Denetişim
Ortak Aklın Harmanı

KURUMSAL RİSK YÖNETİMİNİN RİSKLERİ

(RISKS OF ENTERPRISE RISK MANAGEMENT)

Halis KIRAL*

ÖZ

Risk yönetimine ilişkin yapılan çalışmalarda, Worldcom ve Enron skandallarından küresel finansal krize kadar birbirinden farklı krizlerin ortak sebebi olarak risk yönetiminde yaşanan eksiklik veya yanlışlıklara dikkat çekilmektedir. Risk yönetiminin önemine ilişkin bu teşhis doğru olmakla beraber risk yönetimi genel metodolojisinin ya da bu alanda yayımlanan standart ve çerçevelerin bu krizlerin ortaya çıkmasını neden önleyemediği ya da diğer bir ifadeyle tedavi edemediği sorusu halen cevaplanmayı beklemektedir. Ülkelerin ya da kurumların özel koşulları dikkate alınmadan verilen genel reçetelerin ne oranda tedavi edici olacağı da bu sorunun cevabı aranırken mutlaka dikkate alınmalıdır. Bu çalışmada, risk yönetimine ilişkin uluslararası bilgi ve tecrübe birikimini yansıtmakla birlikte, ülkelerin kendine özgü koşullarından bağımsız olarak hazırlanan standart ve çerçevelerin, ülkelerin veya sektörlerin kendi gerçekleri ile tamamlanmadığı durumlarda, kurumsal risk yönetimi yaklaşımının karşı karşıya kalması muhtemel riskler irdelenmektedir.

Anahtar Kelimeler: Durumsal Risk Yönetimi, Kurumsal Risk Yönetimi, Her Şeyin Risk Yönetimi, İç Kontrol

JEL Kodlaması: H11, H12, M40

ABSTRACT

The studies on risk management highlight the shortcomings or mistakes in risk management as the common reason for various crises from Worldcom and Enron scandals to the global financial crisis. While such diagnosis regarding the importance of risk management is correct, the question remains: why the general methodology of risk management or the standards and frameworks published in this field cannot prevent emergence of these crises or i.e. cure them. The extent to which general prescriptions given without considering the special conditions of countries or institutions can have a curing effect should also be taken into account, when seeking answer to this question. This study examines the risks that the enterprise risk management approach may face in case the standards and frameworks which are prepared regardless of the specific conditions of the countries are not completed with the realities of the countries or sectors, although they reflect international knowledge and experience on risk management.

Keywords: *Situational Risk Management, Enterprise Risk Management, Risk Management of Everything, Internal Control.*

JEL Classification: *H11, H12, M40*

*) Dr. Öğr. Üyesi, Denetim ve Risk Yönetimi Ana Bilim Dalı Başkanı, (CIA, CCSA, CGAP), Ankara Sosyal Bilimler Üniversitesi, Ankara, halis.kiral@asbu.edu.tr, Orcid:0000-0001-7022-872X, Yazı Gönderim Tarihi: 19.11.2018, Yazı Kabul Tarihi: 29.11.2018

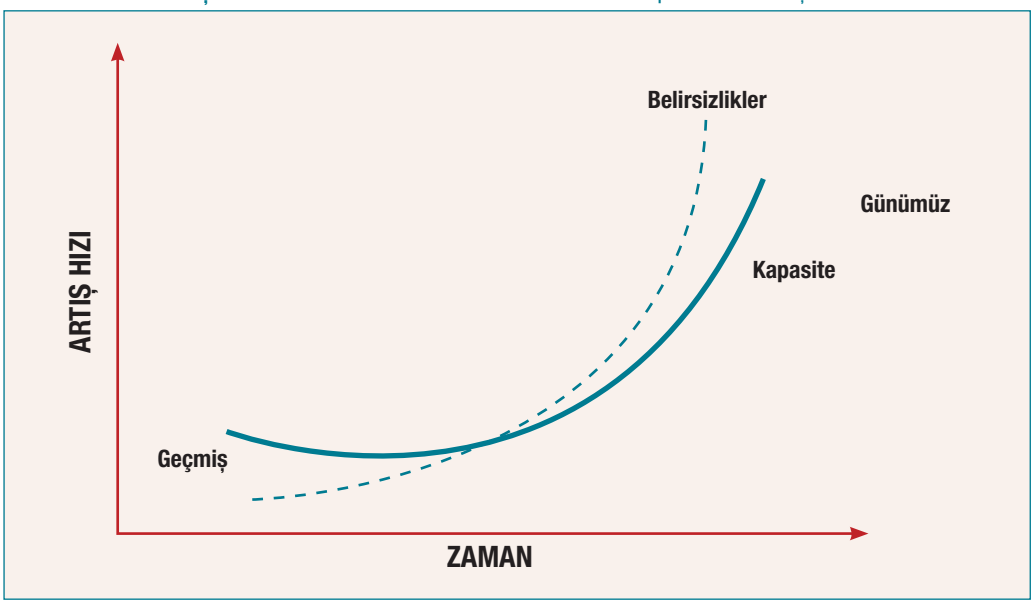
1. GİRİŞ

Hayat risklerle doludur. Her gün insanlar sonuçların önemli olduğu, ancak kararları etkileyen koşulların az ya da çok belirsiz bir ortamda karar almaya çalışırlar (Murray-Webster ve Hillson, 2008). Modern dönem öncesinde insanların karşı karşıya kaldıkları belirsizlikler günümüze kıyasla daha sınırlı olduğundan, insanların bu belirsizliklerle mücadele kapasiteleri daha yüksek olmuştur. Nitekim, henüz birkaç nesil öncesine kadar her bireyin toplum içerisinde kendisine biçilen rolü kabullendiği, birçok insanın mesleğinin babadan oğula geçtiği veya ailesinin toplumdaki konumuna göre belirlendiği bir dünyada, toplumun büyük bir bölümünün yaşamlarının geri kalanında nelerle karşılaşacaklarını kestirebilmelerinin makul sınırlar dâhilinde mümkün olduğu ifade edilebilir (Hillson, 2009). Her ne kadar depremler, yanardağ patlamaları, fırtınalar ve sel gibi doğal afetlerden kaynaklı belirsizlikler her zaman var olsa da, nükleer savaş, küresel ısınma, çevresel felaketler, siber saldırılar ve biyoterör gibi riskler dikkate alındığında modern hayatın eskiye göre daha fazla belirsizlik barındırdığı da bir gerçektir (Furedi, 2001).

Riskler denetlenebildiği ve yönetilebildiği sürece hayatın olağan akışında esaslı bir sorun teşkil etmezler (Power, 2004). Ancak, insanoğlunun risklere karşı mücadelede elde ettiği yetkinlik ya da diğer bir ifadeyle risk yönetiminde sağlanan ilerlemeler, günümüzde toplumun her kesiminin karşı karşıya kaldığı risklerdeki (veya risk algısındaki) artışın oldukça gerisinde kalmıştır. Bu bakımdan, karşı karşıya kaldığımız risklerin, bu riskler ile mücadele kapasitemizin çok üzerine çıktığı rahatlıkla ifade edilebilir (bkz. Şekil 1).

Belirsizlik ve riskler, riskler ile mücadele kapasitemizin üzerine çıkarak risk yönetiminin etkinliğini sınırlamaktadır. Riskler ile mücadele kapasitemizin üzerinde olan riskler denince akla gelen ilk örneklerden biri, kuşkusuz, ekonomik kriz riskidir. Ekonomik kriz ister gelişmiş ekonomilerde isterse gelişmekte olan ekonomilerde olsun, her an karşı karşıya kalınması muhtemel önemli bir risktir. Aslında ekonomik krizin ortaya çıkması ekonomik risklerin etkin olarak yönetilememesinin bir sonucudur. Bu doğrultuda, risk yönetimine ilişkin yapılan akademik çalışmalarda Worldcom ve Enron skandallarından küresel finansal krize kadar birbirinden farklı krizlerin ortak sebebi olarak risk yönetiminde yaşanan eksiklik veya yanlışlıklar işaret edilmektedir. (McGinn, 2009; O'Donnell, 2009; Price, 2008) Risk yönetiminin önemine ilişkin bu 'teşhis' doğru olmakla beraber risk yönetimi genel metodolojisinin ya da bu alanda yayımlanan standart ve çerçevelerin bu krizlerin ortaya çıkmasını neden önleyemediği ya da diğer bir ifadeyle 'tedavi' edeme-

Şekil 1. Belirsizlikler ile Belirsizliklerle Mücadele Kapasitemizin Gelişimi



Kaynak: Yazar tarafından oluşturulmuştur.

diği sorusu halen cevaplanmayı beklemektedir (Taleb, 2008; Power, 2009; Van der Stede, 2011; Mikes, 2011, Cassar ve Gerakos 2013). Ülkelerin ya da kurumların özel koşulları dikkate alınmadan verilen genel 'reçete'lerin ne oranda tedavi edici olacağı da bu sorunun cevabı aranırken mutlaka dikkate alınmalıdır.

Bu çalışmada[1], risk yönetimine ilişkin ortak aklı ve uluslararası bilgi ve tecrübe birikimini yansıtmakla birlikte ülkelerin kendine özgü koşullarından bağımsız olarak hazırlanan çerçevelerin ülke ve/veya sektörlerin kendi gerçekleri ile tamamlan(a)madığı durumlarda kurumsal risk yönetimi yaklaşımının karşı karşıya kalması muhtemel riskler irdelenmektedir. Bu amaçla, çalışmanın ikinci bölümünde risk ve risk yönetimine ilişkin kavramsal çerçeve genel hatlarıyla verilmektedir. Üçüncü bölümde, kurumsal risk yönetiminin geçirdiği aşamalar aktarılmaktadır. Dördüncü bölümde ise kurumsal risk yönetiminin karşılaşması muhtemel riskler ortaya konulmaktadır.

2. RİSKLER VE YÖNETİMİ

Yüzyıllar boyunca farklı dillerde farklı anlamlar bulan, farklı kültürlerden değişik biçimlerde beslenen ve geçtiğimiz yüzyılın son yarısından itibaren akademik çalışmalara da konu olmaya başlayan 'risk' kelimesinin birbirinden farklı tanımları (Hampton, 2009; Hopkin, 2010; Sweeting, 2011; Stamatis, 2014 vb.) bulunmakla birlikte, tüm tanımların ortak noktası riskin, belirsizlik ve sonuçlar ile yakın ilişkili olmasıdır (Hillson ve Murray-Webster, 2005). Her gün bir yenisi eklenen modern zaman belirsizlikleri dikkate alındığında, etrafımızın sayısız belirsizlikle kuşatılmış olduğu düşünülebilir (Furedi, 2001; Beck, 2014). Ancak söz konusu belirsizliklerin, temel olarak iki ana başlık altında toplanması mümkündür. Bunlar; sonuçları itibariyle önemli olanlar ve sonuçları itibariyle önemli olmayanlar. Belirsizliklerin sonuçları itibariyle sınıflandırılması riske yönelik kavramsal ve anlaşılabilir bir tanım sunar. Buna göre, "risk, sonucu itibariyle önem arz eden belirsizliktir". Hangi belirsizliklerin önemli olup, hangilerinin önemsiz olduğuna ilişkin değerlendirilmesi gereken husus ise, amaçlardır. Bu yönüyle de risk, gerçekleşmesi halinde amaçlara erişilmesine olumlu ya da olumsuz etkisi olan belirsizliktir (Hillson, 2009).

Risk yönetimi ise risklerin tanımlanması, değerlendirilmesi ve etkisinin kabul edilebilir bir seviyede tutulabilmesi için gerekli tedbirlerin alınması, bu tedbirlerin düzenli olarak gözden geçirilmesi ve raporlanmasını sağlayan bir yönetim sürecidir (İDKK, 2013). Kurumsal risk yönetimi ise risk yönetimi süreçlerinin kurumunun tamamında bütünleşik ve koordinasyon içinde uygulanmasını ifade etmektedir.

3. 'DURUMSAL' RİSK YÖNETİMİNDEN KURUMSAL RİSK YÖNETİMİNE GEÇİŞ

Esasında kendimizi güvence altına almaya yönelik aldığımız kararlar ya da tehlikeler karşısında verdiğimiz tepkilerden ibaret olan risk yönetimi, içgüdüsel, sezgisel, canlılar için asli ve canlı beyninin birincil fonksiyonlarından birini teşkil eder (Schneier, 2008). Ancak, risk yönetimi beynin birincil ve en ilkel fonksiyonlarından biri olsa bile sistematik hatalara açık olduğu da bir gerçektir (Kahneman, 2011). Ender olaylara ilişkin olasılıkların yanlış hesaplanması (siyah kuğu teorisi[2]), verilerden ziyade yaygın kanaatlere itibar edilmesi, konfor alanından çıkmamak için gerçeklerin görmezden gelinmesi ve karar verilirken yanlış kapsamın dikkate alınması söz konusu sistematik hatalara örnektir (Schneier, 2008).

Sistematik hatalarına rağmen insanoğlu karşılaştığı riskler karşısında diğer canlılar gibi içgüdüsel olarak sürekli bir savunma mekanizması geliştirmek suretiyle hayatta kalabilmiştir. Genlerimize işlemiş bu savunma mekanizmasını, 'belirsizliklerle mücadele disiplini' olan risk yönetiminin başlangıç aşaması olarak görmek yanlış olmayacaktır (Fraser ve Simkins, 2010). Çoğunlukla sistematik bir yöntem teşkil etmeyen bu aşamada, genellikle sağduyu, tecrübe ve içgüdüler ile anlık 'duruma' yönelik risk yönetiminden bahsedilebilir (Merna ve Faisal, 2008).

'Durumsal' risk yönetiminin 'kurumsal'laşması ve bir disiplin olarak ortaya çıkmasının izleri ise II. Dün-

1) Bu çalışmaya görüş ve önerileriyle katkıda bulunan Sayın A. Koray Kazancı, Sayın Ersin Kurnaz, Sayın Evren Ermisket ve Sayın Özgür Satıcı'ya teşekkür ederim.
2) Siyah kuğu teorisi, Nassim Nicholas Taleb'in çok satan "The Black Swan" kitabı ile hayatımıza girmiş finansal bir terim ve bir teoridir. Taleb, etkisinin çok büyük şoklara neden olabileceği ve tahmin edilmesi pek de mümkün olmayan ender olayları Siyah Kuğu'ya benzetir.

ya Savaşını takip eden dönemde görülmeye başlanmış olup, modern risk yönetiminin ilk örneklerine bu dönemde rastlanılmıştır. Risk yönetimine ilişkin akademik anlamdaki ilk kitaplar olan 1963 yılında Mehr ve Hedges tarafından yazılan Ticari İşletmelerde Risk Yönetimi (Risk Management in the Business Enterprise) ile 1964 yılında Williams ve Heins tarafından yazılan Risk Yönetimi ve Sigorta (Risk Management and Insurance), risklerin basitçe yönetilmesine odaklanmış ve yalnızca kurumların finansal risklerini dikkate almıştır.

1980'lerin sonu ve 1990'ların başı işletmeler açısından hem karşılaşılan risk türlerinin arttığı hem de risk yönetiminin giderek önem kazandığı dönemlerdir. 1990'larda, risk yönetiminin uygulama alanı, finansal risklerin yanı sıra operasyonel riskleri de kapsayarak genişlemiş ve özellikle halka açık şirketlerde kurumsal risk yönetimi konuları daha fazla gündeme gelmiştir. İlk Risk Yönetimi Başkanı (Chief Risk Officer – CRO) da bu dönemde görevlendirilmiştir (Hopkin, 2010).

2000'li yılların başında Worldcom ve Enron skandalları genel anlamda dünya finans çevrelerinde ve özel olarak risk yönetimi disiplininde yeni bir döneme girilmesine neden olmuştur. 2001 yılı Aralık ayında iflas etmesinden önce Amerika'nın en yenilikçi, en hızlı büyüyen ve en iyi yönetilen şirketlerinden biri olarak kabul edilen, beyan edilen yıllık geliri 1990'ların başlarında 10 milyar dolar civarındayken 2001 yılı itibariyle 139 milyar dolara ulaşarak Fortune 500 listesinde beşinci sıraya yerleşmeyi başaran Enron Şirketinin iflasıyla dünya tarihinin en önemli muhasebe skandallarından biri gün yüzüne çıkmıştır. Enron'un 2000 yılı itibariyle mali olarak tamamen bitmiş olmasına rağmen, muhasebe kayıtlarında yaptığı manipülasyonlar ile bunu gizlemesi, Amerika genelinde kurumsal yönetime olan güveni derinden sarsmıştır. Benzer risklerin yeniden yaşanmaması için Amerika Birleşik Devletleri'nde 2002 yılında Halka Açık Şirketler Muhasebe Reformu ve Yatırımcıyı Koruma Kanunu veya diğer adıyla Sarbanes-Oxley Kanunu kabul edilmiştir. Sarbanes-Oxley Kanunun yürürlüğe girmesi ile kurumsal yönetim ve finansal raporlama ilkeleri Amerika Birleşik Devletleri'ndeki borsalarda işlem gören halka açık şirketlerin tamamını kapsayacak biçimde yasal bir zorunluluk haline gelmiştir. Özellikle Kanunun 302 ve 404. maddeleri çerçevesinde şirketlerin finansal raporlamaları üzerindeki risklerin belirlenmesi, belirlenen risklere ilişkin kontrollerin belgelendirilmesi ve değerlendirilmesi zorunlu tutulmuş ve kontrollerin etkinliğinden şirket yöneticileri doğrudan sorumlu tutulmuştur.

Sarbanes-Oxley Kanunu "Yönetim İç Kontrol Değerlemesi" başlıklı 404. maddesi başta olmak üzere şirketler açısından Kanuna uyumun hem zaman aldığı hem de oldukça maliyetli olduğu gerekçesiyle eleştirilmektedir[3]. Kanun ile iç kontrol ve risk yönetimine ilişkin olarak getirilen yükümlülüklerin hangi yöntem ve yaklaşımlarla hayata geçirileceği konusu ise daha sonra COSO (Committee of Sponsoring Organizations of the Treadway Commission) tarafından netleştirilmeye çalışılmıştır. Bu amaçla 1992 yılında yayımlanan İç Kontrol Çerçevesinin ardından COSO, bu kez 2004 yılında Kurumsal Risk Yönetimi Çerçevesini yayınlamıştır.

Yayımlanmasının hemen ardından COSO Kurumsal Risk Yönetimi (KRY) Çerçevesinin hızlı bir biçimde popüler olması temel olarak iki nedene bağlanabilir. Bunlardan ilki, COSO'nun Amerika'da faaliyet gösteren halka açık şirketler için Sarbanes-Oxley Kanunu ile getirilen yükümlülükler ile uyumlu bir çerçeve sunmasıdır (Borghesi ve Gaudenzi, 2013). Sarbanes-Oxley Kanunu ile yatırımcıları ve daha geniş anlamıyla halkı korumak, daha doğru bilgilendirmek, halka açık şirketlerin denetim standartlarını belirlemek ve denetçilerini denetlemek amacıyla Halka Açık Şirketler Kamu Muhasebe Gözetim Kurulu (the Public Company Accounting Oversight Board-PCAOB) kurulmuştur. Bu Kurul yayımladığı 2 numaralı standartta COSO Çerçevesinin yönetimin değerlendirilmesi için uygun ve elverişli bir çerçeve sunduğunu belirterek, bir anlamda COSO Çerçevesini Amerika

3) 20 milyar dolar veya daha fazla ciroya sahip büyük ABD işletmelerinin yaklaşık %60'ının, 100.000 adam-saate eşdeğer (bir yıl boyunca 70 kişinin tam zamanlı istihdamı anlamına gelmektedir) yatırım yapması gerektiği tahmin edilmektedir (Borghesi ve Gaudenzi, 2013).

Birleşik Devletleri'nde faaliyet gösteren halka açık şirketler için akredite etmiştir (Borghesi ve Gaudenzi, 2013). Ancak, bu durum COSO Çerçevesinin Amerika'da faaliyet gösteren ve risk olgunluk düzeyi yüksek olan halka açık, büyük şirketlere yönelik olduğu, risk olgunluk seviyesi düşük olan veya kurumsallaşmasını henüz tamamlayamamış göreli olarak daha küçük şirketlerde veya kamu kurumlarında uygulanmasında birtakım zorlukları bulunup bulunmadığı sorularını akla getirmektedir.

COSO Çerçevesinin hızlı bir şekilde popüler olmasının ikinci nedeni ise, COSO'nun yapısından kaynaklanmaktadır. COSO, Uluslararası İç Denetçiler Enstitüsü (IIA), Amerika Yeminli Muhasebeciler Enstitüsü (AICPA), Amerika Muhasebeciler Birliği (AAA), Yönetim Muhasebecileri Enstitüsü (IMA) ve Finans Yöneticileri Derneği'nin (FEI) destekleriyle kurulmuş olan bir yapıdır. Özellikle denetim, muhasebe ve finans alanında faaliyet gösteren önemli mesleki kuruluşların desteği COSO'nun, kurumsal risk yönetimi yarışına önde başlamasını sağlamıştır. Ancak, denetim, muhasebe ve finans ağırlıklı bu yaklaşım aynı zamanda, COSO Çerçevesinin kontrol ve uyum temelli olduğu, yönetim süreçlerine entegre edilmesinde ve stratejik düzeyde uygulanmasında birtakım zorlukları barındırdığını düşündürtmektedir.

COSO çerçevesinin yanı sıra ISO (Uluslararası Standartlar Örgütü), ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği), RIMS (Risk Yönetimi Topluluğu) ve FERMA (Avrupa Risk Yönetimi Birliği Federasyonu) gibi kuruluşlar risk yönetimi üzerine rehber ve standartlar yayımlamışlardır (Kıral, 2014). Bu rehberlerden ISO 31000, risk yönetimi ilkelerinin uygulanması için uluslararası kabul görmüş bir standart olarak 2009 yılında yayınlanmıştır. COSO denetçiler, muhasebeciler ve finans uzmanları tarafından yazılmışken, ISO, risk yönetimi uygulayıcıları ve uluslararası standart uzmanları tarafından yazılmıştır. Bu çerçeve ve standartları referans alan bazı ülkeler risk yönetimine ilişkin kendi rehberlerini yayımlamışlardır. Bu ülkelerden, Avustralya ve Yeni Zelanda risk yönetim modeli olan AS/NZS 4360 Risk Yönetim Rehberi ve İngiltere'nin BS31000 Risk Yönetim Rehberidir. Avustralya/Yeni Zelanda ve İngiltere Risk Yönetim Rehberleri ISO 31000 standartları dikkate alınarak hazırlanmıştır.

4. KURUMSAL RİSK YÖNETİMİNİN RİSKLERİ

Kurumsal Risk Yönetimine olan ilgi kamu kurumları, düzenleyici kurumlar, meslek kuruluşları ve derecelendirme şirketlerinin de talep ve yönlendirmeleriyle son 15 yılda hızla büyümüştür (Arena vd., 2010). Bu talep ve yönlendirmelerin de etkisiyle daha fazla firma ve kurum kurumsal risk yönetimi yaklaşımını benimsemiş ve hayata geçirmeye çalışmışlardır. Ancak, uygulamada kurumsal risk yönetimi yaklaşımının kendisinden beklenen etkileri gerçekleştirmenin oldukça uzağında olduğu yönünde eleştiriler de dile getirilmektedir (Mikes, 2009; Power, 2007).

Esasında kurumsal risk yönetimine ilişkin önemli ölçüde akademik çalışma olmasına rağmen, kurumsal risk yönetiminin uygulama sonuçları ve gerçekte etkileri olup olmadığı konusunda yapılan ampirik çalışma sayısı oldukça sınırlıdır (Arena vd., 2010; Gordon vd., 2009). Bu çalışmaların sınırlı olması, kurumsal risk yönetimi yaklaşımının gerçekten etkin mi olduğu yoksa kurumsal karar ve faaliyetlere herhangi bir etkisi olmayan, yalnızca yatırımcıların veya kamuoyunun "gözünü boyamak" için mi hazırlandığı yönündeki soruların net olarak cevaplanamamasına yol açmaktadır (Arena vd., 2010; Van der Stede, 2011; Paape ve Spekle, 2012).

Sınırlı olan ampirik çalışmalardan birisi, Vinnari ve Skærbæk (2014) tarafından yapılan ve risk yönetim araçlarının etkilerinin analiz edildiği çalışmadır. Yarı yapılandırılmış mülakatları ile yapılan çalışmanın sonucunda, risk yönetiminin giderek daha karmaşık hale geldiği ve paradoksal olarak risk yönetiminin kendisinin sürekli olarak çeşitli ve başka belirsizlikler ürettiğini ileri sürmüşlerdir. Vinnari ve Skærbæk (2014), standartlaştırılmış risk yönetimi çözümlerinin uygulamada zaman zaman yöneticilerin mesleki birikim ve profesyonel anlayışlarıyla çatıştığı ve bu çözümlerin artan bir şekilde uygulamalardan uzaklaştığı tespitlerine yer vermişlerdir.

Kurumsal risk yönetimi anlayışının bizzat kendisinin bazı riskleri barındırdığı yönündeki eleştiriler Vinnari ve Skaerbaek (2014) ile sınırlı değildir. Power (2004, 2009), Miller vd. (2008), Arena vd. (2010) ve Mikes (2011) gibi akademisyenler de kurumsal risk yönetimi yaklaşımının bazı riskleri barındırdığını ileri sürmüşlerdir. Bu risklerden; her şeyin risk yönetimi

anlayışı, teknik araçların yetersizliği ve aşırı kavramsallaşma risklerinin varlığı sebebiyle risk yönetiminin de iç kontrolün yaşadığı riskler ile karşı karşıya kalması muhtemel gözükmektedir.

4.1. Her Şeyin Risk Yönetiminden Hiçbir Şeyin Risk Yönetimine Dönüşme Riski

Power (2004), 1990'lı yılların sonlarından itibaren meydana gelen büyük kurumsal skandallar ve başarısızlıkların ardından, sağlık, güvenlik, sigorta ve proje yönetimi gibi geleneksel birincil riskler ile son zamanlarda ortaya çıkan itibar riski[4] gibi "insan yapımı" ikincil risklerin tümünü tek bir modelde birleştirmeyi amaçlayan kurumsal risk yönetimi çerçevelerinin kurumsal risk yönetimini "**her şeyin risk yönetimi**" anlayışına dönüştürdüğünü ileri sürmüştür (Vinnari and Skærbæk, 2014). Yazar, ayrıca her şeyin risk yönetimi anlayışının doğmasında, ABD'de Sarbanes-Oxley Kanunun önemli bir etken olduğu ve Kanunun, pratikte **"süreç-takıntılı, her şeyin risk yönetimi"** (process-obsessed risk management of everything) anlayışının doğmasına yol açtığını da iddia etmektedir (Power, 2004).

Bu kapsamda, Power (2009) katı bir biçimde kural tabanlı uyumluluk (rule-based compliance) ve denetim izi[5] üretmeye odaklanan kurumsal risk yönetimi anlayışının işlevinin sınırlı olduğunu, yalnızca hayali ve belki de tehlikeli bir güvence duygusu yarattığını ve kurumlar için pahalıya mal olabilecek "hiçbir şeyin risk yönetimi" (the risk management of nothing) ile sonuçlanabilecek yüzeysel bir kavramsal çerçeve oluşturduğunu iddia etmektedir (Mikes, 2011). Her şeyin risk yönetimi anlayışı, ayrıca, risk yönetimini, kurumun tüm süreçlerini kapsayan bir anlayıştan ziyade bir seferlik ve biraz da zoraki bürokratik/idari gerekliliklerin yerine getirilme anlayışının doğmasına neden olmuştur (Arena vd., 2010).

Mevcut kurumsal risk yönetimi çerçevelerinin sahip olduğu her şeyin risk yönetimi anlayışı sonucunda karşı karşıya kalınan hiçbir şeyin risk yönetimi sorununun çözümü için 80/20 Kuralı (Pareto Prensibi) uygulanabilir. Bu Kurala göre, sonuçların %80'i, nedenlerin %20'sinden kaynaklanır ya da diğer bir ifadeyle, faydanın büyük çoğunluğu, çabanın nispeten küçük bir yüzdesinden elde edilir. Bu Kuralı, risk yönetimine uyguladığımızda ise, bir kurumun amaçlarına ulaşmasını etkileyecek risklerin %80'ine, tüm süreçlerin yalnızca %20'sine denk gelen ve kritik olarak kabul edilen süreçler neden olmaktadır. Bu nedenle, etkili bir risk stratejisi geliştirmek ve riskleri başarılı bir şekilde yönetmek için kurumlar her şeyin risk yönetimi anlayışı yerine kurumsal hedeflere ulaşmada en büyük riske neden olan doğru kırılganlıkları belirlemelidir. Ancak, bu kuralı hiç dikkate almadan, önemli veya önemsiz tüm süreçleri kurumsal risk yönetiminin her aşamasında ve sürekli olarak dikkate almak, risk yönetimi çalışmalarını verimsizleştirerek, bu çalışmaları yalnızca belli dönemler itibariyle yapılması gereken bir iş yüküne (rutine) dönüştürmekte ve risk yönetimi çalışmalarının etkilerini ortadan kaldırmaktadır.

Aslında her düzeyde yönetici veya personelin görevlerini yaparken karşılaştığı çok sayıda riskler bulunmaktadır. Bu risklerin büyük çoğunluğu hayatın olağan akışında yasal düzenlemeler, tecrübe ve birikimler ışığında zaten yeterli düzeyde yönetilmektedir. Ancak her kurum için etkin bir biçimde yönetilmediği takdirde ve gerçekleşmesi durumunda insan sağlığını tehdit edebilen, kurumsal faaliyeti aksatabilecek veya kurumun itibar kaybetmesine neden olabilecek belli sayıda kritik risk vardır. Aynı şekilde her düzeyde yönetici veya personel bu riskleri de kendi bilgi birikimi ve tecrübesi ışığında ve çoğunlukla sistematik olmayan yöntemlerle yönetmeye çalışır. İşte tam bu noktada risk yönetimi, sonuçları itibariyle önemli etkileri olabilecek bu risklerin yönetiminde, risk yönetimini amaçlaştırmadan bir çözüm sunmalıdır. Aksi halde risk yönetimi anlayışı samanlıkta iğne aramaktan farksız olacak ve her şeyin risk yönetimi, hiçbir riskin yönetilememesi ile sonuçlanabilecektir.

---

4) Power (2004), itibar riskinin geç modern güvensizliğinin bir belirtisi (a symptom of late modern insecurity) olduğunu belirtmektedir. Yazar ayrıca, Shell'in 1995 yılında Kuzey Denizindeki bir petrol arama platformunu (Brent Spar) batırmak istemesi sebebiyle kamuoyu tepkileri üzerine çekmesiyle gündeme gelen itibar yönetimi fikri ve uygulamasının oldukça yeni olduğunu vurgulamaktadır (Power, 2004).

5) Denetim izi: Bir finansal ya da operasyonel işlemin başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtları ifade etmektedir.

4.2. Teknik Araçların Yetersizliğinden Kaynaklanan Riskler

Özellikle risk yönetiminin erken aşamalarında, sigorta anlayışı kapsamında risklerin devredilmesi söz konusu olduğunda bu risklerin sigorta firmalarınca ölçülmesi ya da finansal riskler söz konusu olduğunda teknik analiz ve ölçümler ile bu risklerin hesaplanması göreceli olarak daha kolay yapılmaktaydı. Ancak risk yönetiminin bu dar ve teknik yaklaşımından (Aseeri ve Bagajewicz, 2004; Jaafari, 2001), kurumsal düzeyde tüm süreçleri kapsayan ve stratejik amaçlarla ilişkilendirilen bir yaklaşıma geçilmesiyle kurumsal risk yönetimi belirsiz ve kullandığı araçlar bakımından iyi tanımlanmamış bir yapıya dönüşmüştür. Bu belirsizliğin sonucu olarak gün geçtikçe daha fazla kurum ve şirket kurumsal risk yönetimini benimsemesine rağmen uygulama sonuçlarının kurum ve şirketleri yeterince tatmin etmediği görülmektedir (Arena vd., 2010).

Kurumsal risk yönetiminin teknik düzeyden stratejik düzeye geçmesiyle risk hesaplaması zorlaşmış ve risk hesaplama yöntemi sübjektif bir hale gelmiştir. Zira Knight (1921), risk hesaplamasının (teknik hesaplara ya da geçmiş tecrübelerin istatistiklerine dayanarak) istatistiksel olarak bilinen bir olasılık dağılımının varlığını gerektirdiği ve bu dağılımı bilmenin mümkün olmaması durumunda riskten geriye sadece hesaplanma imkânı olmayan belirsizliğin kaldığını belirtmiştir. Diğer bir deyişle, neyi bilmediğimizi de bilmediğimiz bir durum söz konusu olmaktadır. Benzer şekilde, Mikes (2011) modele dayalı risk yönetiminin yalnızca belirsizliklerin olasılık dağılımlarının bilindiği veya istatistiksel olarak çıkarılabildiği durumlarda uygulanabileceğini, ancak tamamıyla ölçülemeyen belirsizliklere ilişkin bir şey söylemesinin beklenemeyeceğini belirtmiştir.

Öte yandan Borghesi ve Gaudenzi (2013) ise, işletmenin değerinin ölçümünün geleneksel olarak işletmenin finansal, gelir ve varlıkları dikkate alınarak hesaplandığına dikkat çekerek, risk analizlerinin de benzer yöntemlere dayandığını vurgulamışlardır. Bu durumda, özellikle kamusal ve yarı-kamusal mal ve hizmet üreten kamu kurumları için nasıl bir risk analiz modeli geliştirmemiz gerektiği sorusu halen cevaplanmayı beklemektedir.

4.3. Aşırı Kavramsallaşmadan Kaynaklanan Riskler

Risk yönetiminin bir diğer önemli riski ise, **aşırı kavramsallaşma** riskidir. Risk kapasitesi, risk iştahı, risk toleransı, risk tutumu ve risk eşiği gibi bir şekilde tanımlanabilse de ne şekilde ölçüleceği hala belirsiz olan bir dizi kavramlar ekseninde risk yönetim stratejilerini hayata geçirebilmenin işletme veya kurumlar için zorluğu ortadadır. Ayrıca, hem şirket veya kurumun faaliyet gösterdiği sektörel alana hem de zamana veya yönetimin önceliklerine göre değişebilen bu kavramların (eğer mümkünse bile) belirlenmesinin sübjektif olacağı ve bu sübjektif kararlara göre alınan risk stratejilerinin son derece hassas ve bu stratejilerden sapmanın son derece yüksek olacağı da göz ardı edilmemelidir.

Öte yandan, kavram seçimi de oldukça önemlidir. Örneğin en basitinden, yönetimin kabul edilebilir olduğunu düşündüğü risk seviyesini ifade etmek için kullanılan **'risk iştahı'** kavramını ele almak gerekirse, iştahı bilinç değil güdülerin yönlendirdiği açıktır. Belirlenmesi ve ölçülmesinin mümkün olup olmadığı tartışmaları bir yana bırakıldığında, kurumsal risk yönetimi anlayışının tam da merkezine yerleştirilen risk iştahı kavramının bilinçli bir seçim değil de güdüler ile yakından ilgili 'iştah' kavramıyla şekillendirilmesini sistematik ve bütüncül bir kurumsal risk yönetim anlayışı ile bağdaştırmak zordur.

4.4. Risk Yönetiminin 'İç Kontrolleşme' Riski

Bilindiği gibi iç kontrol ve ilgili kavramlar yeterince netleştirilemeden ve herkes tarafından aynı şekilde anlaşılamadan, diğer bir ifadeyle, 'içleri doldurulamadan' yıpranmış, anlaşılması ve kavranması güç '**soyut terimler lugatı**'na dönüşmüştür. Şüphesiz, iç kontrol kavramlarının anlaşılamadan yıpranmasında ve soyutlaşmasındaki en önemli faktör, bu metinlerin ülke ve sektör koşullarına uyarlan(a)madan doğrudan tercüme edilmesidir. Tercümenin verdiği konfor ile adeta sihirli küre misali her soruya cevap vermesi beklenen COSO küpü veya piramidi ile iç kontrol eğitimi veren çoğu eğiticinin olmazsa olmaz örneği "sınava geç kalmamak için bir öğrencinin risklerini nasıl kontrol etmesi gerektiği olmuş" ancak tek başına bu anlatım biçimi iç kontrol kavramlarının somutlaş-

tırılmasını ve iş süreçlerine uyarlanmasını yeterince sağlayamamıştır.

Böylece kavramlar özü itibariyle doğru ve herkes tarafından aynı şekilde anlaşılamadığından iç kontrol metodolojisi adeta bir '**dokümantasyon ve prosedürler yumağı**'na dönüşmüştür. Bunun sonucu olarak da iç kontrol sistemine yönelik iş ve işlemler, belli dönemler itibariyle yapılması zorunlu, kurumsal hedef ve faaliyetlerle doğrudan ilişkili olmayan ve bunlara katkı da sağlamayan 'iş yükü' olarak görülmeye başlanmıştır. Ancak, bu görüş ve yaklaşıma rağmen özveri ve (bir) gayretle kurumlarda iç kontrol sistemine yönelik çalışmalar yapılmıştır. Daha sonra, bu çalışmaların üst yönetimin öncelikli konular listesinde kendine yer bulamaması ve yıllar geçmesine rağmen üst yönetimde halen "farkındalık" oluşturmaya yönelik çalışmalara devam ediliyor olması, iç kontrol sisteminin henüz canlanamadan solma riski ile karşı karşıya kalmasına neden olmuştur.

Aslında iç kontrol sisteminin anlaşılamaması ve adeta dokümanlara boğulması, kurumları bu dokümantasyon ve prosedürlerden 'kurtarmayı' amaçlayan ve 'müşteri memnuniyeti'ni ön planda tutan **'iç kontrol sistemi kuruculari'**na da gün doğmasına yol açmıştır. Böylece kurumlar iç kontrol sistemi kurma risklerini bu 'kurtarıcı'lara devrederek, risklerini etkin bir biçimde yönetmeye çalışmışlardır. Ancak, 'günün sonunda' iç kontrol kurucuları da herhangi bir kurumda kullanıma hazır 'anahtar teslim' bir iç kontrol sistemi kurmayı başaramamışlardır. Zira herhangi bir kurumda iç kontrol sisteminin kurulabilmesi ve işlerlik kazanabilmesi öncelikle buna ilişkin kurumsal bir ihtiyaç hissedilmesi, kurumun tüm çalışanları ve üst yönetimi tarafından sahiplenilmesi ve gereklerinin yerine getirilmesi ile mümkün olabilecektir. Elbette iç kontrol sisteminin kuruluş aşamasında dış kaynak kullanımı/danışmanlık hizmeti alımı doğal ve kabul edilebilir bir durumdur. Ancak, bu danışmanların kurum çalışanları adına veya onların yerine iç kontrol sistemini kurmalarını ve 'tek tuşa basarak' bu sistemin çalışmasını beklemek iç kontrolün yeterince anlaşılamadığının en somut kanıtı olsa gerektir. İç kontrol için olduğu kadar kurumsal risk yönetimi için de geçerli olan bu tür riskler iyi yönetilemezse, maalesef, risk yönetimini de iç kontrolün içinde bulunduğu tehlike beklemektedir.

5. SONUÇ VE DEĞERLENDİRME

Kurumsal risk yönetimine yönelik yayımlanan uluslararası rehber ve standartlar risk yönetimine ilişkin genel bir çerçeve ve temel prensipleri belirlemektedirler. Ülkelerden veya sektörlerden bağımsız olarak risk yönetimine ilişkin genelgeçer kuralların belirlenmesinin, risk yönetimi anlayışının sistematik olarak ortaya konulması bakımından önemli olduğu bir gerçektir. Ancak bu gerçek, genelgeçer kuralların 'terzi işi' (tailor made) yaklaşımla ülkenin ve/veya sektörün kendine has özelliklerini göz önünde bulundurarak 'uygulanabilir' bir modele dönüştürülmesi konusunun önemini azaltmamaktadır. Aksine, bahsedilen çerçevelerin içinin ülkenin ve sektörün gerçekleri ile doldurulması bu çerçevelerin uygulanabilirliğini de artıracaktır.

Özel sektör, kamu sektörü, kamu teşebbüsleri veya operasyonel, finansal ve güvenlik gibi farklı sektörlerde faaliyet gösteren, birbirinden farklı çeşitli karma yapıların varlığı dikkate alındığında katı bir biçimde standartlaştırılmış çerçevelerin bu yapıların tümüne nüfuz edebilmeleri ve kurumsal yönetim süreçlerine erişebilmeleri oldukça zor gözükmektedir. Aslında bu durum, sürekli değişen bir dünyada değişmez çözümler bulmaya çalışan tüm çaba ve girişimlerin karşılaşması muhtemel bir sonuçtur.

Dolayısıyla ülke ve sektör koşullarını dikkate alarak, tanımlanması ve ölçülmesi pek de mümkün olmayan kavramlardan kaçınarak ve tüm süreçlerin risk yönetimi değil, önemli ve az sayıda risklerin etkin yönetimini esas alan bir modele ihtiyaç bulunmaktadır. Aksi halde, risk yönetiminin, iç kontrolün yaşadığına benzer bir risk ile karşı karşıya kalması kaçınılmaz olacaktır.

Bu bakımdan iç kontrol alanında yaşanan durumun risk yönetimi alanında da yaşanmaması için halen elimizde imkân bulunmaktadır. Bunun için öncelikli olarak risk yönetimine ilişkin yaygın kabul gören standart ve çerçevelerden yararlanılmakla birlikte bu çerçeve ve standartları olduğu gibi çevirip yayımlama kolaylığından kaçınarak, ülke ve sektör birikimlerinin yansıtıldığı bir risk yönetimi modeli tasarlanmalıdır. Yalnızca Türkiye'deki bankacılık sektörüne bakıldığında bile, son yıllarda oluşan bilgi birikimi ve tecrübenin en az söz konusu standart ve çerçeveler kadar değerli ve dikkate alınması gereken bir unsur olduğu görülecektir.

Öte yandan, kurumsal risk yönetimi, kurumun tümünde uygulanan sistematik bir süreçtir. Kurumsal risk yönetiminin etkinliğini bir kurumun veya işletmenin tüm faaliyetlerinin sistematik bir hale getirilmesini ifade eden kurumsallaşmadan bağımsız düşünmek mümkün değildir. Bu kapsamda, herhangi bir kurum veya işletme kurumsallaştığı ölçüde kurumsal risk yönetimi de kurumsallaşacaktır. Henüz kurumsallaşmanın erken aşamalarında bulunan bir kurum veya işletmede kurumsal risk yönetiminin tartışılıyor olması ise, *"köy kahvesinde soğuk füzyon tartışma*[6]*"*nın ötesinde bir anlam taşımayacaktır.

Kaynakça

1) ARENA, M., ARNABOLDI, M. ve AZZONE, G. (2010). The Organizational Dynamics of Enterprise Risk Management. *Accounting, Organizations and Society* 35, 659–675.

2) ASEERI, A. ve BAGAJEWICZ, M. J. (2004). New Measures and Procedures to Manage Financial Risk with Applications to the Planning of Gas Commercialization in Asia". *Computers and Chemical Engineering*, 28(12), 2791–2821.

3) BECK, U. (2014). *Risk Toplumu-Başka Bir Modernliğe Doğru*. K. Özdoğan ve B. Doğan (çev.). İstanbul: İthaki Yayınları.

4) BORGHESI, A. ve GAUDENZI, B., (2013). *Risk Management: How to Assess, Transfer, and Communicate Critical Risks*. Springer, Milan, New York.

5) CASSAR, G., ve GERAKOS, J. (2013). "Does Risk Management Work?" Chicago Booth Research Paper No. 13-13. Available at SSRN: http//ssrn.com/abstract = 1722250.

6) FRASER, J. ve SIMKINS, B. (2010). *Enterprise Risk Management*. John Wiley and Sons.

7) FUREDİ, F. (2001). *Korku Kültürü*, Çev. Barış Yıldırım, Ayrıntı Yayınları, İstanbul.

8) GORDON, L., LOEB, M ve TSENG, C.-Y. (2009). "Enterprise Risk Management and Firm Performance: A Contingency Perspective". *Journal of Accounting and Public Policy* 28, 301–327.

9) HAMPTON, J. (2009). *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity*, AMACOM, Special Ed.

10) HILLSON D. A. ve MURRAY-WEBSTER R. (2005). *Understanding and Managing Risk Attitude*. Aldershot, UK: Gower

11) HILLSON, D. A. (2009). *Managing Risk in Projects*. Farnham, Surrey, UK, Gower.

12) HOPKIN, P. (2010). *Fundamentals of Risk Management: Understanding Evaluating and Implementing Effective Risk Management*, Kogan Page.

13) İDKK (İÇ DENETİM KOORDİNASYON KURULU). (2013). *Kamu İç Denetim Rehberi*, Ankara.

14) JAAFARI, A. (2001). "Management of Risks, Uncertainties and Opportunities on Projects: Time for a Fundamental Shift". *International Journal of Project Management*, 19(2), 89–101.

15) KAHNEMAN, D. (2011). *Thinking Fast and Slow*. Farrar, Straus and Giroux.

16) KIRAL, H. (2014), "İç Denetimin Kurumsal Risk Yönetimindeki Rolü", H. Kıral, (Ed.), İç Denetim "Yönetime Değer Katmak" (317-332). Ankara: İç Denetim Koordinasyon Kurulu Yayınları No:1.

17) KNIGHT, F.H. (1921). *Risk, Uncertainty, and Profit*, Hart, Schaffner & Marx, Boston, MA.

18) MCGINN, K. (2009). Walking on eggshells. Waste Age, 1(February), 24. https://www.waste360.com/Waste_Safety/insurance-trends-enterprise-risk-management-200902, Erişim Tarihi: 15.08.2018

19) MEHR, R.I. ve HEDGES, B.A. (1963). *Risk Management in the Business Enterprise*, Irwin, Homewood, Illinois.

20) MERNA, T. ve FAISAL, F. A. (2008). *Corporate Risk Management*, 2nd Edition, John Wiley & Sons Ltd.

21) MIKES, A. (2009). "Risk management and calculative cultures", *Management Accounting Research*, Vol. 20 No. 1, pp. 18-40.

22) MIKES, A. (2011). "From counting risk to making risk count: boundary-work in risk management", *Accounting, Organizations and Society*, Vol. 36 Nos 4/5, pp. 226-245.

23) MILLER, P., KURUNMAKI, L. ve O'LEARY, T. (2008). "Accounting, hybrids and the management of risk", *Accounting, Organizations and Society*, Vol. 33 Nos 7/8, pp. 942-967.

24) MURRAY-WEBSTER, R.ve HİLLSON, D.A. (2008). *Managing Group Risk Attitude*, Gower, Aldershot, UK.

25) O'DONNELL, A. (2009). Regaining trust. Insurance & Technology, 1(January), 28.

26) PAAPE, L. ve SPEKLE, R. (2012). "The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study". *European Accounting Review,* 21, 533–564.

27) POWER, M. (2004). *The Risk Management of Everything: Rethinking the Politics of Uncertainty*, Demos, London.

28) POWER, M. (2007). *Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press, Oxford.

6) Bu ifade Sayın Gökhan Macit ile Karayolları Genel Müdürlüğü İç Denetim Birim Başkanı iken yapılan söyleşiden alıntıdır.

29) POWER, M. (2009). "The Risk Management of Nothing", *Accounting, Organizations and Society*, Vol. 34 Nos 6/7, pp. 849-855.

30) PRICE, T. (2008). Uncovering Unknown Risk. Wall Street & Technology, 1(December), 36.

31) SCHNEIER, B. (2008), "Does Risk Management Make Sense?" Information Security Magazine, https://www.schneier.com/blog/archives/2008/10/does_risk_manag.html, Erişim Tarihi: 18.07.2018

32) STAMATIS, D. H. (2014). *Introduction to Risk and Failures: Tools and Methodologies*, CRC Press.

33) SWEETING, P. (2011). *Financial Enterprise Risk Management*, Cambridge University Press.

34) TALEB, N. (2008). *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets.* New York, NY: Random House.

35) VAN DER STEDE, W. A. (2011). "Management Accounting Research in the Wake of the Crisis: Some Reflections". *European Accounting Review*, 20 (4), 605–623.

36) VINNARI, E. ve SKÆRBÆK, P. (2014). "The uncertainties of risk management: A field study on risk management internal audit practices in a Finnish municipality, *Accounting, Auditing & Accountability Journal*, Vol. 27 No. 3, 2014, pp. 489-526.

37) WILLIAMS, A. ve HEINS M.H. (1964). *Risk Management and Insurance*, McGrawHill, New York.