin sisteme çok hızlı iletilmesi sağlanmıştır. Böylece “Açılış Seansı” ve “2. Seansın Elektronik Emir İletimi Seansı” bölümünde Disket ve ExAPI aracılığı ile sisteme saniyede 6 emir gönderilebilme imkanı oluşmuştur. Bu hız Sürekli Müzayede seansı içerisinde ExAPI ile emir iletiminde saniyede 1-3 arasındadır.

ExAPI uygulamasıyla birlikte her aracı kurum kendi internet sitesinden, şubelerinden veya şirket merkezindeki terminallerinden süre ile kısıtlı kalmaksızın elektronik olarak ileteceği emirleri, sisteminde toplayarak aracı kurum merkez ofisinde bulunan ExAPI terminali aracılığıyla piyasaların açıldığı andan itibaren, İMKB HSP Alım Satım Sistemi'ne elektronik olarak aktarabilmiştir. Bu yöntemle aracı kurumların, müşterilerine daha hızlı hizmet vermesi ve toplanan emirlerin kısa bir süre içerisinde aracı kurum sistemi tarafından öncelik sırasına göre sisteme iletilmesi mümkün olmakta ve ExAPI terminaline gelecek cevap mesajlarının aracı kurum sistemi tarafından işlenmesi sonucunda emir ve işlem teyitleri, hesap bazında detaylı olarak anında izlenebilmektedir.

Aracı kurumların bilgi sistemleri altyapısı olarak uzak ağ altyapısı incelendiğinde bütün aracı kurumların İMKB ve İMKB Takas ve Saklama Bankası A.Ş. (Takasbank) ile özel kiralık hatlar üzerinden direkt bağlantıları bulunmaktadır. Şekil 1’de gösterilen bu bağlantılar genelde yedekli olarak tesis edilmekte, böylece bu kritik hatlarda kesinti yaşanması büyük ölçüde engellenmektedir. Gerçekleştirdikleri işlemler açısından aracı kurumların veri transferinde bulunması gereken diğer kurumlar ise Merkezi Kayıt Kuruluşu (MKK) ve VOB’dur. Aracı kurumların neredeyse tamamı bu iki kuruma Takasbank üzerinden bağlanmakta, az sayıda aracı kurum bu bağlantılarını yedekleyerek bu iki kuruma direkt hat tesis etmektedir. Bundan dolayı, aracı kurumların MKK işlemleri ve türev işlemlerini gerçekleştirebilmeleri Takasbank ile olan bağlantılarının kesilmemesine bağlıdır. Aracı kurumların bu kurumsal bağlantılarının yanı sıra bir diğer uzak alan ağ bağlantısı ise internet bağlantılarıdır. Aracı kurumlar internet üzerinden alım satım işlemleri gerçekleştirmekte, gerek yasal olarak gerekse hizmetlerinin kalitesini arttırmak amacıyla birçok bilgi, belge ve raporları web sayfaları üzerinden duyurmaktadırlar. Aynı zamanda aracı kurumların sermaye yeterliliği tabloları, kamuyu aydınlatma formları, mali tablo ve raporlar gibi yasal olarak hazırlamak zorunda oldukları birçok bilgiyi belli zamanlarda SPK, TSPAKB, İMKB gibi ilişkili oldukları kurumlara internet üzerinden göndermeleri gerekmektedir. Bu nedenle aracı kurumların

internet erişimlerinin sürekliliğinin sağlanması başta elektronik ortamda hizmet veren aracı kurumlar olmak üzere tüm aracı kurumlar için hayati önem taşımaktadır. Bu bakımdan; aracı kurumlar genelde bu bağlantılarını iki farklı hizmet sağlayıcısından iki ayrı alt-yapı ile sağlamış, böylece olası sorun halinde en az bir hattın çalışır durumda kalması, normal çalışma sırasında ise internet şubesine gelen işlemlerin yük paylaşımı yapılarak daha kaliteli bir hizmet sunulması hedeflenmiştir.

Aracı kurumların bilgi sistemlerinde kritik olarak kabul edilebilecek diğer bir husus kul-

landıkları uygulamalar ve veritabanı sistemleridir. Aracı kurumlar bünyelerinde genellikle Windows işletim sistemini tercih etmekte ve bu işletim sistemi üzerinde çeşitli uygulamalar geliştirmekte veya dışarıdan tedarik etmektedirler. Bu uygulamaların içinde en önemlisi, belki de aracı kurumların bilgi sistemleri açısından en değerli varlığı muhasebe uygulamasıdır. Aracı kuruma farklı yollarla gelen tüm sözlü ve yazılı emirler sonunda bu uygulama üzerinden geçip gerekli finansal işlemler ve kontroller yapıldıktan

sonra ilgili borsanın terminali aracılığıyla (örn. ExAPI uygulaması) ile borsaya iletilmektedir. Bu bakımdan aracı kurumların birçoğu bu kritik uygulama ile ilgili yedekleme, yetkilendirme ve erişebilirlik gibi kontrolleri içeren prosedürler hazırlamaktadır. Aracı kurumların muhasebe uygulaması olarak tercih ettikleri uygulamaların başında Geneks (Gendex), IDB (IDB Borsa) veya TradeSoft (ATP, GTP) firmalarının uygulamaları yer almaktadır. Bu uygulamalar aynı zamanda aracı kuruma bağlanan müşterilerin Internet Protocol (IP) numaralarını belirlemek amacıyla da kullanılmaktadır. Bu şekilde elde edilen IP numaraları aracı kurumların büyük

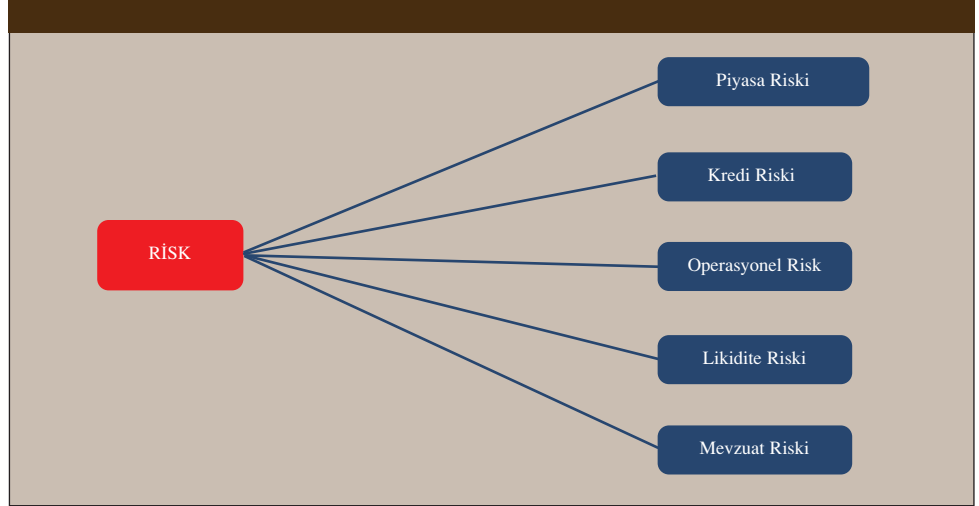
Aracı kurumların internet erişimlerinin sürekliliğinin sağlanması başta elektronik ortamda hizmet veren aracı kurumlar olmak üzere tüm aracı kurumlar için hayati önem taşımaktadır.

çoğunluğunda merkez sunucuda, diğerlerinde ise genellikle CD, DVD gibi veri depolama üniteleri veya kişisel bilgisayarlarda saklanmaktadır. Bilgi sistemleri açısından aracı kurumlarda önem arz eden bir diğer husus müşterilerin bilgilerinin yer aldığı, gerçekleştirilen işlemlerin ve muhasebe bilgilerinin tutulduğu veritabanlarıdır. Aracı kurumlar gerek itibar açısından gerekse yasal zorunluktan dolayı bu bilgilerin güvenliğini sağlamak ve yedeklerini alarak saklamak zorundadırlar.

Aracı kurumlardaki bir diğer önemli husus telefon ve elektronik ortam üzerinden gelen emirlerdir. Müşterilerden gelen tüm emirlerin, müşterilerle yapılan tüm görüşmelerinin detaylı bir şekilde kayıt altına alınması ve raporlanması gerekmektedir. Bu kapsamda aracı kurumların tamamında gelişmiş kayıt sistemleri kullanılmaktadır. Bunun için kullanılan cihazlar incelendiğinde, bu cihazların neredeyse tamamının analog sistemlere destek verecek yapıda olduğu, IP ve dijital cihaz kullanımının henüz tercih edilmediği görülmektedir.

Bilgi sistemleri güvenliği ise özellikle internet üzerinden yoğun işlem yapan aracı kurumlar açısından önem arz etmektedir. Genelde aracı kurumlar müşterilerine hizmet verdiği sunucular ile aracı kurumun kendi yerel ağını güvenlik duvarı (firewall) vasıtasıyla fiziksel olarak ayırmakta, olası bir saldırı veya istenmeyen durum oluştuğunda tüm sistemin etkilenmesini engellemektedirler. Ayrıca müşteri ile aracı kurum arasındaki bağlantıların "Secure Socket Layer (SSL)"¹¹ olması, aracı kurumların neredeyse tamamında gerçekleştirilmektedir.

Aracı kurumların kullandıkları bir diğer



önemli uygulama ise "Kamuyu Aydınlatma Platformu (KAP)"¹²dur. Aracı kurumlar KAP üzerinden sertifika yüklü akıllı kartlarını kullanarak internet yoluyla gerekli bildirimleri (mali tabloları, özel durumları vb.) elektronik imza teknolojisi kullanarak güvenli bir şekilde göndermektedirler.

3. Operasyonel Risk

Finansal kuruluşlar arasında önemli bir yere sahip olan aracı kurumlar faaliyetlerini sürdürürken risklerle karşı karşıya kalabilmekte, bu risklerin doğurabileceği olumsuz sonuçları yaşayabilmekte ve hatta iflas riski ile yüzleşebilmektedirler. Aracı kurumların iflas etmesi diğer ticari işletmelerden farklı olarak sadece aracı kurumun ortaklarının zarar etmesiyle sınırlı kalmayarak, yatırımcıların ve tüm finansal sistemin zarar görmesine yol açabilmektedir. Bu bakımdan; aracı kurumlar, faaliyetlerini sürdürürken karşılaşılabilecekleri riskleri tanımlayıp yaşayabilecekleri olumsuz durumlardan korunmak amacıyla gerekli önlemleri almalıdırlar. Aksi takdirde söz konusu riskler aracı kurumun faaliyetlerinin geçici veya sürekli durdurulmasına, yetki belgelerinin iptaline ve iflas aşamasına kadar gelmesine sebebiyet verilmektedir.

Piyasaların hareketliliği, globalleşme, artan işlem hacmi, karmaşık finansal ürünler ve işlem şekilleri, gelişen bilgi ve iletişim teknolojileri yeni finansal riskler doğurmuştur. Finansal kuruluşların karşılaştıkları bu riskleri genel anlamda piyasa riski, kredi riski ve operasyonel risk olarak sınıflandırmak

mümkündür. Bununla birlikte; IOSCO, bu sınıflandırmayı detaylandırıp likidite riski ile mevzuat riskini ayrı ele alarak riskleri Şekil 2'de görüldüğü gibi beş gruba ayırmış, böylece daha etkin bir risk yönetimi gerçekleştirilebileceğini belirtmiştir.

Görüldüğü üzere finansal kuruluşların karşılaştığı risklerden biri de operasyonel risk olup, aslında tüm risklerden daha eski ve temel bir risk olmasına rağmen bu risk ile ilgili bilincin gelişmesi diğer risklere göre daha geç olmuştur. 1980'li yıllardan itibaren türev araçların yaygın olarak kullanılması, uluslararası finansal piyasalarda yaşanan hızlı gelişim ve değişim, teknolojiye olan aşırı bağımlılık, artan işlem hacimleri, bölgesel ya da global krizler ve terörist saldırılar, bu riskle ilgili çalışmaların hızlandırma gereğini ortaya çıkarmıştır.

Operasyonel riskler, en genel anlamda, piyasa ve kredi riski gibi finansal riskler dışında kalan tüm riskler olarak tanımlanmıştır. Ancak bu tanım çok geniş kapsamlı olduğundan ve aslında operasyonel riskin ne olduğu değil, ne olmadığını açıkladığından operasyonel riskin yönetimi açısından açık bir fikir vermemektedir. Basel II ile birlikte operasyonel riskler için sermaye bulundurulması zorunlu hale getirilmiş ve operasyonel riskin yeni tanımı "yetersiz veya başarısız iç süreçler, insanlar, sistemler ya da dışsal olaylar sonucu ortaya çıkan zarara uğrama riski" şeklinde yapılmıştır. Uluslararası geçerli bu tanım, operasyonel risklerin kaynaklarına odaklanmakta ve operasyonel risklerin insanlar, süreçler, sistemler ve dışsal olaylar

olmak üzere başlıca dört kaynaktan gelebileceğini kabul etmektedir (Altıntaş, 2006: 461-462). IOSCO Teknik Komitesi ise 1998 yılında yayınlamış olduğu “Aracı Kurumlar ve Düzenleyici Otoriteler için Risk Yönetimi ve Kontrolü” başlıklı raporunda, operasyonel riski “işlem süreçlerinin ve yönetim sisteminin uygun işlememesi sonucu finansal zarara uğrama riski” olarak tanımlamaktadır. Basel Komitesi tarafından belirtilen ve operasyonel riskin kaynaklarını oluşturan dört unsur “Personel”, “Bilgi Sistemleri”, “Süreçler” ve “Dış Olaylar” olarak sıralanmıştır.

4. Aracı Kurumların Bilgi Sistemlerinden Kaynaklı Operasyonel Riskler

Bilgi sistemlerinden kaynaklı operasyonel riskler kurumun sistemlerinde iç veya dış kaynaklı etkenlere bağlı olarak meydana gelen aksaklıkların neden olduğu risklerdir. Son yıllarda finans kurumları rekabete ayak uydurmak, ürün seçeneklerini arttırmak, müşteriye daha hızlı ve kolay hizmet sunmak için teknoloji konusuna oldukça önem vermekte, bu hizmetleri sağlayacak sistemleri bünyelerinde kurmaktadır. Ancak bu sistemlerde oluşabilen iletişim hatlarının kesilmesi, yedekleme sistemindeki yetersizlikler veya zararlı kodlar gibi aksaklıklardan dolayı finans kurumları zarar görebilmektedir. Özellikle internet üzerinden işlem gerçekleştiren veya bünyelerinde farklı yazılım ve işletim sistemlerine sahip kurumların bu tür risklerle karşılaşma olasılığı daha fazladır. Bundan dolayı, bu tür kurumların bilgi sistemleri güvenliğine ayrı bir önem vermeleri, güvenlik duvarı, şifreleme gibi uygulamaları hayata geçirmeleri gerekmektedir. Aksi takdirde sistemlerde çeşitli aksaklıkların ortaya çıkması sonucunda kurumun önemli bir itibar ve müşteri kaybına uğraması söz konusudur. Sistemden kaynaklanan bu tür operasyonel kayıp türüne bir örnek, 1995 yılında bir Rus bilgisayar korsanının, Citibank’ın sistemindeki bir boşluktan yararlanarak bankanın sistemine girmeyi başarması ve tüm müşterilerin hesap hareketlerine ulaşmasıdır.

Aracı kurumlar sermaye piyasası mevzuatı gereğince yazılı dökümlerini almakla birlikte muhasebe, arşiv, kamuyu aydınlatma gibi birçok sürecini bilgi sistemlerine yüklemişler, başta vadeli işlemlere ait emirler olmak üzere iletilen emirlerde internet ve tele-

fon yoluyla emir alımını tercih etmişlerdir. Bu kapsamda aracı kurumlar önceki bölümde genel olarak açıklanan bilgi sistemlerini kurmuş ve yönetmeye başlamışlardır. Böylece aracı kurumlar işlemlerinde bilgi sistemlerini kullanarak daha hızlı, kaliteli ve ucuz hizmet verebilmişlerdir. Ancak işlemlerin bu ortama taşınması beraberinde çeşitli riskler getirmiştir.

Aracı kurumların bilgi sistemleri kullanmasından kaynaklanan risklerin arasında aracı kurumlarda yaşanan ispat sorunu gelmektedir. “Aracılık Faaliyetinde Belge ve Kayıt Düzeni Hakkında Tebliğ (SPK Seri: V, No:6 sayılı Tebliğ)”in 9. ve 17. maddelerinde müşterilerden telefon ve benzeri iletişim araçları ile emir alınabileceği, bu emirlerde ispat yükünün aracı kuruluşa ait olduğu, ancak müşteri mutabakatını içermeyen aracı kuruluş kayıtlarının tek taraflı delil oluşturamayacağı, aracı kuruluşların bu tip emirleri müşteri imzası aranmaksızın yazılı hale getirmeleri gerektiği hususu düzenlenmiştir. Bu sebeple, internet üzerinden alınan emirlerde aracı kurumun bilgisayar kayıtları ile mutabakat unsurları birbirini teyit ettiği takdirde aracı kurum kayıtları delil olarak kullanılabilir. Menkul kıymet alım satımı gerçekleştiren yatırımcılar tarafından imzalanacak müşteri emir formları Hukuk Usulü Muhakemeleri Kanunu’nun 287. maddesi uyarınca kesin delil niteliğindedir. Buna karşın internet üzerinden alınan müşteri emirlerinin bilgisayar kayıtları yazılı hale getirilse bile, müşteri imzasını taşıması nedeniyle kesin delil olarak nitelendirilmesi mümkün gözükmemektedir. Bu durum elektronik ortamda emir iletimi sürecinde suistimaller oluşabilmesine yol açmaktadır. Çalışmamızın bir önceki bölümünde sıralanan standart yazılımları kullanan aracı kurumlarda bu tür risklerin oluşma ihtimali oldukça azalmış olmakla birlikte, kendi yazılımlarını kullanan veya emrin iletilmesi sürecinde yazılıma manuel müdahaleye imkân yaratan kurumlarda bu tür olaylar olasıdır.

Aracı kurumlar için risk taşıyan bir diğer husus aracı kurumların uzak alan ağ bağlantılarıdır. Aracı kurumların özellikle internet, İMKB ve Takasbank ile olan uzak alan ağ bağlantılarının kesintiye uğramaması gerekmektedir. Aracı kurumlar internet üzerinden emir almakta, yatırım danışmanlığı, portföy yöneticiliği gibi hizmetler sağlamakta ve ser-

maye piyasası mevzuatı gereğince internet sayfalarında çeşitli duyurular yayımlamaktadırlar. Aracı kurumların internet dışında İMKB ve Takasbank ile olan bağlantılarını da sürekli aktif tutacak önlemleri almaları gerekmektedir. Özellikle elektronik ortamda alım satım hizmeti veren aracı kurumlar ExAPI terminalini kullanarak İMKB’ye erişmekte ve aracılık faaliyetlerini yerine getirmektedirler. Aynı zamanda aracı kurumun internet sayfasını kullanarak emir ileten müşterilerin istekleri de bu yolla borsaya eriştiğinden, bu hat ve ExAPI terminali kesintiye uğramamalıdır. Aracı kurumların aynı zamanda faaliyetlerini yerine getirebilmeleri için Takasbank ile de gün içinde sürekli iletişim halinde bulunmaları gerekmektedir. Bu bağlantı aynı zamanda MKK ve VOB A.Ş.’ye erişimi de sağladığından bu hatın sürekliliği önem kazanmaktadır.

Aracılık hizmetlerinde gerek kasıtlı gerekse istemeyerek yapılan müşteri kaynaklı bilgi güvenliği ihlalleri başka bir operasyonel risk kaynağıdır. Aracı kurumlar müşterilerini güvenlik önlemleri hakkında yeterince bilgilendirmedikleri zaman bu risk daha da artabilmektedir. Kişisel bilgilerini, hesap numaralarını gerektiği biçimde koruyamayan, aracı kuruma erişim sırasında kullandıkları bilgisayarlarda gerekli güvenlik önlemlerini almayan müşteriler aracı kurumlar için risk yaratabilmektedir. Bu tür müşterilere ait bilgileri ele geçiren kötü niyetli kişiler gerek müşteriyi gerekse aracı kurumu zora sokacak faaliyetlerde bulunabilmektedirler. Burada dikkat edilmesi gereken bir diğer konu bilişim suçları ve bu konuda yürürlükte olan kanun ve düzenlemelerdir. Örneğin, 2006 yılında yaşanan bir olayda kötü niyetli bir kişi; bilgisayarının güvenliğini sağlamayan, sanal klavye uygulama-

Menkul kıymet alım satımı gerçekleştiren yatırımcılar tarafından imzalanacak müşteri emir formları Hukuk Usulü Muhakemeleri Kanunu’nun 287. maddesi uyarınca kesin delil niteliğindedir. Buna karşın internet üzerinden alınan müşteri emirlerinin bilgisayar kayıtları yazılı hale getirilse bile, müşteri imzasını taşıması nedeniyle kesin delil olarak nitelendirilmesi mümkün gözükmemektedir.

masını kullanmayan, havale işlemlerini sınırlandırarak parola kullanımını aktif hale getirmeyen bir banka müşterisinin şifresini ele geçirerek kendi hesabına para aktarmış, böylece banka müşterisini mağdur etmiştir. Bunun üzerine banka müşterisi banka aleyhine dava açmış ve açılan dava sonucunda Yargıtay; bir güven kurumu olarak faaliyet gösteren bankayı, müşterisinin haberi olmadan başka bir hesaba para aktarılmasının önlenmesi konusunda ek güvenlik tedbirlerini almadığı için kusurlu bulmuştur.² Aracı kurumların da internet üzerinden hizmet verdiği düşünülürse benzer risk aracı kurumlar için de geçerlidir. Çalışmamızın 1.bölümünde belirtildiği üzere HSP Alım Satım Sistemi ile aracı kuruma ait ExAPI arasında kurulan iletişimin güvenliği İMKB tarafından sağlanmakta, HSP Alım Satım Sistemine ulaşan her mesajın, ilgili aracı kurum tarafından yollanıp yollanmadığı kontrol edilmektedir. Buna karşın aracı kurumun sistemine izinsiz girilerek HSP Alım Satım Sistemine mesajlar iletilirse, bu mesajlar aracı kuruma ait ExAPI tarafından

Aracı kurumun sistemine izinsiz girilerek HSP Alım Satım Sistemine mesajlar iletilirse, bu mesajlar aracı kuruma ait ExAPI tarafından yollandığı için öngörülen güvenlik önlemlerini aşıp, İMKB tarafından geçerli bir mesaj kabul edilecek ve sisteme ulaşabilecektir. Bu nedenle aracı kurumların, kendi sistemlerinin güvenliğini sağlayacak önlemleri almaları gerekmektedir.

yollandığı için öngörülen güvenlik önlemlerini aşıp, İMKB tarafından geçerli bir mesaj kabul edilecek ve sisteme ulaşabilecektir. Bu nedenle aracı kurumların, kendi sistemlerinin güvenliğini sağlayacak önlemleri almaları gerekmektedir. Bu kapsamda, aracı kurumların da müşterilerine ilişkin kimlik doğrulama sırasında bankalarda olduğu gibi “Tek Kullanımlık Güvenli Şifre (OTP/One Time Password)” kullanımını gerçekleştirmeleri önemlidir.

Aracı kurumların bilgi sistemlerinde yaşanabilecek bir diğer riskli durum işlem hacminin artması sonucu bilgisayarların saklama ve işlem kapasitelerinin yetersiz kalması,

işlem hızının yavaşlaması veya durmasıdır. Aracı kurumlar yatırım danışmanlığı, kamu-yu aydınlatma gibi birçok hizmetini internet üzerinden vermekte, müşterilerinden internet aracılığıyla emir almaktadırlar. İşlem hacminin yoğun olduğu zamanlarda internet üzerinden verilen bu hizmetlerin yavaşlaması veya durması, muhasebe uygulamasının bulunduğu sunucunun yetersiz kalması gibi problemler müşteri taleplerinin karşılanamamasına, dolayısıyla aracı kurumun faaliyetlerinin kesintiye uğramasına yol açmaktadır.

Aracı kurumların bilgi sistemlerinden dolayı karşılaşılabilecekleri bir diğer risk ise itibar riskidir. Sistemlerin veya sunulan hizmetlerin umulduğu şekilde çalışmaması itibar riski yaratabilmekte ve olumsuz kamu tepkisine neden olabilmektedir. İtibar riski ayrıca bir hizmet ile sorunlar yaşayan ancak sorunun çözülmesinde yeterli bilgi verilmeyen müşterilerin bulunduğu durumlarda da ortaya çıkabilmektedir. Örneğin, internet kesintisi yaşandığında alternatif iletişim yollarının bulunmadığı veya duyurulmadığı durumlarda, müşterilerin memnuniyetsizlikleri

daha da artabilmektedir. Unutulmaması gereken bir diğer durum ise itibar riskinin tek bir aracı kurumu değil, tüm finansal sistemi etkileyebileceğidir. Örneğin internet üzerinden alım satım hizmeti veren bir aracı kurum müşteri bilgilerinin gizliliğini sağlayamadığında veya internet erişiminin kesildiğinde bir itibar riski oluşabilecek, bu durum diğer aracı kurumların güvenliği de sorgulanabilir hale getirecektir.

Bilgi sistemlerinden kaynaklanan riskler değerlendirilirken ele alınması gereken bir diğer husus ise dışarıdan hizmet alımıdır. Finans sektöründe yaygın bir eğilim, stratejik olarak ana faaliyetler üzerinde odaklanmak ve kendi uzmanlık alanına girmeyen konular için diğer kuruluşlardan yardım almaktır. Benzer şekilde aracı kurumların bazıları da bilgi sistemlerinin işletilmesi için dışarıdan hizmet almakta, böylece bilgi işlem maliyetlerini azaltmak ve bu sistemlerden kaynaklanan riskleri transfer etmektedirler. Ancak dışarıdan hizmet alınması yeni riskler getirebilmektedir. Aracı kurumun sistemlerine, özellikle müşteri bilgilerinin bulunduğu ve-



ritabanına kurum personeli olmayan birinin erişimi aracı kurum için büyük bir risktir. Ayrıca hizmet sağlayıcılar aracı kurum tarafından talep edilen hizmetlerin sağlanması için gerekli uzmanlığa sahip olmayabilirler veya teknolojilerini zamanında yenileyemeyebilirler. Bu şekilde hizmet sağlayıcının bilgi sistemlerinin durması aracı kurumun ürün ve hizmetleri sunabilmesini tehlikeye sokabilir.

5. Sonuç

Bilgi ve iletişim teknolojilerindeki ilerlemeler, internetin artan kullanımı, finans piyasalarındaki ürün ve hizmetlerdeki değişimler aracı kurumları bilgi teknolojilerine dayalı kuruluşlar haline getirmiştir. Aracı kurumların güvenilir bir ortamda çalışması sermaye piyasasında istikrarı sağlamak için gerekli koşullardan biridir. Bu koşulun sağlanmadığı ortamda tasarruf sahipleri zarar görebilecek, sermaye piyasasına duyulan güven sarsılabilecek ve tasarruf oranı azalarak finansal sektör ile reel sektör arasındaki aracılık süreci bozulabilecektir. Bu nedenle sermaye piyasasında bir güven kurumu olarak faaliyet gösteren aracı kurumların bilgi sistemlerinden kaynaklı operasyonel risklerinin yönetilmesi gerekmektedir.

Aslında aracı kurumlardan gerek kuruluş aşamasında gerekse faaliyetlerini yürütürken bilgi sistemleri ile ilgili kontrolleri tamamlamaları, etkin sistemler kurlmaları ve bu hususları yazılı hale getirmeleri istenmiştir. Bununla birlikte; aracı kurumların bilgi sistemlerine verdikleri önem henüz yeterli düzeye erişmemiş olup, faaliyetlerinde bilgi sistemleri ve interneti kullanan aracı kurumlar bu konularda gerekli ve yeterli kontrolleri tam olarak oluşturmamışlardır.

Bu kapsamda, aracı kurumların gerek müşterilere gerekse ilgili kurumlara göndereceği tüm belgelerde elektronik imza kullanması, ayrıca aracı kurumların sadece gönderecekleri belgelerde değil, elektronik ortamda düzenledikleri ve saklamak zorunda kaldıkları tüm bilgi, belge ve defterleri elektronik imza kullanarak arşivlemeleri değerlendirilmelidir. Böylece yasal zorunluluklar yerine getirilmiş, verilerin değiştirilemez bir biçimde uzun bir süre saklanabilmesi sağlanmış, yapılacak denetimlerde geçmiş verilere erişilmesi ile bu verilerin analiz edilmesi süreci

kolaylaştırılmış ve kısaltılmış, ispat problemlerinin aşılmasında ilerleme kaydedilmiş ve büyük bir kâğıt maliyetinden kurtulmuş olunabilir.

Aracı kurumların üçte birinde bilgi işlem çalışanı olmadığı ve iç denetim sistemi kapsamında çalışan kişi sayısının genelde düşük olduğu dikkate alınırsa bütün aracı kurumlarda bilgi sistemleri denetimi maliyetli olabilir. Bunun yerine aracı kurumlarda sınıflandırmaya gidilerek, örneğin internet üzerinden işlem hacmi belli bir düzeyde olan veya merkez dışı örgüt sayısı belli rakama ulaşan aracı kurumlarda güvenlik taraması hizmetinin zorunlu tutulması gibi hususlar ele alınarak aracı kurumların bilgi sistemlerine yönelik bir düzenleme yapılması değerlendirilebilir. Bu düzenlemede aracı kurumların bilgi sistemlerinde bulunması gereken asgari unsurlara yer verilip, iç denetçilerin bilgi sistemleri denetimi sırasında hangi usul ve esasları aramaları gerektiği belirtilebilir.

Aracı kurumların müşteri verilerinin bulunduğu sistemlerin yedeklerini belli periyotlarda almaları, bu yedeklerin örneğin SEC 17a-3 ve SEC 17a-4'de belirtildiği gibi silinmez, değiştirilemez medyalar alınması, bu yedeklerin orijinallerinden başka yerlerde tutulması ve indekslenmesi aracı kurumların iş sürekliliği açısından önemli olacaktır. Ayrıca aracı kurumlar dış kaynaklardan hizmet almaktan doğan riskleri sınırlayacak politikalar benimsemelidir. Aracı kurum yönetimi kendilerine hizmet sağlayanların operasyonel ve mali performansını izlemeli, taraflar arasındaki beklentilerin açıkça anlaşılmasını, yükümlülüklerin yazılı ve uygulanabilir sözleşmelerde tanımlanmasını sağlamalıdır. Dışarıdan hizmet alma, aracı kurumun hassas bilgileri hizmet sağlayıcı ile paylaşmasını gerektirebilir. Aracı kurum yönetimi, hizmet sağlayıcının hassas verileri korumayı hedefleyen politika ve prosedürlerini inceleyerek, güvenlik açısından hizmet sağlayıcının faaliyetlerini kurum içinde yapıyor mu gibi değerlendirmelidir. Bu şekilde; bilgi sistemlerinden kaynaklı risklerin yönetildiği aracı kurumlar sayesinde sermaye piyasalarına olan güven artacak, süreçlere hız, gizlilik süreklilik, bütünlük, izlenebilirlik gibi hususlar eklenebilecektir.

Kaynakça

Altıntaş, M. Ayhan, "Bankacılıkta Risk Yönetimi ve Sermaye yeterliliği", Ankara, Turhan Yayınevi, 2006.

IOSCO, "Risk Management and Control Guidance for Securities Firms and Their Supervisors", A Report by the Technical Committee of the International Organization of Securities Commissions, 1998.

İMKB, "Sermaye Piyasası ve Borsa Temel Bilgiler Kılavuzu", 2008.

Kınık, Tevfik, "Elektronik Finansın Gelişimi Karşısında Aracı Kuruluşlar", SPK Yeterlilik Etüdü, Ekim 2002, Ankara.

Leblebici Teker, Dilek; Ülegin, Başak, "Bankacılıkta Operasyonel Risk Ölçüm Modellerinin Türk Bankacılık Sektöründe Faaliyet Gösteren bir Bankaya Uygulanması" İstanbul, İTÜ Dergisi Cilt: 2, Sayı: 1, 2005.

Mazıbaşı, Murat, "Operasyonel Riske Basel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme", Ankara, Araştırma Raporları: 2005/1, BDDK, 2005.

Özbilgin, İzzet Gökhan, "Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar", Sayıştay Dergisi, Sayı: 49, 2003.

TSPAKB, "Aracı Kuruluşların Faaliyetleri", Yıllık Rapor, 2008.

TSPAKB, "Aracı Kuruluşların Faaliyetleri", Yıllık Rapor, 2009.

Dipnotlar

¹Çalışmada yer alan görüşler yazarın kendisine aittir.

²SSL (Secure Sockets Layer): İnternet üzerinde iki taraf arasında oluşan trafiğin şifrelenerek, bilgini gizliliğinin ve bütünlüğünün korunmasını sağlayan bir protokoldür.

Aracı kurumların müşteri verilerinin bulunduğu sistemlerin yedeklerini belli periyotlarda almaları, bu yedeklerin örneğin SEC 17a-3 ve SEC 17a-4'de belirtildiği gibi silinmez, değiştirilemez medyalar alınması, bu yedeklerin orijinallerinden başka yerlerde tutulması ve indekslenmesi aracı kurumların iş sürekliliği açısından önemli olacaktır.